I

Name……………………………………………………………………………..

Roll No. …………………………….Year 20………..20……………

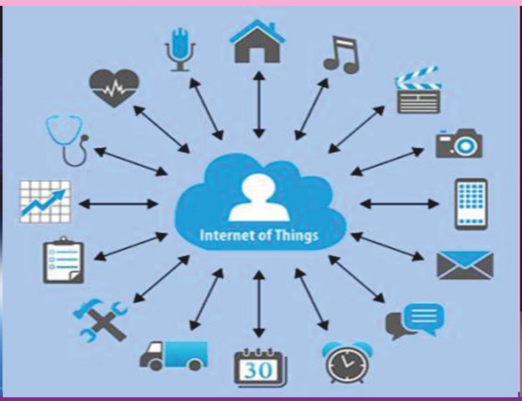
Exam Seat No.……………………………………………………………….

COMPUTER GROUP | SEMESTER – VI | DIPLOMA IN ENGINEERING AND TECHNOLOGY

LEARNING MANUAL

FOR

Emerging Trends in Computer Engineering and Information Technology (22618)



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI

(Autonomous) (ISO 9001 : 2015) (ISO / IEC 27001 : 2013)

A Learning Material for

Emerging Trends in Computer Engineering and Information Technology

(22618)

Semester - VI

(CO, CM, CW, IF)

Maharashtra State

Board of Technical Education, Mumbai

(Autonomous)(ISO:9001:2015) (ISO/IEC 27001:2013)

Maharashtra State
Board of Technical Education, Mumbai

(Autonomous) (ISO:9001:2015) (ISO/IEC 27001:2013)
4th Floor, Government Polytechnic Building, 49, Kherwadi,
Bandra (East), Mumbai -400051.
(Printed on May, 2018)

Maharashtra State
Board of Technical Education

Certificate

This is to certify that Mr. / Ms. ………………………………….. Roll No……………………….of ……….. Semester of Diploma in……..……………………..……………………………of Institute…………………………………….……….(Code……… ………..) has attained pre-defined practical outcomes(PROs) satisfactorily in course**Emerging Trends in CO and IT(22618)**for the academic year 20…….to 20…..... as prescribed in the curriculum.

Place ……………….   Enrollment No……………………

Date:…....................   Exam Seat No. …………………....

Course Teacher   **Head of the Department**   **Principal**

Seal of the
Institute

Preface

The primary focus of any engineering work in the technical education system is to develop the much needed industry relevant competency & skills. With this in view, MSBTE embarked on innovative “I” scheme curricula for engineering diploma programmes with outcome based education through continuous inputs from socio economic sectors. The industry experts during the consultation while preparing the Perspective Plan for diploma level technical education categorically mentioned that the curriculum, which is revised and implemented normally further revised after 4-5 years. The technological advancements being envisaged and faced by the industry in the present era are rapid and curriculum needs to be revised by taking care of such advancements and therefore should have a provision of accommodating continual changes. These views of industry experts were well taken & further discussed in the academic committee of MSBTE, wherein it was decided to have a dynamism in curriculum for imparting the latest technological advancements in the respective field of engineering. In order to provide an opportunity to students to learn the technological advancements, a course with a nomenclature of “Emerging Trends in Computer Engineering & Information Technology” is introduced in the 6th semester of Computer Engineering & Information Technology Group.

The technological advancements to be depicted in the course called emerging trends was a challenging task and therefore it was decided to prepare a learning material with the involvement of industrial and academic experts for its uniformity in the aspect of delivery, implementation and evaluation.

Advancements and applications of Computer Engineering and Information Technology are ever changing. Emerging trends aims at creating awareness about major trends that will define technological disruption in the upcoming years in the field of Computer Engineering and Information Technology. IoT, Digital Forensics and Hacking are some emerging areas which are covered in this course and are expected to generate increasing demand as IT professionals and open avenues of entrepreneurship. Considering the necessity of Artificial intelligence (AI) which is an area of computer science that emphasizes the creation of intelligent machines that work and react like humans, it is important for Diploma to be aware of AI concept.

This learning manual is designed to help all stakeholders, especially the students and teachers and to develop in the student the pre-determined outcomes. It is expected to explore further by both students and teachers, on the various topics mentioned in learning manual to keep updated themselves about the advancements in related technology.

MSBTE wishes to thank the Learning Manual development team, specifically Mr. Nareshumar Harale, Chairman of the Course Committee, Industry Experts, Smt. M.U. Kokate Coordinator of the Computer Engineering & Mr. J. R. Nikhade, Coordinator of the Information Technology and academic experts for their intensive efforts to formulate the learning material on “Emerging Trends in Computer Engineering & Information Technology”. Being emerging trend and with the provision of dynamism in the curricula, any suggestions towards enrichment of the topic and thereby course will be highly appreciated.

(Dr. Vinod M.Mohitkar)
Director
MSBTE, Mumbai

COURSE OUTCOMES (COs) achieved through this course

- Describe Artificial Intelligence, Machine learning and deep learning
- Interpret IoT concepts
- Compare Models of Digital Forensic Investigation.
- Describe Evidence Handling procedures.
- Describe Ethical Hacking process.
- Detect Network, Operating System and applications vulnerabilities

Emerging Trendsin Computer Engineering and Information Technology

Index

Unit-1 Artificial Intelligence

Content

1.1 Introduction of AI

- Concept
- Scope of AI
- Components of AI
- Types of AI
- Application of AI

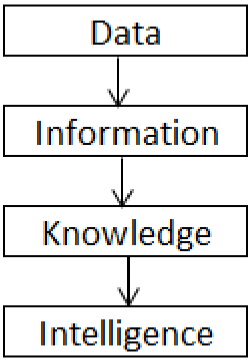
1.2 Concept of machine learning and deep learning.

1.1 Introduction of AI

A branch of Computer Science named Artificial Intelligence (AI)pursues creating the computers / machines as intelligent as human beings. John McCarthy the father of Artificial Intelligence described AI as, **“The science and engineering of making intelligent machines, especially intelligent computer programs”.** Artificial Intelligence (AI) is a branch of Science which deals with helping machines find solutions to complex problems in a more human-like fashion.

Artificial is defined in different approaches by various researchers during its evolution, such as “Artificial Intelligence is the study of how to make computers do things which at the moment, people do better.”

There are other possible definitions “like AI is a collection of hard problems which can be solved by humans and other living things, but for which we don’t have good algorithms for solving.” e. g., understanding spoken natural language, medical diagnosis, circuit design, learning, self-adaptation, reasoning, chess playing, proving math theories, etc.



- **Data:** Data is defined as symbols that represent properties of objects events and their environment.
- **Information:** Information is a message that contains relevant meaning, implication, or input for decision and/or action.
- **Knowledge:** It is the (1) cognition or recognition (know-what), (2) capacity to act(know-how), and(3)understanding (know-why)that resides or is contained within the mind or in the brain.

- **Intelligence:** It requires ability to sense the environment, to make decisions, and to control action.

1.1.1 Concept:

Artificial Intelligence is one of the emerging technologies that try to simulate human reasoning in AI systems The art and science of bringing learning, adaptation and self-organization to the machine is the art of Artificial Intelligence. Artificial Intelligence is the ability of a computer program to learn and think.Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that work and reacts like humans. AI is built on these three important concepts

Machine learning: When you command your smartphone to call someone, or when you chat with a customer service chatbot, you are interacting with software that runs on AI. But this type of software actually is limited to what it has been programmed to do. However, we expect to soon have systems that can learn new tasks without humans having to guide them. The idea is to give them a large amount of examples for any given chore, and they should be able to process each one and learn how to do it by the end of the activity.

Deep learning: The machine learning example I provided above is limited by the fact that humans still need to direct the AI's development. In deep learning, the goal is for the software to use what it has learned in one area to solve problems in other areas. For example, a program that has learned how to distinguish images in a photograph might be able to use this learning to seek out patterns in complex graphs.

Neural networks: These consist of computer programs that mimic the way the human brain processes information. They specialize in clustering information and recognizing complex patterns, giving computers the ability to use more sophisticated processes to analyze data.

1.1.2 Scope of AI:

The ultimate goal of artificial intelligence is to create computer programs that can solve problems and achieve goals like humans would. There is scope in developing machines in robotics, computer vision, language detection machine, game playing, expert systems, speech recognition machine and much more.

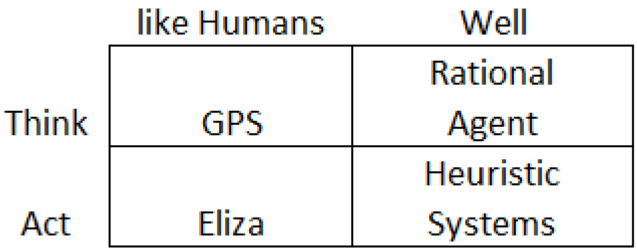
The following factors characterize a career in artificial intelligence:

- Automation
- Robotics
- The use of sophisticated computer software

Individuals considering pursuing a career in this field require specific education based on the foundations of math, technology, logic and engineering perspectives. Apart from these, good communication skills (written and verbal) are imperative to convey how AI services and tools will help when employed within industry settings.

AI Approach:

The difference between machine and human intelligence is that the human think / act rationally compare to machine. Historically, all four approaches to AI have been followed, each by different people with different methods.



	like Humans	Well
Think	GPS	Rational Agent
Act	Eliza	Heuristic Systems

Fig 1.1 AI Approaches

Think Well:

Develop formal models of knowledge representation, reasoning, learning, memory, problem solving thatcan be rendered in algorithms. There is often an emphasis on a systems that are provably correct, and guarantee finding an optimal solution.

Act Well:

For a given set of inputs, generate an appropriate output that is not necessarily correct but gets the job done.

- A heuristic (heuristic rule, heuristic method) is a rule of thumb, strategy, trick, simplification, or any other kind of device which drastically limits search for solutions in large problem spaces.
- Heuristics do not guarantee optimal solutions; in fact, they do not guarantee any solution at all:
- all that can be said for a useful heuristic is that it offers solutions which are good enough most of the time

Think like humans:

Cognitive science approach. Focus not just on behavior and I/O but also look at reasoning process.

The Computational model should reflect “how” results were obtained. Provide a new language forexpressing cognitive theories and new mechanisms for evaluating them.

GPS (General Problem Solver): Goal not just to produce humanlike behavior (like ELIZA), but to produce a sequence of steps of the reasoning process that was similar to the steps followed by a person in solving the same task.

Act like humans:

Behaviorist approach-Not interested in how you get results, just the similarity to what human results are.

Example: ELIZA: A program that simulated a psychotherapist interacting with a patient and successfully passed the Turing Test. It was coded at MIT during 1964-1966 by Joel Weizenbaum. First script was DOCTOR. The script was a simple collection of syntactic patterns not unlike regular expressions. Each pattern had an associated reply which might include bits of the input (after simple transformations (my →your) Weizenbaum was shocked at reactions: Psychiatrists thought it had potential. People unequivocally anthropomorphized.

1.1.3 Components of AI

The core components and constituents of AI are derived from the concept of logic, cognition and computation; and the compound components, built-up through core components are knowledge, reasoning, search, natural language processing, vision etc.

Level	Core	Compound	Coarse components
Logic	**Induction** **Proposition** **Tautology** **Model Logic**	**Knowledge** **Reasoning** **Control** **Search**	**Knowledge based systems** **Heuristic Search** **Theorem Proving**
Cognition	**Temporal Learning** **Adaptation** **Self-organization**	**Belief** **Desire** **Intention**	**Multi Agent system** **Co-operation** **Co-ordination** **AI Programming**
Functional	**Memory** **Perception**	**Utterance**	**Vision** **Natural Language** **Speech Processing**

The core entities are inseparable constituents of AI in that these concepts are fused at atomic level. The concepts derived from logic are propositional logic, tautology, predicate calculus, model and temporal logic. The concepts of cognitive science are of two types: one is functional which includes learning, adaptation and self-organization, and the other is memory and perception which are physical entities. The physical entities generate some functions to make the compound components

The compound components are made of some combination of the logic and cognition stream. These are knowledge, reasoning and control generated from constituents of logic such as predicate calculus, induction and tautology and some from cognition (such as learning and adaptation). Similarly, belief, desire and intention are models of mental states that are predominantly based on cognitive components but less on logic. Vision, utterance (vocal) and expression (written) are combined effect of memory and perceiving organs or body sensors such as ear, eyes and vocal. The gross level contains the constituents at the third level which are knowledge-based systems (KBS), heuristic search, automatic theorem proving, multi-agent systems, Al languages such as PROLOG and LISP, Natural language processing (NLP). Speech processing and vision are based mainly on the principle of pattern recognition.

AI Dimension: The philosophy of Al in three-dimensional representations consists in logic, cognition and computation in the x-direction, knowledge, reasoning and interface in the y-direction. The x-y plane is the foundation of AI. The z-direction consists of correlated systems of physical origin such as language, vision and perception as shown in Figure.1.1

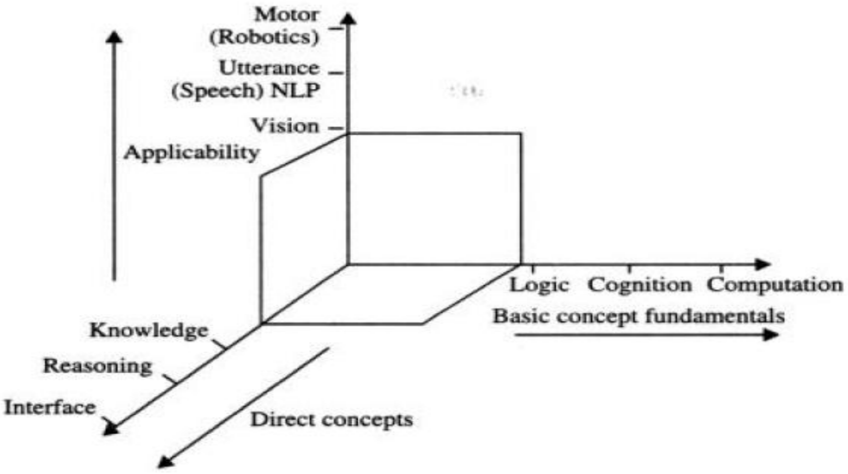


Fig. 1.2 Three dimensional model of AI

The First Dimension (Core)

The theory of logic, cognition and computation constitutes the fusion factors for the formation of one of the foundations on coordinate x-axis. Philosophy from its very inception of origin covered all the facts, directions and dimensions of human thinking output. Aristotle's theory of syllogism, Descartes and Kant's critic of pure reasoning and contribution of many other philosophers made knowledge-based on logic. It were Charles Babbage and Boole who demonstrated the power of computation logic. Although the modern philosophers such as Bertrand Russell correlated logic with mathematics but it was Turing who developed the theory of computation for mechanization. In the 1960s, Marvin Minsky pushed the logical formalism to integrate reasoning with knowledge.

Cognition:

Computers has became so popular in a short span of time due to the simple reason that they adapted and projected the information processing paradigm (IPP) of human beings: sensing organs as input, mechanical movement organs as output and the central nervous system (CNS) in brain as control and computing devices, short-term and long-term memory were not distinguished by computer scientists but, as a whole, it was in conjunction, termed memory.

In further deepening level, the interaction of stimuli with the stored information to produce new information requires the process of learning, adaptation and self-organization. These functionalities in the information processing at a certain level of abstraction of brain activities demonstrate a state of mind which exhibits certain specific behaviour to qualify as intelligence. Computational models were developed and incorporated in machines which mimicked the functionalities of human origin. The creation of such traits of human beings in the computing devices and processes originated the concept of intelligence in machine as virtual mechanism. These virtual machines were termed in due course of time artificial intelligent machines.

Computation

The theory of computation developed by Turing-finite state automation—was a turning point in mathematical model to logical computational. Chomsky's linguistic computational theory generated a model for syntactic analysis through a regular grammar.

The Second Dimension

The second dimension contains knowledge, reasoning and interface which are the components of knowledge-based system (KBS). Knowledge can be logical, it may be processed as information which is subject to further computation. This means that any item on the y-axis is correlated with any item on the x-axis to make the foundation of any item on the z-axis. Knowledge and reasoning are difficult to prioritize, which occurs first: whether knowledge is formed first and then reasoning is performed or as reasoning is present, knowledge is formed. Interface is a means of communication between one domain to another. Here, it connotes a different concept then the user's interface. The formation of a permeable membrane or transparent solid structure between two domains of different permittivity is termed interface. For example, in the industrial domain, the robot is an interface. A robot exhibits all traits of human intelligence in its course of action to perform mechanical work. In the KBS, the user's interface is an example of the interface between computing machine and the user. Similarly, a program is an interface between the machine and the user. The interface may be between human and human, i.e. experts in one domain to experts in another domain. Human-to-machine is program and machine-to-machine is hardware. These interfaces are in the context of computation and AI methodology.

The Third Dimension

The third dimension leads to the orbital or peripheral entities, which are built on the foundation of x-y plane and revolve around these for development. The entities include an information system. NLP, for example, is formed on the basis of the linguistic computation theory of Chomsky and concepts of interface and knowledge on y-direction. Similarly, vision has its basis on some computational model such as clustering, pattern recognition computing models and image processing algorithms on the x-direction and knowledge of the domain on the y-direction.

The third dimension is basically the application domain. Here, if the entities are near the origin, more and more concepts are required from the x-y plane. For example, consider information and automation, these are far away from entities on z-direction, but contain some of the concepts of cognition and computation model respectively on x-direction and concepts of knowledge (data), reasoning and interface on the y-direction.

In general, any quantity in any dimension is correlated with some entities on the other dimension.

The implementation of the logical formalism was accelerated by the rapid growth in electronic technology, in general and multiprocessing parallelism in particular.

1.1.4 Types of AI

Artificial Intelligence can be divided in various types, there are mainly two types of main categorization which are based on capabilities and based on functionally of AI. Following is flow diagram which explain the types of AI.

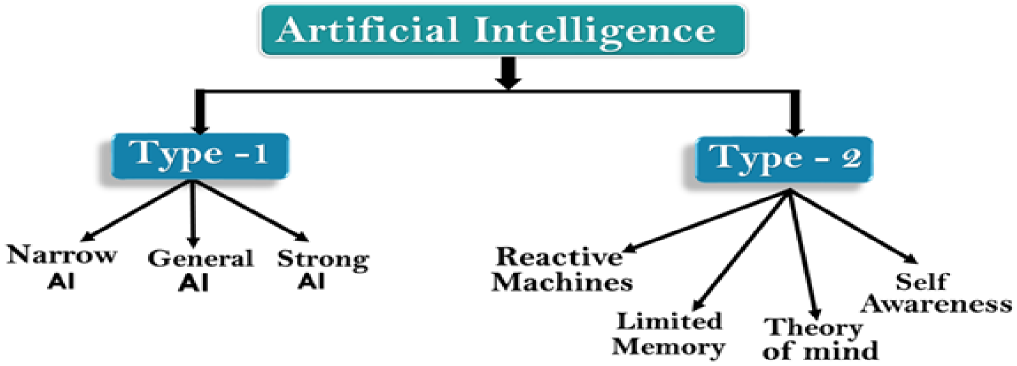


Fig 1.3 Types of AI

AI type-1: Based on Capabilities

1. Weak AI or Narrow AI:

- Narrow AI is a type of AI which is able to perform a dedicated task with intelligence. The most common and currently available AI is Narrow AI in the world of Artificial Intelligence.
- Narrow AI cannot perform beyond its field or limitations, as it is only trained for one specific task. Hence it is also termed as weak AI. Narrow AI can fail in unpredictable ways if it goes beyond its limits.
- Apple Siriis a good example of Narrow AI, but it operates with a limited pre-defined range of functions.
- IBM's Watson supercomputer also comes under Narrow AI, as it uses an Expert system approach combined with Machine learning and natural language processing.
- Some Examples of Narrow AI are playing chess, purchasing suggestions on e-commerce site, self-driving cars, speech recognition, and image recognition.

2. General AI:

- General AI is a type of intelligence which could perform any intellectual task with efficiency like a human.
- The idea behind the general AI to make such a system which could be smarter and think like a human by its own.
- Currently, there is no such system exist which could come under general AI and can perform any task as perfect as a human.
- The worldwide researchers are now focused on developing machines with General AI.
- As systems with general AI are still under research, and it will take lots of efforts and time to develop such systems.

3. Super AI:

- Super AI is a level of Intelligence of Systems at which machines could surpass human intelligence, and can perform any task better than human with cognitive properties. It is an outcome of general AI.
- Some key characteristics of strong AI include capability include the ability to think, to reason, solve the puzzle, make judgments, plan, learn, and communicate by its own.
- Super AI is still a hypothetical concept of Artificial Intelligence. Development of such systems in real is still world changing task.

Artificial Intelligence type-2: Based on functionality

1. Reactive Machines

- Purely reactive machines are the most basic types of Artificial Intelligence.
- Such AI systems do not store memories or past experiences for future actions.
- These machines only focus on current scenarios and react on it as per possible best action.
- IBM's Deep Blue system is an example of reactive machines.
- Google's AlphaGo is also an example of reactive machines.

2. Limited Memory

- Limited memory machines can store past experiences or some data for a short period of time.
- These machines can use stored data for a limited time period only.
- Self-driving cars are one of the best examples of Limited Memory systems. These cars can store recent speed of nearby cars, the distance of other cars, speed limit, and other information to navigate the road.

3. Theory of Mind

- Theory of Mind AI should understand the human emotions, people, beliefs, and be able to interact socially like humans.
- This type of AI machines are still not developed, but researchers are making lots of efforts and improvement for developing such AI machines.

4. Self-Awareness

- Self-awareness AI is the future of Artificial Intelligence. These machines will be super intelligent, and will have their own consciousness, sentiments, and self-awareness.
- These machines will be smarter than human mind.
- Self-Awareness AI does not exist in reality still and it is a hypothetical concept.

1.1.5 Application of AI

AI has been dominant in various fields such as −

- **Gaming:** AI plays crucial role in strategic games such as chess, poker, tic-tac-toe, etc., where machine can think of large number of possible positions based on heuristic knowledge.

- **Natural Language Processing:** It is possible to interact with the computer that understands natural language spoken by humans.
- **Expert Systems:** There are some applications which integrate machine, software, and special information to impart reasoning and advising. They provide explanation and advice to the users.
- **Vision Systems:** These systems understand, interpret, and comprehend visual input on the computer. For example,
    - A spying aeroplane takes photographs, which are used to figure out spatial information or map of the areas.
    - Doctors use clinical expert system to diagnose the patient.
    - Police use computer software that can recognize the face of criminal with the stored portrait made by forensic artist.
- **Speech Recognition:** Some intelligent systems are capable of hearing and comprehending the language in terms of sentences and their meanings while a human talks to it. It can handle different accents, slang words, noise in the background, change in human’s noise due to cold, etc.
- **Handwriting Recognition:** The handwriting recognition software reads the text written on paper by a pen or on screen by a stylus. It can recognize the shapes of the letters and convert it into editable text.
- **Intelligent Robots:** Robots are able to perform the tasks given by a human. They have sensors to detect physical data from the real world such as light, heat, temperature, movement, sound, bump, and pressure. They have efficient processors, multiple sensors and huge memory, to exhibit intelligence. In addition, they are capable of learning from their mistakes and they can adapt to the new environment.

1.2 Concept of machine learning and deep learning

1.2.1 Machine Learning:

- Machine learning is a branch of science that deals with programming the systems in such a way that they automatically learn and improve with experience. Here, learning means recognizing and understanding the input data and making wise decisions based on the supplied data.
- It is very difficult to cater to all the decisions based on all possible inputs. To tackle this problem, algorithms are developed. These algorithms build knowledge from specific data and past experience with the principles of statistics, probability theory, logic, combinatorial optimization, search, reinforcement learning, and control theory.

The developed algorithms form the basis of various applications such as:

- Vision processing
- Language processing
- Forecasting (e.g., stock market trends)
- Pattern recognition
- Games
- Data mining
- Expert systems

- Robotics

Machine learning is a vast area and it is quite beyond the scope of this tutorial to cover all its features. There are several ways to implement machine learning techniques, however the most commonly used ones are **supervised** and **unsupervised learning**.

Supervised Learning: Supervised learning deals with learning a function from available training data. A supervised learning algorithm analyzes the training data and produces an inferred function, which can be used for mapping new examples. Common examples of supervised learning include:

- classifying e-mails as spam,
- labeling webpages based on their content, and
- voice recognition.

There are many supervised learning algorithms such as neural networks, Support Vector Machines (SVMs), and Naive Bayes classifiers. Mahout implements Naive Bayes classifier.

Unsupervised Learning: Unsupervised learning makes sense of unlabeled data without having any predefined dataset for its training. Unsupervised learning is an extremely powerful tool for analyzing available data and look for patterns and trends. It is most commonly used for clustering similar input into logical groups. Common approaches to unsupervised learning include:

- k-means
- self-organizing maps, and
- hierarchical clustering

1.2.2 Deep Learning

Deep learning is a subfield of machine learning where concerned algorithms are inspired by the structure and function of the brain called artificial neural networks.

All the value today of deep learning is through supervised learning or learning from labelled data and algorithms.

Each algorithm in deep learning goes through the same process. It includes a hierarchy of nonlinear transformation of input that can be used to generate a statistical model as output.

Consider the following steps that define the Machine Learning process

- Identifies relevant data sets and prepares them for analysis.
- Chooses the type of algorithm to use
- Builds an analytical model based on the algorithm used.
- Trains the model on test data sets, revising it as needed.
- Runs the model to generate test scores.

Deep learning has evolved hand-in-hand with the digital era, which has brought about an explosion of data in all forms and from every region of the world. This data, known simply as big data, is drawn from sources like social media, internet search engines, e-commerce platforms, and online cinemas, among others. This enormous amount of data is readily accessible and can be shared through fintech applications like cloud computing.

However, the data, which normally is unstructured, is so vast that it could take decades for humans to comprehend it and extract relevant information. Companies realize the incredible potential that can result from unraveling this wealth of information and are increasingly adapting to AI systems for automated support.

Applications of Machine Learning and Deep Learning

- Computer vision which is used for facial recognition and attendance mark through fingerprints or vehicle identification through number plate.
- Information Retrieval from search engines like text search for image search.
- Automated email marketing with specified target identification.
- Medical diagnosis of cancer tumors or anomaly identification of any chronic disease.
- Natural language processing for applications like photo tagging. The best example to explain this scenario is used in Facebook.
- Online Advertising.

References:

- https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_overview.htm
- https://www.javatpoint.com/introduction-to-artificial-intelligence
- https://www.tutorialspoint.com/tensorflow/tensorflow_machine_learning_deep_learning.htm

Sample Multiple Choice Questions

1. __________________is a branch of Science which deals with helping machines find solutions to complex problems in a more human-like fashion
   a. Artificial Intelligence
   b. Internet of Things
   c. Embedded System
   d. Cyber Security
2. In _______________ the goal is for the software to use what it has learned in one area to solve problems in other areas.
   a. Machine learning
   b. Deep learning
   c. Neural networks
   d. None of these
3. Computer programs that mimic the way the human brain processes information is called as
   a. Machine learning
   b. Deep learning
   c. Neural networks
   d. None of these

4. The core components and constituents of AI are derived from
   a. concept of logic
   b. cognition
   c. computation
   d. All of above
5. Chomsky's linguistic computational theory generated a model for syntactic analysis through
   a. regular grammar
   b. regular expression
   c. regular word
   d. none of these`
6. These machines only focus on current scenarios and react on it as per possible best action
   a. Reactive Machines
   b. Limited Memory
   c. Theory of Mind
   d. Self-Awareness

Unit-2 Internet of Things

Content

2.1 Embedded Systems:

Embedded system concepts, purpose of embedded systems, Architecture of embedded systems, embedded processors-PIC, ARM, AVR,ASIC

2.2 IoT: Definition and characteristics of IoT

- Physical design of IoT,
  - Things of IoT,
  - IoT Protocols
- Logical design of IoT,
  - IoT functional blocks,
  - IoT Communication models,
  - IoT Communication APIs,
- IoT Enabling Technologies,
- IoT levels and deployment templates,
- IoT Issues and Challenges, Applications
- IoT Devices and its features: Arduino, Uno, Raspberry Pi, Nodeμ
- Case study on IoT Applications using various Sensors and actuators

2.1 Embedded Systems:

Definition:

An embedded system is a microcontroller or microprocessor based system which is designed to perform a specific task.

OR

An embedded system is a combination of computer hardware and software, either fixed in capability or programmable, designed for a specific function or functions within a larger system.

2.1.1 Embedded system concepts

An embedded system can be defined as a microprocessor or microcontroller-based, software-driven, reliable, real-time control system, designed to perform a specific task. An embedded system may be either an independent system or a part of a large system. Embedded System consists of Input Device, Microcontroller (The Brain) and Output Device. There is a main difference between the embedded system and general purpose system is the computing device like a microprocessor has external peripherals i.e. Real-time Clock, USB, Ethernet, WiFi, Bluetooth, ports etc.) connected to it and are visible outside. But an embedded device contains few or all the peripherals inside the module which is called as SOC (System On Chip).

2.1.2 Purpose of embedded systems:

The embedded system is used in many domain areas such as consumer electronics, home automation, telecommunication, automotive industries, healthcare, control and instrumentation, banking application, military application etc. According to application usage, the embedded system may have the different functionalities. Every embedded system is designed to accomplished the purpose of any one or a combination of following task.

- **Data collection/storage/Representation:** Data is collected from the outside world using various sensors for storage, analysis, manipulation and transmission. The data may be information such as voice, text, image, graphics, video, electrical signals or other measurable quantities. The Collected data may be stored or transmitted to other device or processed by the embedded system for meaningful representation.
- **Data communication in embedded system:**The data can be transmitted either through wireless media or wired media. The data can be an analog or digital. The data transmission can be done through wireless media such as Bluetooth, ZigBee, Wi-FI, GPRS, Edge etc or wired media such as RS232C, USB, TCP/IP, PC2, Firewire port, SPI, CAN, I^2C etc.
- **Data processing:**The data which may in the form of Voice, Image, Video, electrical signal or any other measurable quantities is collected by an embedded system and used for various kind of processing depending on the application
- **Monitoring the performance/operation of embedded system:**The embedded systems mostly used for monitoring purpose. For example, ECG (Electro cardiogram) machine is used to monitor the heartbeat of the patient.
- **Control the embedded system:**The embedded system having control functionalities executes control over some variables as per the input variable. The embedded system having control functionalities contains both sensor and actuator. Sensors are connected as input to the ports of the system to capture the change in measuring variable and actuator are connected to output port as a final control element to control the system as per change in input variables within the specified range. For example, air conditioning system at home is used to control the room temperature as per the specified limit.
- **Application specific user's interface:** Most of the embedded system comes with Application specific user's interface such as switches, buttons, display, light, bell, keypad etc. For example, mobile phone comes with user interface such as Keyboard, LCD or LED display, Speaker, vibration alert etc.

2.1.3 Architecture of Embedded System:

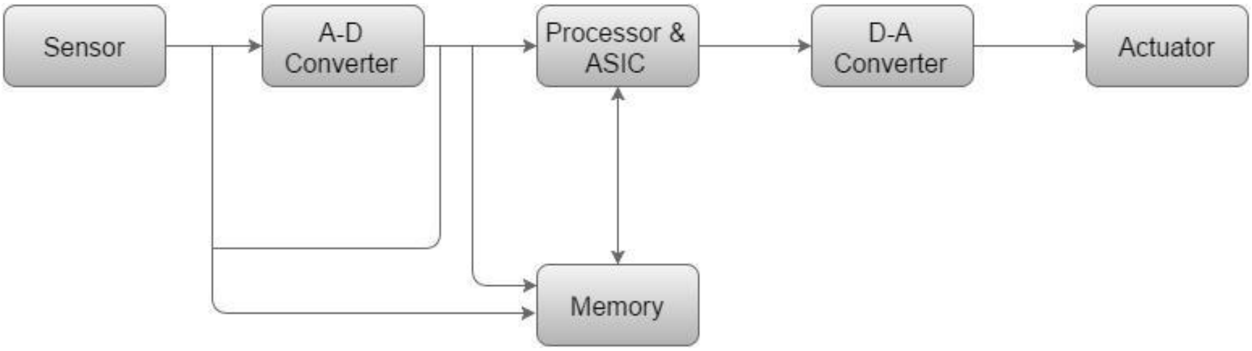


Fig.2.1: Basic Structure of an Embedded System

- **Sensor** – Sensor is used to measure the physical quantity and converts it to an electrical signal which can be read by any electronic device like an A-D converter.
- **A-D Converter** − An analog-to-digital converter converts the analog signal given by the sensor into a digital signal.
- **Processor & ASICs** − Processors process the data to measure the output and store it to the memory.
- **D-A Converter** − A digital-to-analog converter converts the digital data given by the processor to analog data.
- **Actuator** − An actuator compares the output given by the D-A Converter to generates the actual or expected output.

An embedded system has three main components:

- **Embedded system hardware:** An embedded system uses a hardware platform to execute the operation. Hardware of the embedded system consist of Power Supply, Reset, Oscillator Circuit, Memory i.e. Program and data, Processor (Microcontroller, ARM, PIC, ASIC), Timers, Input/Output circuits, Serial communication ports, SASC (System application specific circuits), Interrupt Controller, Parallel ports. Normally, an embedded system includes the following hardware as shown in Fig. 2.2.

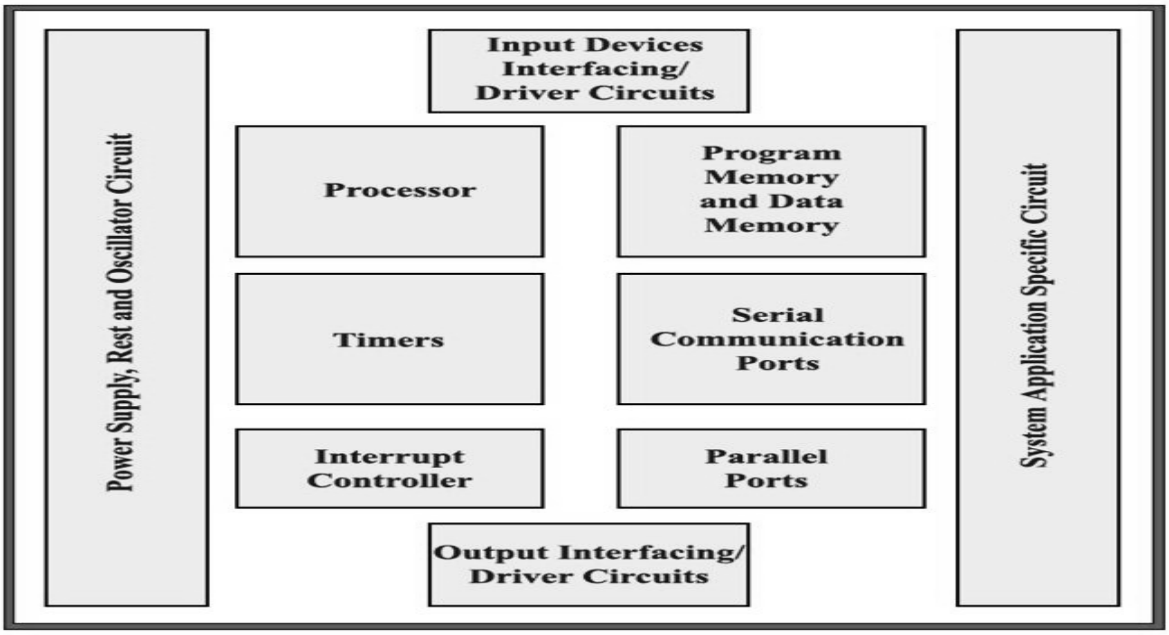

Power Supply, Rest and Oscillator Circuit
Input Devices Interfacing/ Driver Circuits
Processor
Program Memory and Data Memory
Timers
Serial Communication Ports
Interrupt Controller
Parallel Ports
Output Interfacing/ Driver Circuits
System Application Specific Circuit

Fig. 2.2: Embedded System Hardware

- **Embedded system software:** The software of an embedded system is written to execute a particular function. The software used in the embedded system is set of instructions i.e. program. The microprocessors or microcontrollers used in the hardware circuits of embedded systems are programmed to perform specific tasks by following the set of instructions. These programs are mainly written using any programming software like Proteus or Lab-view using any programming languages such as C or C++ or embedded C. Then, the program is stored into the microprocessors or microcontrollers memory that are used in the embedded system circuits.

- **Embedded Operating system:** An embedded operating system (OS) is a dedicated operating system designed to perform a specific task for a device. The main job of an embedded operating system is to run the code that allows the device to perform its job. The embedded OS also allow the device's hardware accessible to the software that is running on top of the OS. Embedded operating systems are also known as real-time operating systems (RTOS). The most common examples of embedded operating system around us include Windows Mobile/CE (handheld Personal Data Assistants), Symbian (cell phones) and Linux, Palm OS, iOS - Subset of Mac OS X, used in Apple's mobile devices

2.1.4 Embedded processors PIC, ARM, AVR, ASIC

Embedded Processor consists of Control Unit (CU), Execution unit (EU), inbuilt Program and Data Memory, Timer, Interrupts, Serial communication port, Parallel ports, Input and Output Driver Circuits, Power supply, Reset and Oscillator Circuits, System Application Specific Circuits such as ADC, DAC etc.

(a) PIC (Programmable/Peripheral Interface Controllers)

PIC microcontrollers are the smallest microcontrollers which can be programmed to perform a large range of tasks. PIC microcontrollers are used in many electronic devices such as phones, computer control systems, alarm systems, embedded systems, etc PIC microcontroller architecture consists of RAM, ROM, CPU, timers, counters, A/D converter, Ports, Flash memory, general purpose register (GPR), special purpose register (SPR), Stack, Interrupt and supports the protocols such as SPI, CAN, and UART for interfacing with other peripherals.

Features of PIC

- RISC (reduced instruction set computer) architecture.
- On chip program ROM in the form of flash memory.
- On Chip RAM (random access memory)
- On Chip Data EEPROM
- Include Timers.
- Include ADC (Analog to Digital converter).
- Include USART protocol for PC communication.
- Contains I/O ports and I/O port register are bit accessible and port accessible both.
- Include CAN, SPI and I2C PROTOCOL for serial communication.
- Support n-stage pipelining
- Provide interrupts

Application of PIC:

1. **Motor Control, Digital Power & Lighting**
   - Motor Control
   - Digital Power
   - Lighting
   - Automotive
   - Home Appliance
   - High Temperature for 150C

2. **Human Interface**
   - Graphics Solutions
   - Segmented LCD
   - Touch Sensing Solutions
   - Audio and Speech
3. **Connectivity**
   - Wireless
   - USB
   - Ethernet
   - CAN

(b) AVR (Alf-EgilBogenVegardWollan RISC microcontroller or Advanced Virtual RISC)

AVR was developed in the year 1996 by Atmel Corporation and the architecture of AVR was designerd by Alf-EgilBogen and VegardWollan. AVR and stands for Alf-EgilBogenVegardWollanRISC microcontroller, also known as Advanced Virtual RISC. AVR microcontroller executes most of the instructions in single execution cycle. AVRs are about four times faster than PICs and consumes less power. AVRs can be operated in different power saving modes.

Features of AVR

AVRs provides a wide range of features:

- Internal, self-programmable instruction flash memory up to 256 KB
- In-system programmable (ISP) using serial/parallel low-voltage proprietary interfaces andOn-chip debugging support through JTAG
- Internal data EEPROM up to 4 KB and SRAM up to 16 KB
- External 64 KB little endian data space in some models of AVR
- 8-bit and 16-bit timers
- PWM output, Analog comparator
- 10 or 12-bit A/D converters, with multiplex of up to 16 channels
- 12-bit D/A converters
- Synchronous/asynchronous serial peripherals (UART/USART), Serial Peripheral Interface Bus (SPI), I^2C
- Multiple power-saving sleep modes
- Lighting and motor control (PWM) controller models
- CAN, USB. Ethernet, LCD, DMA controller support
- Low-operating voltage devices i.e.1.8 V

Applications of AVR

- Signal sensing and Data acquisition
- Motion control and Interface motors
- Displays on LCD
- Interface any type of sensors and transducers
- Interface GSM and GPS

- Control and automation of industrial plants, mechanical & electrical systems
- Automation of heavy machineries
- Developments for UAVs (Unmanned Aerial Vehicles)
- Light sensing,Temperature sensing & controlling devices
- Fire detection & safety devices
- Industrial instrumentation devices
- Process control devices

(c) ARM microcontroller

The ARM (Advanced RISC machine) is a 32-bit Reduced Instructions Set Computer (RISC) microcontroller and introduced by the Acron computers' organization in 1987.The ARM architecture uses a 'Harvard architecture' which support separate data and instruction buses for communicating with the ROM and RAM memories.The ARM microcontrollers support for both low-level and high-level programming languages.

Features of ARM microcontroller

- Load/store RISC architecture.
- An ARM and Thumb instruction sets i.e. 32-bit instructions can be freely intermixed with 16-bit instructions in a program.
- Efficient multi-core processing and easier coding for developers.
- Support multi-processing
- Enhanced power-saving design.
- 64 and 32-bit execution states for scalable high performance.
- Supports Memory Management Unit (MMU) and the Memory Protection Unit (MPU).
- Support for Digital Signal Processing (DSP) algorithms.
- Smaller size, reduced complexity and lower power consumption.
- Floating-point support

Applications of ARM microcontroller

- Smartphones
- Multimedia players
- 3dshandheld game consoles
- Digital cameras
- Tablet computers
- Industrial instrument control systems
- Wireless networking and sensors
- Automotive body system
- Robotics
- Consumer electronics
- Set-top boxes
- Digital television
- Smart watches
- Wireless lan, 802.11, Bluetooth

(d) ASIC (Application-specific integrated circuit)

An ASIC (application-specific integrated circuit) is a microchip designed for a special application, such as a particular kind of transmission protocol or a hand-held computer. You might contrast it with general integrated circuits, such as the microprocessor and the random access memory chips in your PC. ASICs are used in a wide-range of applications, including auto emission control, environmental monitoring, and personal digital assistants (PDAs). An ASIC can be pre-manufactured for a special application or it can be custom manufactured (typically using components from a "building block" library of components) for a particular customer application.

The advantages of ASIC include the following.

- The small size of ASIC makes it a high choice for sophisticated larger systems.
- As a large number of circuits built over a single chip, this causes high-speed applications.
- ASIC has low power consumption.
- As they are the system on the chip, circuits are present side by side. So, very minimal routing is needed to connect various circuits.
- ASIC has no timing issues and post-production configuration.

The disadvantages of ASIC include the following.

- As these are customized chips they provide low flexibility for programming.
- As these chips have to be designed from the root level they are of high cost per unit.
- ASIC have larger time to market margin.

2.2 IoT Definition:

- The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices.
- Internet of Things (IoT) refers to physical and virtual objects that have unique identities and are connected to the internet to facilitate intelligent applications that make energy, logistics, industrial control, retail, agriculture and many other domains "smarter".
- Internet of things (IoT) is a new revolution in which endpoints connected to the internet and driven by the advancements in sensor networks, mobile devices, wireless communications, networking and cloud technologies.

Characteristics of IoT:

- **Dynamic &Self-Adapting:**IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context, or sensed environment.For example, the surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether it is day or night.
- **Self-Configuring:**IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring).

- **Interoperable Communication Protocols:**IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.
- **Unique Identity:** Each IoT device has a unique identity and a unique identifier (such as an IP address or a URI). IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and managementinfrastructure.
- **Integrated into Information Network:** IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.
- **Enormous scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet.

Features of IoT:

- **Connectivity:** Connectivity refers to establish a proper connection between all the things of IoT to IoT platform it may be server or cloud.
- **Analyzing:** After connecting all the relevant things, it comes to real-time analyzing the data collected and use them to build effective business intelligence.
- **Integrating:** IoT integrating the various models to improve the user experience as well.
- **Artificial Intelligence:** IoT makes things smart and enhances life through the use of data.
- **Sensing:** The sensor devices used in IoT technologies detect and measure any change in the environment and report on their status.
- **Active Engagement:** IoT makes the connected technology, product, or services to active engagement between each other.
- **Endpoint Management:** It is important to be the endpoint management of all the IoT system otherwise; it makes the complete failure of the system.

Advantages and Disadvantages ofIoT:

Advantages of IoT

- **Efficient resource utilization:** If we know the functionality and the way that how each device work we definitely increase the efficient resource utilization as well as monitor natural resources.
- **Minimize human effort:** As the devices of IoT interact and communicate with each other and do lot of task for us, then they minimize the human effort.
- **Save time:** As it reduces the human effort then it definitely saves out time. Time is the primary factor which can save through IoT platform.
- **Improve security:** Now, if we have a system that all these things are interconnected then we can make the system more secure and efficient.

- **Reduced Waste**: IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- **Enhanced Data Collection**: Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

Disadvantages of IoT

- **Security:** As the IoT systems are interconnected and communicate over networks. The system offers little control despite any security measures, and it can be lead the various kinds of network attacks.
- **Privacy**: Even without the active participation on the user, the IoT system provides substantial personal data in maximum detail.
- **Complexity:** The designing, developing, and maintaining and enabling the large technology to IoT system is quite complicated.
- **Flexibility:** Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- **Compliance**: IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

2.2.1 Physical design of IoT:

➢ **Things of IoT:**

- The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.
- IoT devices can exchange data with other connected devices and applications (directly or indirectly), or collect data from other devices and process the data either locally or send the data to centralized servers or cloud-based application back-ends for processing the data, or perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints (i.e., memory, processing capabilities, communication latencies and speeds, and deadlines).

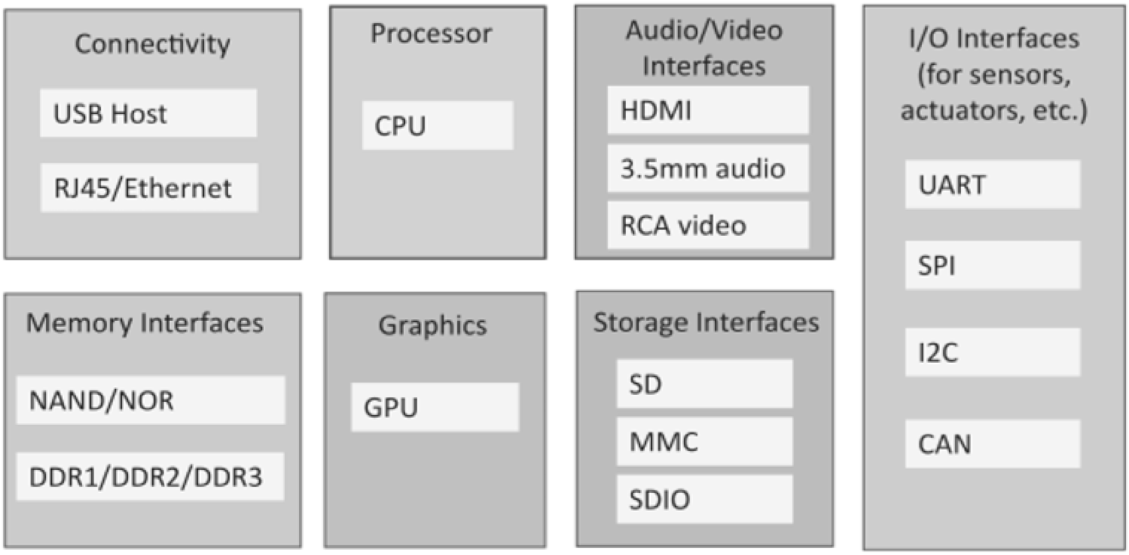


Fig2.3 Generic Bock Diagram of an IoT Device

- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless. These include (i) I/O interfaces for sensors, (ii) interfaces for Internet connectivity, (iii) memory and storage interfaces and (iv) audio/video interfaces.
- An IoT device can collect various types of data from the on-board or attached sensors, such as temperature, humidity, light intensity. The sensed data can be communicated either to other devices or cloud-based servers/storage.
- IoT devices can be connected to actuators that allow them to interact with other physical entities (including non-IoT devices and systems) in the vicinity of the device. For example, a relay switch connected to an IoT device can turn an appliance on/off based on the commands sent to the IoT device over the Internet.
- IoT devices can also be of varied types, for instance, wearable sensors, smart watches, LED lights, automobiles and industrial machines.
- Almost all IoT devices generate data in some form or the other which when processed by data analytics systems leads to useful information to guide further actions locally or remotely.
- For instance, sensor data generated by a soil moisture monitoring device in a garden, when processed can help in determining the optimum watering schedules.
- Following Figure shows different types of IoT devices.

- **IoT Protocols**

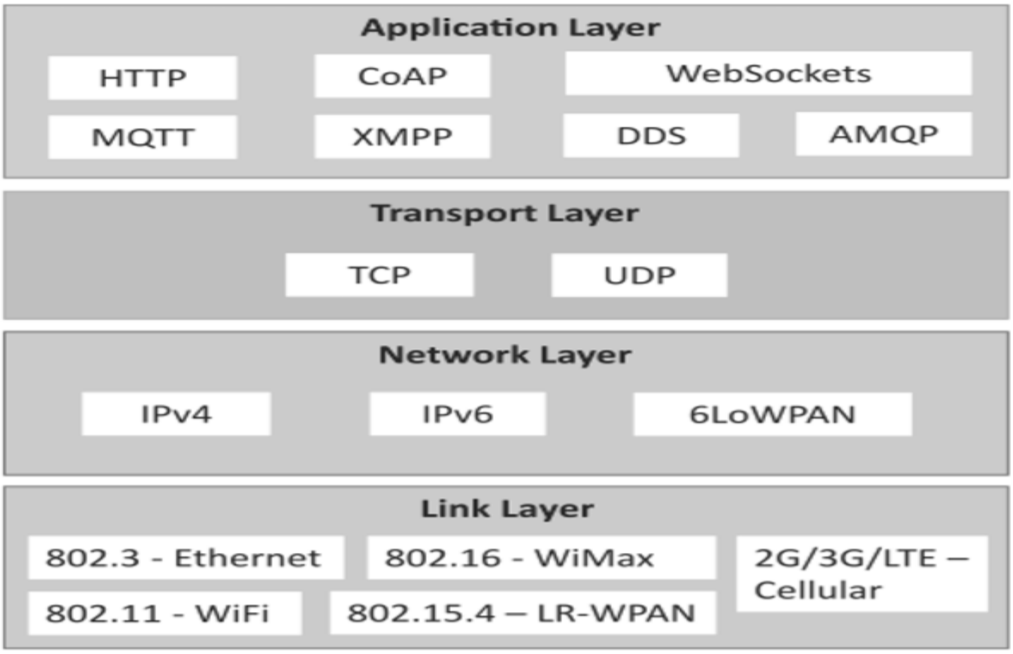


Fig. 2.4IoT Protocols

Link Layer Protocols:

- Link layer protocols determine how the data is physically sent over the network's physical layer or medium (e.g., copper wire, coaxial cable, or a radio wave).
- Link layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (such as a coaxial cable).

802.3-Ethernet: IEEE 802.3 is a collection of wired Ethernet standards for the link layer. For example, 802.3 is the standard for 10BASE5 Ethernet that uses coaxial cable as a shared medium, 802.3.i is the standard for 10BASE-T Ethernet over copper twisted-pair connections, 802.3.j is the standard for 10BASE-F Ethernet over fiber optic connections, 802.3ae is the standard for 10 Gbit/s Ethernet over fiber, and so on.

802.11- WiFi: IEEE 802.11 is a collection of wireless local area network (WLAN) communication standards, including extensive description of the link layer. 802.11a operates in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60 GHz band. These standards provide data rates from 1 Mb/s to upto 6.75 Gb/s.

802.16-WiMax: IEEE 802.16 is a collection of wireless broadband standards, including extensive descriptions for the link layer (also called WiMax). WiMaxstandards provide data rates from 1.5 Mb/s to 1 Gb/s. The recent update (802.16m) provides data rates of 100 Mbit/s for mobile stations and 1 Gbit/s for fixed stations.

802.15.4-LR-WPAN: IEEE 802.15.4 is a collection of standards for low-rate wireless personal area networks (LR-WPANs). These standards form the basis of specifications for high level communication protocols such as ZigBee. LR-WPAN standards provide data rates from 40 Kb/s 250 Kb/s. These standards provide low-cost and low-speed communication for power constrained devices.

2G/3G/4G - Mobile Communication: There are different generations of mobilecommunication standards including second generation (2G including GSM and CDMA), third generation (3G - including UMTS and CDMA2000) and fourth generation (4G - including LTE). IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/s (for 2G) to upto 100 Mb/s (for 4G) and are available from the 3GPP websites.

Network/Internet Layer Protocols:

The network layers are responsible for sending of IP datagrams from the source network to the destination network. This layer performs the host addressing and packet routing. The datagrams contain the source and destination addresses which are used to route them from the source to destination across multiple networks. Host identification is done using hierarchical IP addressing schemes such as IPv4 or IPv6.

IPv4: Internet Protocol version 4 (IPv4) is the most deployed Internet protocol that is used to identify the devices on a network using a hierarchical addressing scheme. IPv4 uses a 32-bit address scheme that allows total of 232 or 4,294,967,296 addresses. IPv4 has been succeeded by IPv6. The IP protocols establish connections on packet networks, but do not guarantee delivery of packets. Guaranteed delivery and data integrity are handled by the upper layer protocols (such as TCP).

IPv6: Internet Protocol version 6 (IPv6) is the newest version of Internet protocol and successor to IPv4, IPv6 uses 128-bit address scheme that allows total of 2128 or 3.4 x 1038 addresses.

6LOWPAN: 6LOWPAN (IPv6 over Low power Wireless Personal Area Networks) brings IP protocol to the low-power devices which have limited processing capability. 6LOWPAN operates in the 2.4 GHz frequency range and provides data transfer rates of 250 Kb/s. 6LOWPAN works with the 802.15.4 link layer protocol and defines compression mechanisms for IPv6 datagrams over IEEE 802.15.4-based networks.

Transport Layer Protocols:

The Transport layer protocols provide end-to-end message transfer capability independent of the underlying network. The message transfer capability can be set up on connections, either using handshakes (as in TCP) or without handshakes/acknowledgements (as in UDP). The transport layer provides functions such as error control, segmentation, flow control and congestion control.

TCP: Transmission Control Protocol (TCP) is the most widely used transport layer protocol, that is used by web browsers (along with HTTP, HTTPS application layer protocols), email programs (SMTP application layer protocol) and file transfer (FTP). TCP is a connection oriented and stateful protocol. TCP ensures reliable transmission of packets in-order and also provides error detection capability so that duplicate packets can be discarded and lost packets are retransmitted.

UDP: UDP is a connectionless protocol. UDP is useful for time-sensitive applications that have very small data units to exchange and do not want the overhead of connection setup. UDP is a transaction oriented and stateless protocol. UDP does not provide guaranteed delivery, ordering of messages and duplicate elimination. Higher levels of protocols can ensure reliable delivery or ensuring connections created are reliable.

Application Layer Protocols:

Application layer protocols define how the applications interface with the lower layer protocols to send the data over the network. The application data, typically in files, is encoded by the application layer protocol and encapsulated in the transport layer protocol which provides connection or transaction oriented communication over the network. Port numbers are used for application addressing (for example port 80 for HTTP, port 22 for SSH, etc.). Application layer protocols enable process-to-process connections using ports.

HTTP: Hypertext Transfer Protocol (HTTP) is the application layer protocol that forms the foundation of the World Wide Web (WWW). HTTP includes commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS, etc. The protocol follows a request-response model where a client sends requests to a server using the HTTP commands. HTTP is a stateless protocol and each HTTP request is independent of the other requests. An HTTP client can be a browser or an application running on the client (e.g., an application running on an IoT device, a mobile application or other software). HTTP protocol uses Universal Resource Identifiers (URIs) to identify HTTP resources.

COAP: Constrained Application Protocol (CoAP) is an application layer protocol for machine-to-machine (M2M) applications, meant for constrained environments with constrained devices and constrained networks. Like HTTP, COAP is a web transfer protocol and uses a request-response model, however it runs on top of UDP instead of TCP. COAP uses a client-server architecture where clients communicate with servers using connectionless datagrams. COAP is designed to easily interface with HTTP. Like HTTP, COAP supports methods such as GET, PUT, POST, and DELETE. COAP draft specifications are available on IEFT Constrained environments (CORE) Working Group website.

WebSocket: WebSocket protocol allows full-duplex communication over a single socket connection for sending messages between client and server. WebSocket is based on TCP and allows streams of messages to be sent back and forth between the client and server while keeping the TCP connection open. The client can be a browser, a mobile application or an IoT device.

MQTT: Message Queue Telemetry Transport (MQTT) is a light-weight messaging protocol based on the publish-subscribe model. MQTT uses a client-server architecture where the client (such as an IoT device) connects to the server (also called MQTT Broker) and publishes messages to topics on the server. The broker forwards the messages to the clients subscribed to topics. MQTT is well suited for constrained environments where the devices have limited processing and memory resources and the network bandwidth is low.

XMPP: Extensible Messaging and Presence Protocol (XMPP) is a protocol for real-time communication and streaming XML data between network entities. XMPP powers wide range of applications including messaging, presence, data syndication, gaming, multi-party chat and voice/video calls. XMPP allows sending small chunks of XML data from one network entity to another in near real-time. XMPP is a decentralized protocol and uses a client-server architecture. XMPP supports both client-to-server and server-to-server communication paths. In the context of IoT, XMPP allows real-time communication between IoT devices.

DDS: Data Distribution Service (DDS) is a data-centric middleware standard for device-to-device or machine-to-machine communication. DDS uses a publish-subscribe model where publishers (e.g. devices that generate data) create topics to which subscribers (e.g., devices that want to consume data) can subscribe. Publisher is an object responsible for data distribution and the subscriber is responsible for receiving published data. DDS provides quality-of-service (QoS) control and configurable reliability.

AMOP: Advanced Message Queuing Protocol (AMQP) is an open application layer protocol for business messaging. AMQP supports both point-to-point and publisher/subscriber models, routing and queuing. AMQP brokers receive messages from publishers (e.g., devices or applications that generate data) and route them over connections to consumers (applications that process data). Publishers publish the messages to exchanges which then distribute message copies to queues. Messages are either delivered by the broker to the consumers which have subscribed to the queues or the consumers can pull the messages from the queues.

2.2.2 Logical design of IoT:

Logical design of an IoT system refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.

IoT functional blocks:

An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication, and management

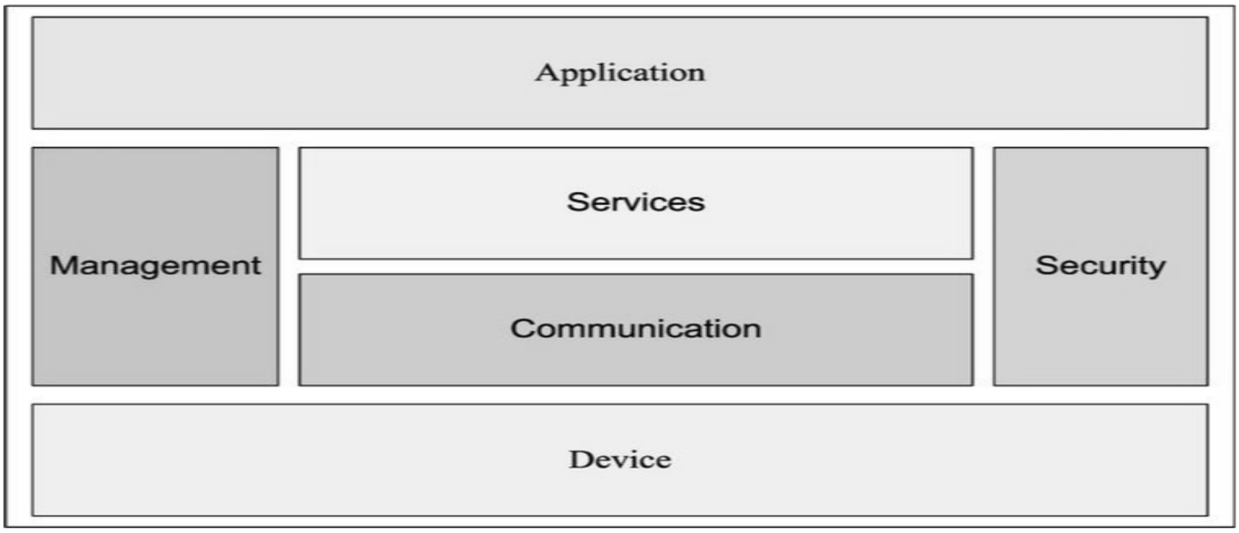


Fig. 2.5Fundamental block of IoT

- **Device:** An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.
- **Communication:** The communication block handles the communication for the IoT system.
- **Services:** An IoT system uses various types of IoT services such as services for device monitoring, device control services, data publishing services and services for device discovery.
- **Management:** Management functional block provides various functions to govern the IoT system.
- **Security:** Security functional block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and data security.
- **Application:** IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view or analyze the processed data.

IoT Communication models:

Request-Response: Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests. When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client. Request-Response model is a stateless communication model and each request-response pair is independent of others.

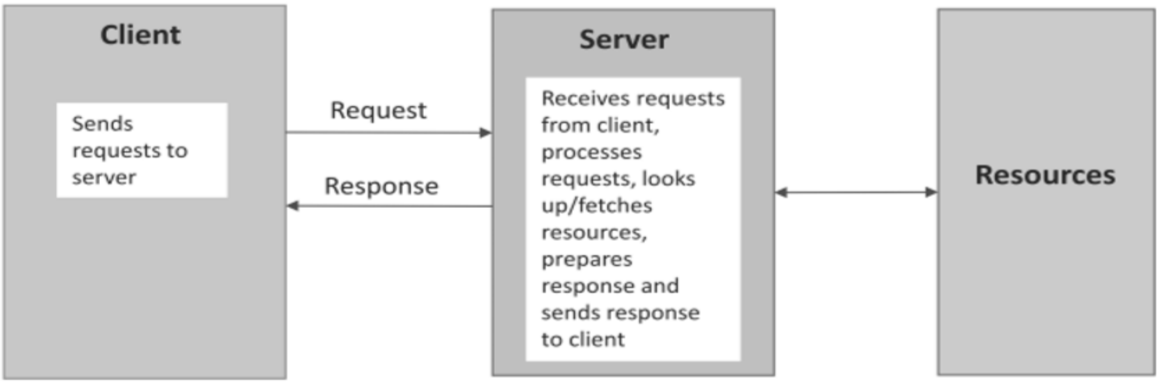

Client
Sends requests to server
Request
Response
Server
Receives requests from client, processes requests, looks up/fetches resources, prepares response and sends response to client
Resources

Fig.2.6Request-Response communication model

Publish-Subscribe: Publish-Subscribe is a communication model that involves publishers, brokers and consumers. Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers. Consumers subscribe to the topics which are managed by the broker. When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.

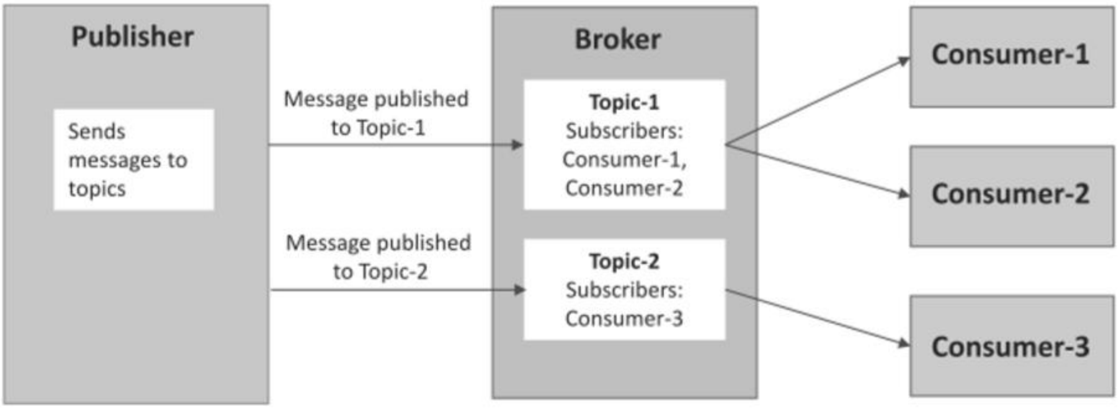


Fig.2.7Publish-Subscribe communication model

Push-Pull: Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumers. Queues help in decoupling the messaging between the producers and consumers. Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate rate at which the consumers pull data.

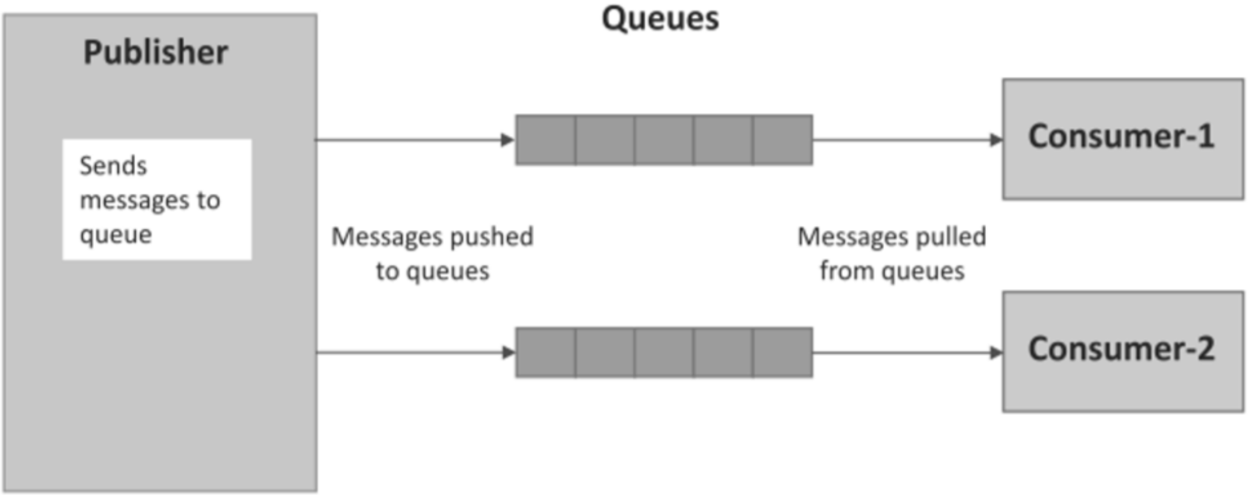


Fig. 2.8Push-Pull communication model

Exclusive Pair: Exclusive Pair is a bi-directional, fully duplex communication model that uses a persistent connection between the client and server. Once the connection is setup it remains open until the client sends a request to close the connection. Client and server can send messages to each other after connection setup. Exclusive pair is a stateful communication model and the server is aware of all the open connections.

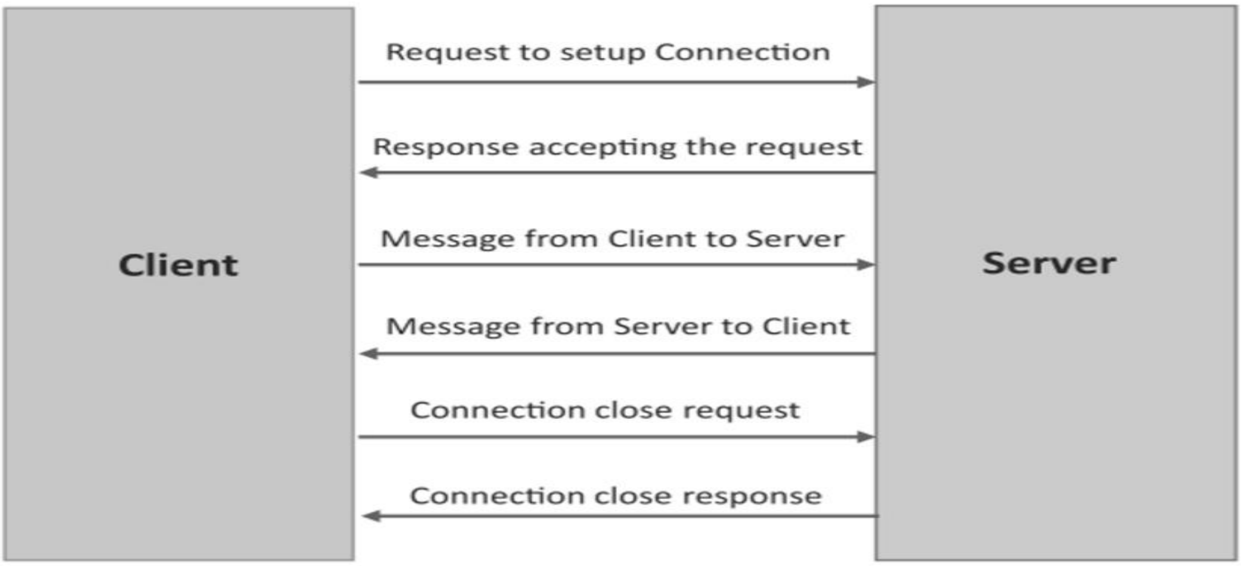

Client
Request to setup Connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection close response
Server

Fig.2.9 Exclusive Pair communication model

IoT Communication APIs:

REST-based Communication APIs

REST is acronym for **RE**presentational **S**tate **T**ransfer. It is architectural style for distributed hypermedia systems. It is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.The REST architectural constraints are as follows:

- **Client–server** – By separating the user interface concerns from the data storage concerns, we improve the portability of the user interface across multiple platforms and improve scalability by simplifying the server components.
- **Stateless** – Each request from client to server must contain all of the information necessary to understand the request, and cannot take advantage of any stored context on the server. Session state is therefore kept entirely on the client.
- **Cacheable** – Cache constraints require that the data within a response to a request be implicitly or explicitly labeled as cacheable or non-cacheable. If a response is cacheable, then a client cache is given the right to reuse that response data for later, equivalent requests.
- **Uniform interface** – By applying the software engineering principle of generality to the component interface, the overall system architecture is simplified and the visibility of interactions is improved. In order to obtain a uniform interface, multiple architectural constraints are needed to guide the behavior of components. REST is defined by four interface constraints: identification of resources; manipulation of resources through representations; self-descriptive messages; and, hypermedia as the engine of application state.
- **Layered system** – The layered system style allows an architecture to be composed of hierarchical layers by constraining component behavior such that each component cannot “see” beyond the immediate layer with which they are interacting.

- **Code on demand (optional)** – REST allows client functionality to be extended by downloading and executing code in the form of applets or scripts. This simplifies clients by reducing the number of features required to be pre-implemented.

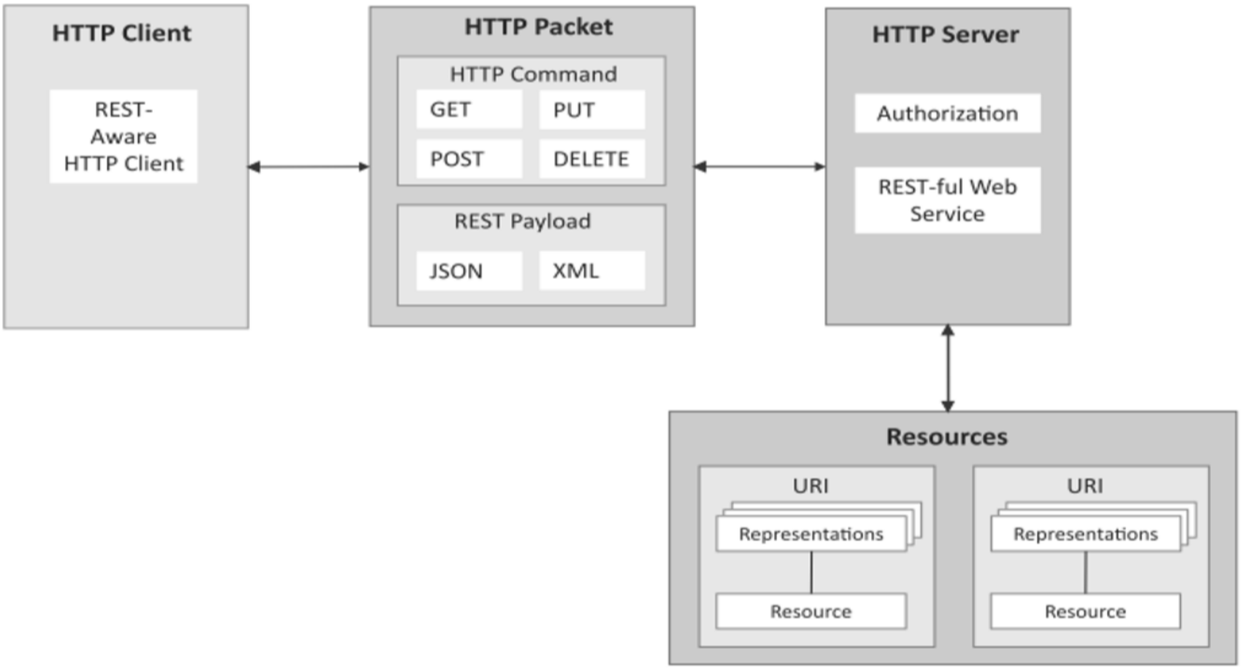


Fig.2.10 Communication with REST APIs

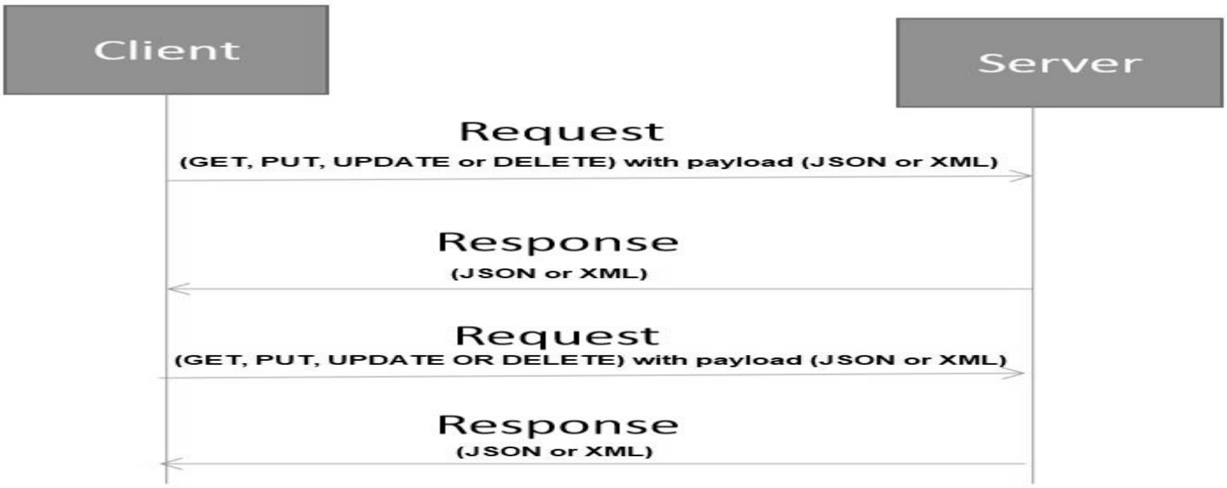

Client
Server
Request
(GET, PUT, UPDATE or DELETE) with payload (JSON or XML)
Response
(JSON or XML)
Request
(GET, PUT, UPDATE OR DELETE) with payload (JSON or XML)
Response
(JSON or XML)

Fig. 2.11Request-Response Model used by REST

A RESTful web service is a "web API" implemented using HTTP and REST principles.

HTTP Method	Resource Type	Action	Example
GET	Collection URI	List all the resources in a collection	http://example.com/api/ tasks/(list all tasks)
GET	Element URI	Get information about a resource	http://example.com/api/ tasks/1/(get information on task-1)
POST	Collection URI	Create a new	http://example.com/api/

		resource	tasks/(create a new task from data provided in the request)
POST	Element URI	Generally not used	
PUT	Collection URI	Replace the entire collection with another collection	http://example.com/api/ tasks/(replace entire collection with data provided in the request)
PUT	Element URI	Update a resource	http://example.com/api/ tasks/1/(update task-1 with data provided in the request)
DELETE	Collection URI	Delete the entire collection	http://example.com/api/ tasks/(delete all tasks)
DELETE	Element URI	Delete a resource	http://example.com/api/ tasks/1/(delete task-1)

Table 2.1: HTTP request methods and actions

WebSocket-based Communication APIs:

WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follow the exclusive pair communication model described in previous section and as shown in Figure.

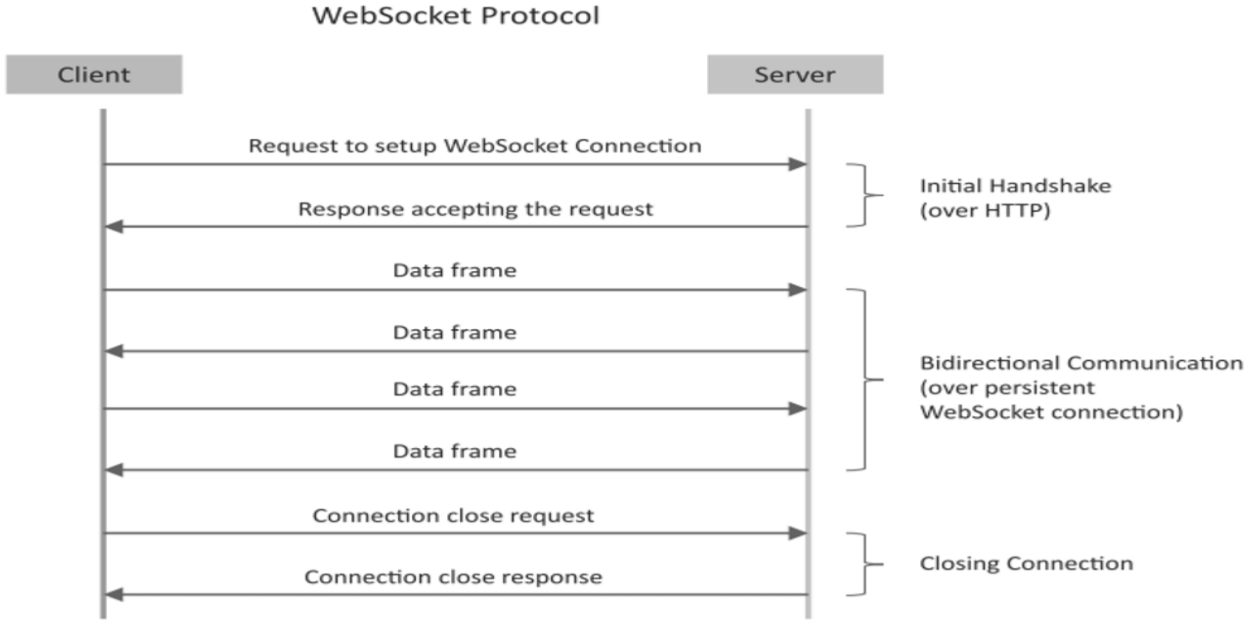

WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake (over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication (over persistent WebSocket connection)
Connection close request
Connection close response
Closing Connection

Fig.2.12Exclusive pair model used by WebSocket APIs

Unlike request-response APIs such as REST, the WebSocket APIs allow full duplex communication and do not require a new connection to be setup for each message to be sent. WebSocket communication begins with a connection setup request sent by the client to the server. This request (called a WebSocket handshake) is sent over HTTP and the server interprets it as an upgrade request. If the server supports WebSocket protocol, the server responds to the WebSocket handshake response. After the connection is setup, the client and server can send data/messages to each other in full-duplex mode. WebSocket APIs reduce the network traffic and latency as there is no overhead for connection setup and termination requests for each message. WebSocket is suitable for IoT applications that have low latency or high throughput requirements.

2.2.3 IoT Enabling Technologies:

IoT is enabled by several technologies including wireless sensor networks, cloud computing, big data analytics, embedded systems, security protocols and architectures, communication protocols, web services, mobile internet and semantic search engines. Following are some technologies which play a key role in IoT.

Wireless Sensor Networks: A Wireless Sensor Network (WSN) comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. AWSN consist of a number of end-nodes and routers and a coordinator. End nodes have several sensors attached them. End nodes can also act as routers. Routers are responsible for routing the data packets from end-nodes to the coordinator. The coordinator collects the data from all the nodes. Coordinator also acts as a gateway that connects the WSN to the Internet. Some examples of WSNs used in IoT systems are described as follows:

- Weather monitoring systems
- Indoor air quality monitoring systems.
- Soil moisture monitoring systems
- Surveillance systems
- Smart grids
- Structural health monitoring systems

ZigBee is one of the most popular wireless technologies used by WSNs. ZigBee specifications are based on IEEE 802.15.4. ZigBee operates at 2.4 GHz frequency and offers data rates upto 250 KB/s and range from 10 to 100 meters depending on the power output and environmental conditions.

Cloud Computing:

Cloud computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud computing services are offered to user in different forms:

- **Infrastructure-as-a-Service (IaaS):**IaaS provides the users the ability to provision computing and storage resources. These resources are provided to the users as virtual machine instances and virtual storage. Users can start, stop, configure and manage the virtual machine instances and virtual storage. Users can deploy operating systems and applications of their choice on the virtual resources provisioned in the cloud. The cloud service provider manages the underlying infrastructure. Virtual resources provisioned by the users are billed based on a pay-per-use paradigm. Some examples of the wide usage of IaaS are automated, policy-driven operations such as backup, recovery, monitoring, clustering, internal networking, website hosting, etc. The service provider is responsible for building the servers and storage, networking firewalls/ security, and the physical data center. Some key players offering IaaS are Amazon

EC2, Microsoft Azure, Google Cloud Platform, GoGrid, Rackspace, DigitalOcean among others.

- **Platform-as-a-Service (PaaS):** PaaS provides the users the ability to develop and deploy application in the cloud using the development tools, application programming interfaces (APIs), software libraries and services provided by the cloud service provider. The cloud service provider manages the underlying cloud infrastructure including servers, network, operating systems and storage. The users, themselves, are responsible for developing, deploying, configuring and managing applications on the cloud infrastructure. The PaaS environment enables cloud users (accessing them via a webpage) to install and host data sets, development tools and business analytics applications, apart from building and maintaining necessary hardware. Some key players offering PaaS are Bluemix, CloudBees, Salesforce.com, Google App Engine, Heroku, AWS, Microsoft Azure, OpenShift, Oracle Cloud, SAP and OpenShift.

- **Software-as-a-Service (SaaS):**SaaS provides the users a complete software application or the user interface to the application itself. The cloud service provider manages the underlying cloud infrastructure including servers, network, operating systems, storage and application software, and the user is unaware of the underlying architecture of the cloud. Applications are provided to the user through a thin client interface (e.g., a browser). SaaS applications are platform independent and can be accessed from various client devices such as workstations, laptop, tablets and smart-phones, running different operating systems. Since the cloud service provider manages both the application and data, the users are able to access the applications from anywhere.SaaS lets users easily access software applications -- such as emails -- over the internet. Most common examples of SaaS are Microsoft Office 360, AppDynamics, Adobe Creative Cloud, Google G Suite, Zoho, Salesforce, Marketo, Oracle CRM, Pardot Marketing Automation, and SAP Business ByDesign.

Benefits of cloud computing services

- Faster implementation and time to value
- Anywhere access to applications and content
- Rapid scalability to meet demand
- Higher utilization of infrastructure investments
- Lower infrastructure, energy, and facility costs
- Greater IT staff productivity and across organization
- Enhanced security and protection of information assets

Big Data Analytics:

Big Data analytics is the process of collecting, organizing and analyzing large sets of data (called Big Data) to discover patterns and other useful information. Big Data analytics can help organizations to better understand the information contained within the data and will also help identify the data that is most important to the business and future business decisions. Analysts working with Big Data typically want the knowledge that comes from analyzing the data.Big Data Analytics involved several steps starting from data cleansing, data munging (or wrangling), data processing and visualization.

2.2.4 IoT levels and deployment templates:

IoT Level1: System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level1 is Home automation.

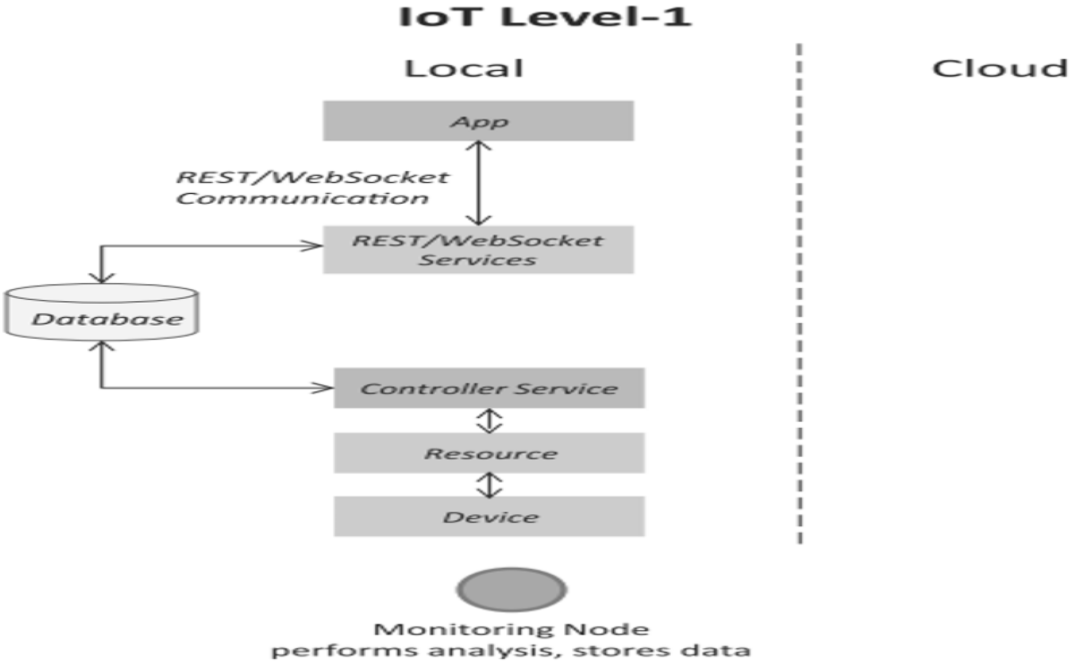


Fig.2.13IoT Level-1

IoT Level2: has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. An e,g., of Level2 IoT system for Smart Irrigation.

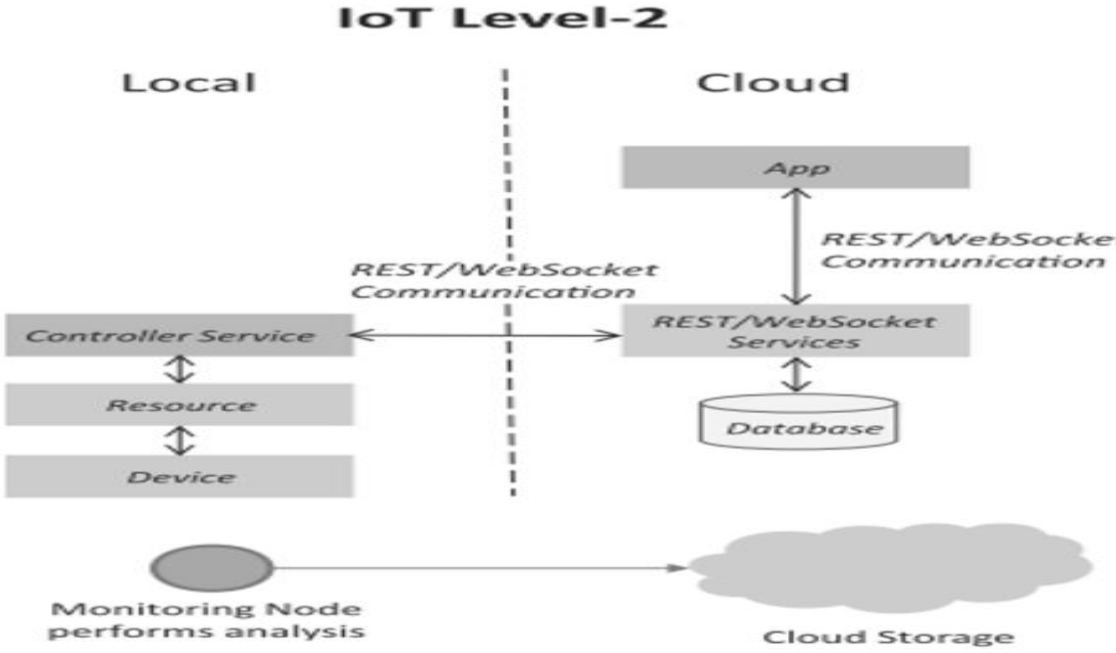


Fig. 2.14IoT Level-2

IoT Level3: system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example of IoT level3 system for tracking package handling.

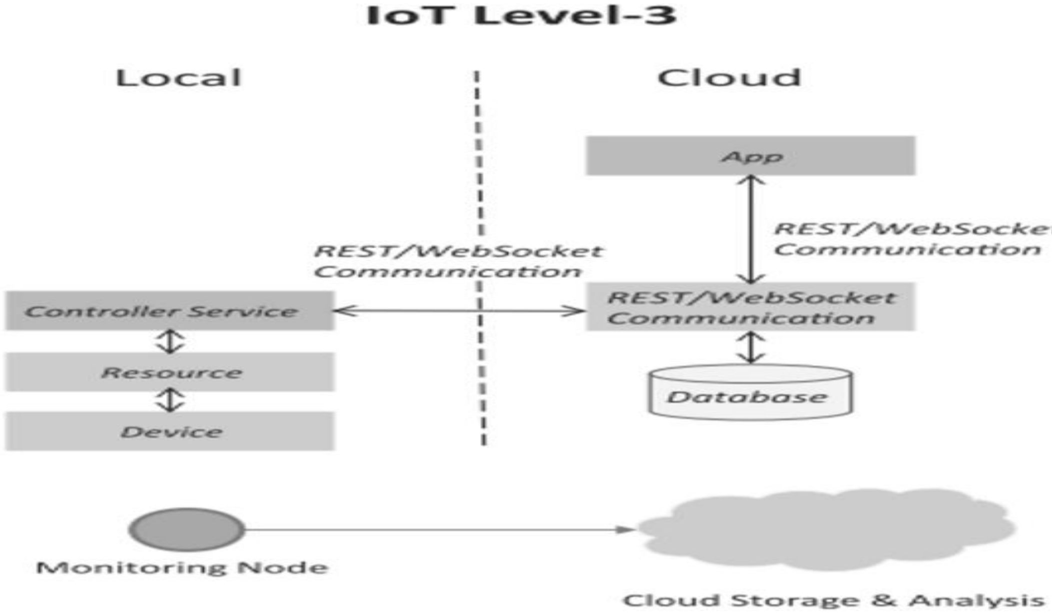


Fig. 2.15IoT Level-3

IoT Level4: System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example of a Level4 IoT system for Noise Monitoring.

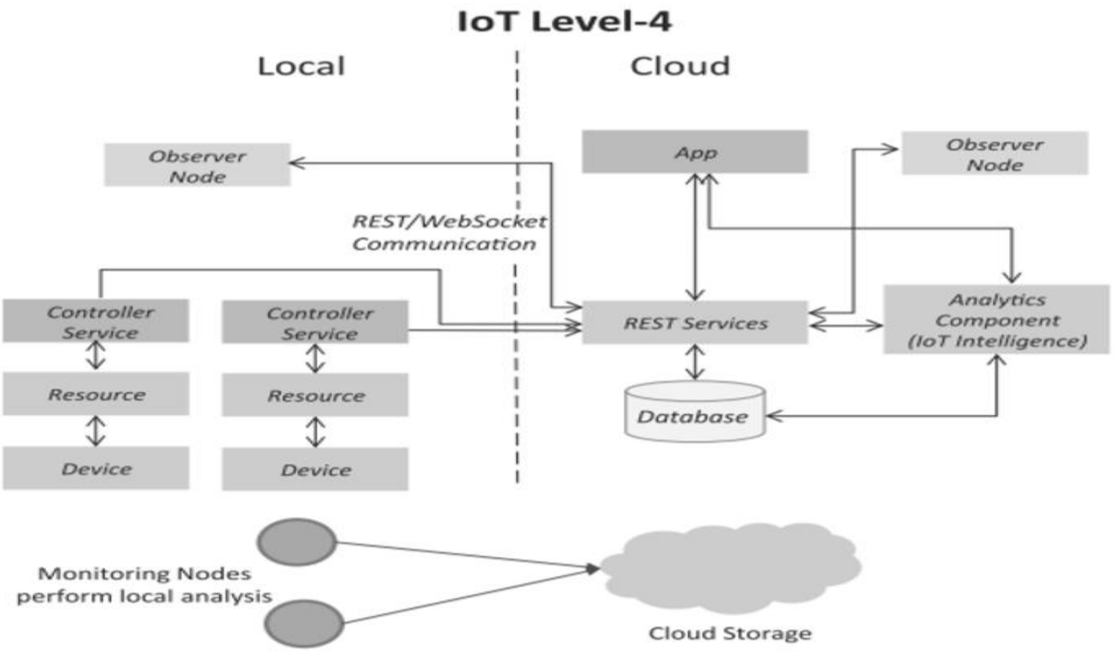


Fig.2.16IoT Level-4

IoT Level5: System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data from the end nodes and sends to the cloud. Data is stored and analyzed in the cloud and application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, in which data involved is big and analysis requirements are computationally intensive. An example of Level5 system for Forest Fire Detection.

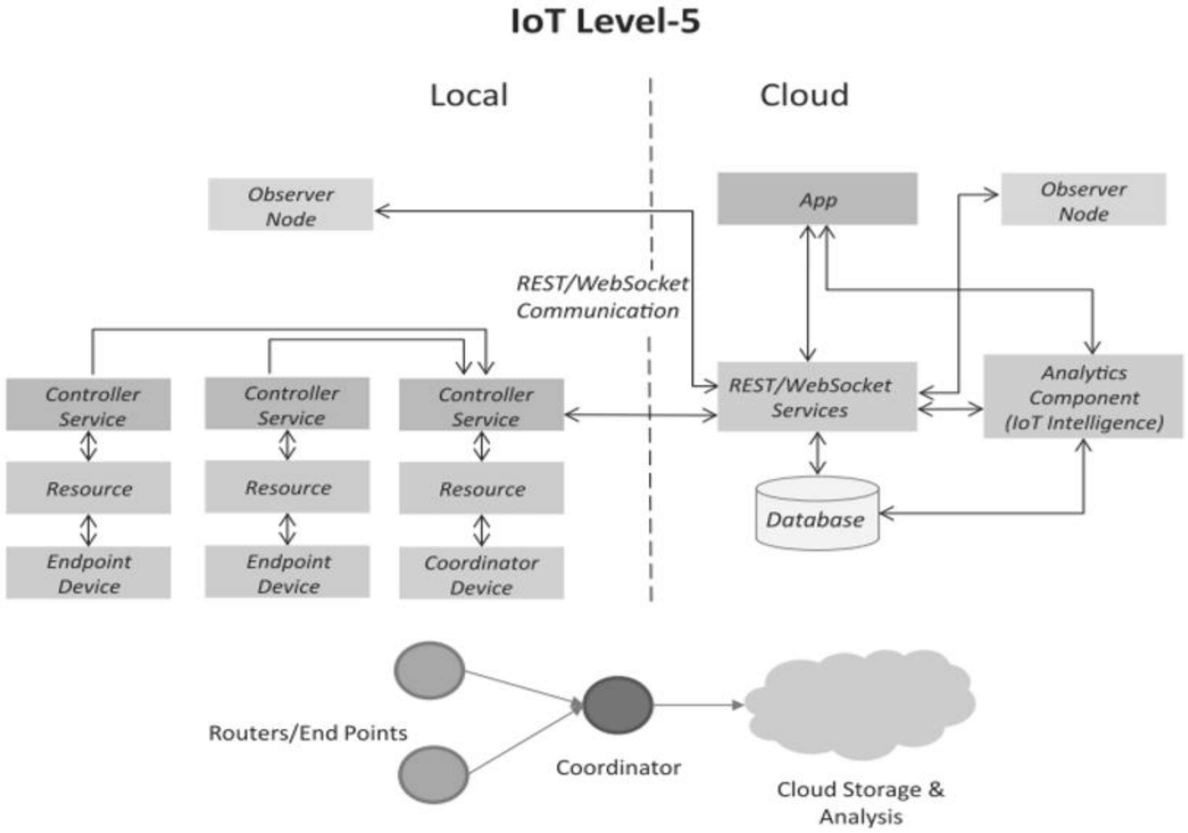


Fig.2.17IoT Level-5

IoT Level6: System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud data base. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends control commands to nodes. An example of a Level6 IoT system for Weather Monitoring System.

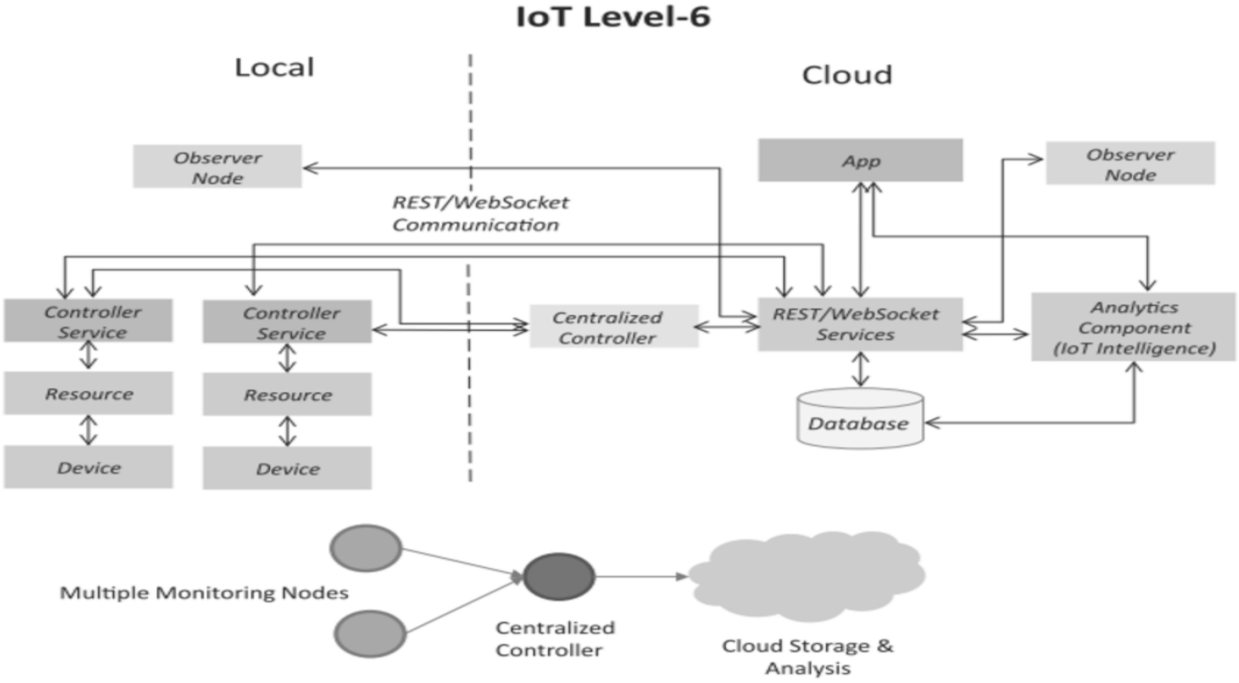


Fig. 2.18IoT Level-6

2.2.5 IoT Issues and Challenges, Applications

Most of Issues and Challenges relevant to IoTare:

- **Data Privacy:** Some manufacturers of smart TVs collect data about their customers to analyze their viewing habits so the data collected by the smart TVs may have a challenge for data privacy during transmission.
- **Data Security:** Data security is also a great challenge. While transmitting data seamlessly, it is important to hide from observing devices on the internet.
- **Insurance Concerns:** The insurance companies installing IoT devices on vehicles collect data about health and driving status in order to take decisions about insurance.
- **Lack of Common Standard:** Since there are many standards for IoT devices and IoT manufacturing industries. Therefore, it is a big challenge to distinguish between permitted and non-permitted devices connected to the internet.
- **Technical Concerns:** Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence there is a need to increase network capacity, therefore, it is also a challenge to store the huge amount of data for analysis and further final storage.
- **Security Attacks and System Vulnerabilities:** There has been a lot of work done in the scenario of IoT security up till now. The related work can be divided into system security, application security, and network security.

- **System Security:** System security mainly focuses onoverallIoT system to identify different security challenges, todesign different security frameworks and to provide propersecurity guidelines in order to maintain the security of anetwork.
- **Application security:** Application Security works forIoT application to handle security issues according to scenariorequirements.
- **Network security:** Network security deals with securingtheIoT communication network for communication ofdifferentIoT devices.

Applications-Domain Specific IoTs

Home Automation:

- **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed.
- **Smart Appliances:** make the management easier and also provide status information to the users remotely.
- **Intrusion Detection:** use security cameras and sensors (PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.
- **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPG etc.,

Cities:

- **Smart Parking:** make the search for parking space easier and convenient for drivers. Smart parking are powered by IoT systems that detect the no. of empty parking slots and send information over internet to smart application back ends.
- **Smart Lighting:** for roads, parks and buildings can help in saving energy.
- **Smart Roads:** Equipped with sensors can provide information on driving condition, travel time estimating and alert in case of poor driving conditions, traffic condition and accidents.
- **Structural Health Monitoring:** uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.
- **Surveillance:** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution.
- **Emergency Response:**IoT systems for fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructures.

Environment:

- **Weather Monitoring:** Systems collect data from a no. of sensors attached and send the data to cloud based applications and storage back ends. The data collected in cloud can then be analyzed and visualized by cloud based applications.

- **Air Pollution Monitoring:** System can monitor emission of harmful gases (CO2, CO, NO, NO2 etc.,) by factories and automobiles using gaseous and meteorological sensors. The collected data can be analyzed to make informed decisions on pollutions control approaches.
- **Noise Pollution Monitoring:** Due to growing urban development, noise levels in cities have increased and even become alarmingly high in some cities. IoT based noise pollution monitoring systems use a no. of noise monitoring systems that are deployed at different places in a city. The data on noise levels from the station is collected on servers or in the cloud. The collected data is then aggregated to generate noise maps.
- **Forest Fire Detection:** Forest fire can cause damage to natural resources, property and human life. Early detection of forest fire can help in minimizing damage.
- **River Flood Detection:** River floods can cause damage to natural and human resources and human life. Early warnings of floods can be given by monitoring the water level and flow rate. IoT based river flood monitoring system uses a no. of sensor nodes that monitor the water level and flow rate sensors.

Retail:

- **Inventory Management:**IoT systems enable remote monitoring of inventory using data collected by RFID readers.
- **Smart Payments:** Solutions such as contact-less payments powered by technologies such as Near Field Communication(NFC) and Bluetooth.
- **Smart Vending Machines:** Sensors in a smart vending machines monitors its operations and send the data to cloud which can be used for predictive maintenance.

Logistics:

- **Route generation &scheduling:**IoT based system backed by cloud can provide first response to the route generation queries and can be scaled upto serve a large transportation network.
- **Fleet Tracking:** Use GPS to track locations of vehicles in real-time.
- **Shipment Monitoring:**IoT based shipment monitoring systems use sensors such as temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect food spoilage.
- **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting data on Vehicle operation’s (speed, RPMetc.,) and status of various vehicle sub systems.

Agriculture:

- **Smart Irrigation:** to detemine moisture amount in soil.
- **Green House Control:** to improve productivity.

Industry:

- Machine diagnosis and prognosis
- Indoor Air Quality Monitoring

Health and Life Style:

- Health & Fitness Monitoring
- Wearable Electronics

2.2.6 IoT Devices and its features: Arduino, Uno, Raspberry Pi, Nodeµ

IoT Devices:

- Internet of Things Devices is non-standard devices that connect wirelessly to a network with each other and able to transfer the data. IoT devices are enlarging the internet connectivity beyond standard devices such as smartphones, laptops, tablets, and desktops.
- There are large varieties of IoT devices available based on IEEE 802.15.4 standard. These devices range from wireless motes, attachable sensor-boards to interface-board which are useful for researchers and developers.
- IoT devices include computer devices, software, wireless sensors, and actuators. These IoT devices are connected over the internet and enabling the data transfer among objects or people automatically without human intervention.
- Some of the common and popular IoT devices are given below

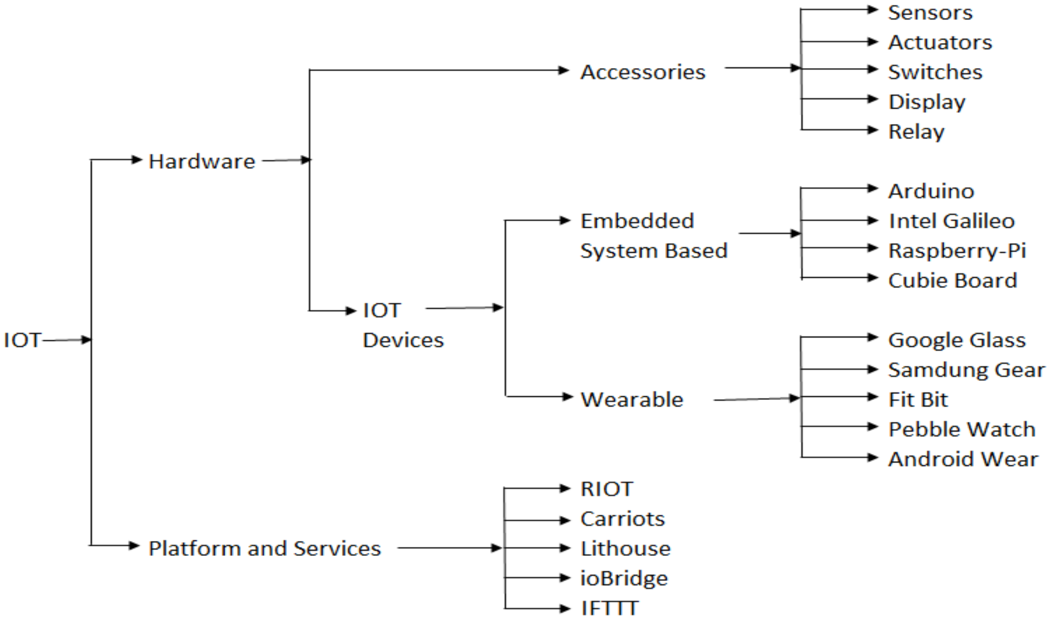


Fig. 2.19IoT Devices and Technologies

Properties of IoT Devices

Some of the essential properties of IoT devices are mention below:

- **Sense:** The devices that sense its surrounding environment in the form of temperature, movement, and appearance of things, etc.
- **Send and receive data:** IoT devices are able to send and receive the data over the network connection.
- **Analyze:** The devices can able to analyze the data that received from the other device over the internet networks.

- **Controlled:** IoT devices may control from some endpoint also. Otherwise, the IoT devices are themselves communicate with each other endlessly leads to the system failure.

Arduino Uno:

- Arduino devices are the microcontrollers and microcontroller kit for building digital devices that can be sense and control objects in the physical and digital world.
- Arduino boards are furnished with a set of digital and analog input/output pins that may be interfaced to various other circuits.
- Some Arduino boards include USB (Universal Serial Bus) used for loading programs from the personal computer.
- Arduino is an open-source electronics platform based on easy-to-use hardware and software.

Properties of Arduino:

- **Inexpensive:**Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50.
- **Cross-platform:** The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- **Simple, clear programming environment:** The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with how the Arduino IDE works.
- **Open source and extensible software:** The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- **Open source and extensible hardware:** The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in orderto understand how it works and save money.

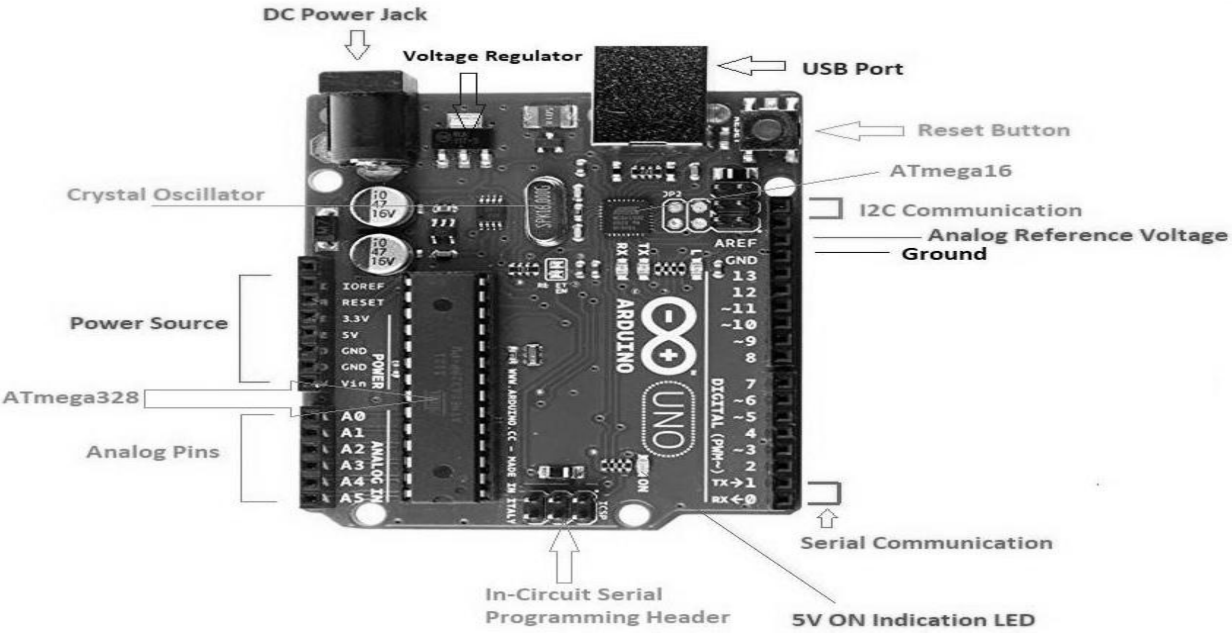


Fig. 2.20 Arduino Uno

Raspberry Pi:

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. The Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins that allow you to control electronic components for physical computing and explore the Internet of Things (IoT). Raspberry Pi has an ARMv6 700 MHz single-core processor, a VideoCore IV GPU and 512MB of RAM. it uses an SD card for its operating system and data storage. The Raspberry Pi officially supports Raspbian, a lightweight linux OS based on Debian. Back in 2006, while Eben Upton, his colleagues at University of Cambridge, in conjunction with Pete Lomas and David Braben, formed the Raspberry Pi Foundation.

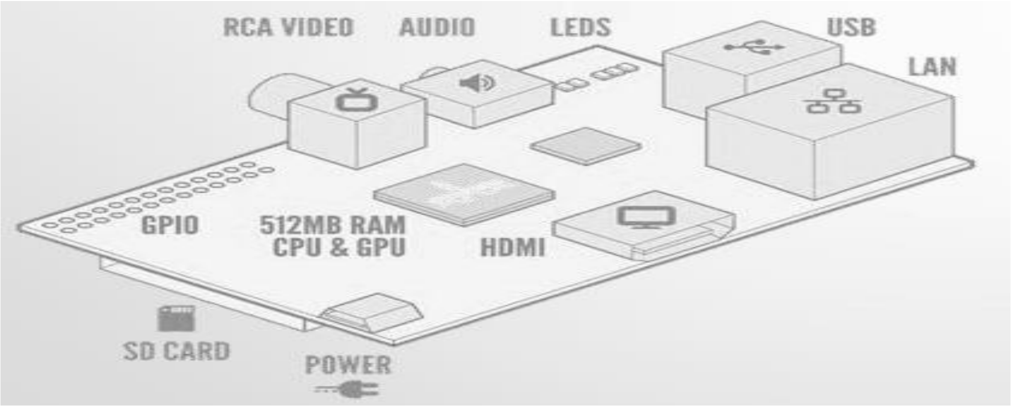


Fig. 2.21 Raspberry Pi Model

Components of Raspberry Pi Board

- **ARM CPU/GPU** -- This is a Broadcom BCM2835 System on a Chip (SoC) that's made up of an ARM central processing unit (CPU) and a Videocore 4 graphics processing unit (GPU). The CPU handles all the computations that make a computer work (taking input, doing calculations and producing output), and the GPU handles graphics output.

- **GPIO** -- These are exposed general-purpose input/output connection points that will allow the real hardware hobbyists the opportunity to tinker.
- **RCA** -- An RCA jack allows connection of analog TVs and other similar output devices.
- **Audio out** -- This is a standard 3.55-millimeter jack for connection of audio output devices such as headphones or speakers. There is no audio in.
- **LEDs** -- Light-emitting diodes, for all of your indicator light needs.
- **USB** -- This is a common connection port for peripheral devices of all types (including your mouse and keyboard). Model A has one, and Model B has two. You can use a USB hub to expand the number of ports or plug your mouse into your keyboard if it has its own USB port.
- **HDMI** -- This connector allows you to hook up a high-definition television or other compatible device using an HDMI cable.
- **Power** -- This is a 5v Micro USB power connector into which you can plug your compatible power supply.
- **SD cardslot** -- This is a full-sized SD card slot. An SD card with an operating system (OS) installed is required for booting the device. They are available for purchase from the manufacturers, but you can also download an OS and save it to the card yourself if you have a Linux machine and the wherewithal.
- **Ethernet** -- This connector allows for wired network access and is only available on the Model B.

Advantages of Different Raspberry Pi Models

- The size of the raspberry pi is in small of credit card
- The price of the raspberry pi is low
- Gathering a set of raspberry pi to work as a server is more effective than the normal server.

Applications of Raspberry pi

The different applications of the raspberry pi model are

- Media steamer
- Tablet computer
- Home automation
- Internet radio
- Controlling robots
- Cosmic Computer
- Arcade machines
- Raspberry pi based projects

Nodeµ

- NodeMCU is an open source IoT platform.
- The NodeMCU (Node MicroController Unit) is an open source software and hardware development environment that is built around a very inexpensive System-on-a-Chip (SoC) called the ESP8266.
- The ESP8266 can be controlled from your local Wi-Fi network or from the internet (after port forwarding). The ESP-01 module has GPIO pins that can be programmed to turn an LED or a relay ON/OFF through the internet.
- The module can be programmed using an Arduino/USB-to-TTL converter through the serial pins (RX,TX).
- It uses the Lua scripting and C language with arduinosoftware(using arduino library).
- It has 10 GPIO, every GPIO can be PWM, I2C, 1-wire. It is Wi-Fi enabled device.
- NodeMCU Development board is featured with wifi capability, analog pin, digital pins and serial communication protocols.
- NodeMCUDev Kit has Arduino like Analog (i.e. A0) and Digital (D0-D8) pins on its board. It supports serial communication protocols i.e. UART, SPI, I2C etc. Using such serial protocols we can connect it with serial devices like I2C enabled LCD display, Magnetometer HMC5883, MPU-6050 Gyro meter + Accelerometer, RTC chips, GPS modules, touch screen displays, SD cards etc.

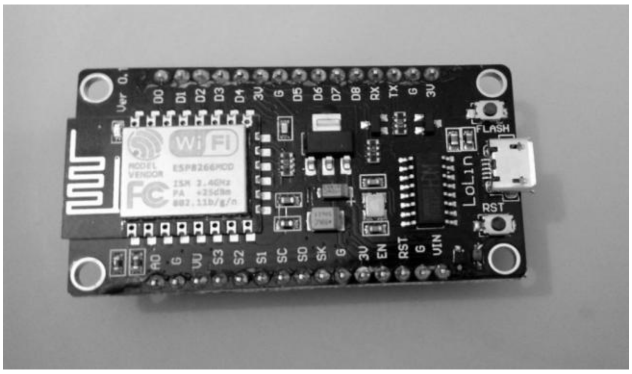

D0 D1 D2 D3 D4 3V G D5 D6 D7 D8 RX TX G 3V
WiFi
ESP8266MOD
FLASH
LoLin
RST
A0 G VU S3 S2 S1 SC SO SK G 3V EN RST G VIN

Fig. 2.22 NodeMcuESP8266

2.2.7 Case study on IoT Applications using various Sensors and actuators

Sensors: A sensor is an electronic instrument that is able to measure the physical quantity and generate a considerate output. These output of the sensors are usually in the form of electrical signals. Sensors are placed as such they can directly interact with the environment to sense the input energy with the help of sensing element. This sensed energy is converted into a more suitable form by a transduction element. There are various types of sensors such as position, temperature, pressure, speed sensors, but fundamentally there are two types – analog and digital. The different types come under these two basic types. A digital sensor is incorporated with an Analog-to-digital converter while analog sensor does not have any ADC.

Actuators: An actuator is a device that alters the physical quantity as it can cause a mechanical component to move after getting some input from the sensor. In other words, it receives control input (generally in the form of the electrical signal) and generates a change in the physical system through producing force, heat, motion, etcetera. An actuator can be interpreted with the example of the stepper motor, where an electrical pulse drives the motor. Each time a pulse given in the input accordingly motor rotates in a predefined amount. A stepper motor is suitable for the applications where the position of the object has to be controlled precisely, for example, robotic arm.

Types of IoT Sensors

Temperature sensors: These devices measure the amount of heat energy generated from an object or surrounding area. They find application in air-conditioners, refrigerators and similar devices used for environmental control. They are also used in manufacturing processes, agriculture and health industry.

Temperature sensors include thermocouples, thermistors, resistor temperature detectors (RTDs) and integrated circuits (ICs).

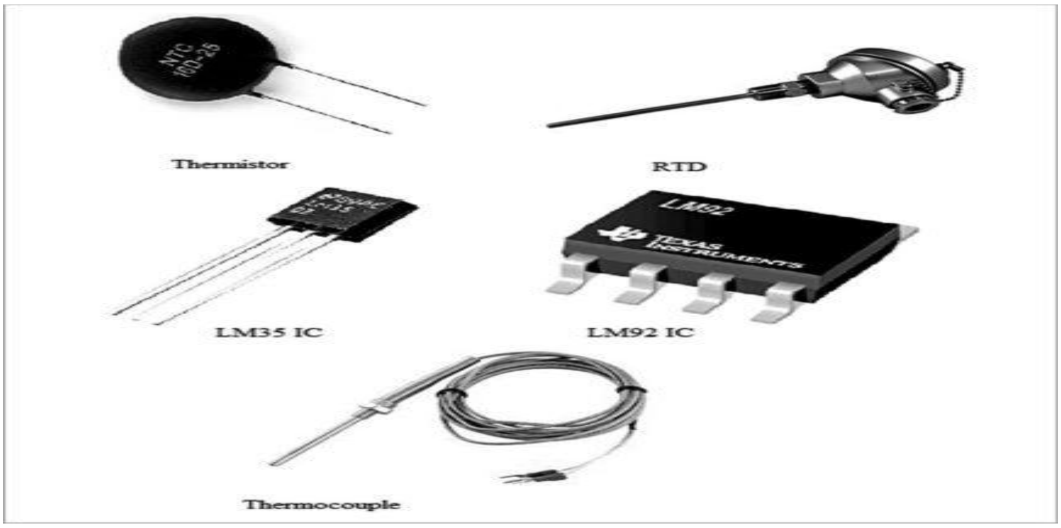


Fig. 2.23 Temperature Sensors

Humidity sensors: The amount of water vapour in air, or humidity, can affect human comfort as well as many manufacturing processes in industries. So monitoring humidity level is important. Most commonly used units for humidity measurement are relative humidity (RH), dew/frost point (D/F PT) and parts per million (PPM).

Fig. 2.24 Humidity Sensor

Motion sensors: Motion sensors are not only used for security purposes but also in automatic door controls, automatic parking systems, automated sinks, automated toilet flushers, hand dryers, energy management systems, etc. You use these sensors in the IoT and monitor them from your smartphone or computer. HC-SR501 passive infrared (PIR) sensor is a popular motion sensor for hobby projects.

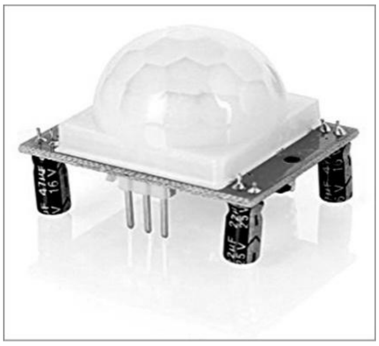


Fig. 2.25 Motion Sensor

Gas sensors: These sensors are used to detect toxic gases. The sensing technologies most commonly used are electrochemical, photo-ionisation and semiconductor. With technical advancements and new specifications, there are a multitude of gas sensors available to help extend the wired and wireless connectivity deployed in IoT applications.

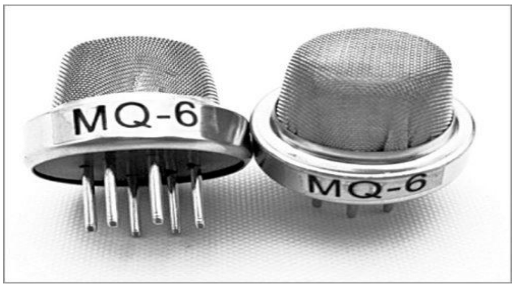


Fig. 2.26 Gas Sensor

Smoke sensors: Smoke detectors have been in use in homes and industries for quite a long time. With the advent of the IoT, their application has become more convenient and user-friendly. Furthermore, adding a wireless connection to smoke detectors enables additional features that increase safety and convenience.

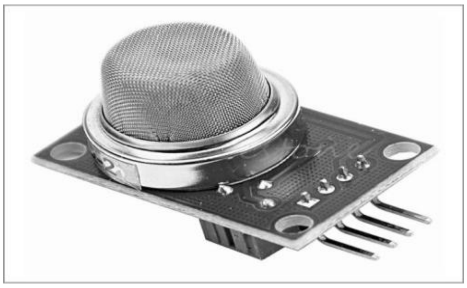


Fig. 2.27 Smoke Sensor

Pressure sensors: These sensors are used in IoT systems to monitor systems and devices that are driven by pressure signals. When the pressure range is beyond the threshold level, the device alerts the user about the problems that should be fixed. For example, BMP180 is a popular digital pressure sensor for use in mobile phones, PDAs, GPS navigation devices and outdoor equipment. Pressure sensors are also used in smart vehicles and aircrafts to determine force and altitude, respectively. In vehicle, tyre pressure monitoring system (TPMS) is used to alert the driver when tyre pressure is too low and could create unsafe driving conditions.

Image sensors: These sensors are found in digital cameras, medical imaging systems, night-vision equipment, thermal imaging devices, radars, sonars, media house and biometric systems. In the retail industry, these sensors are used to monitor customers visiting the store through IoT network. In offices and corporate buildings, they are used to monitor employees and various activities through IoT networks.

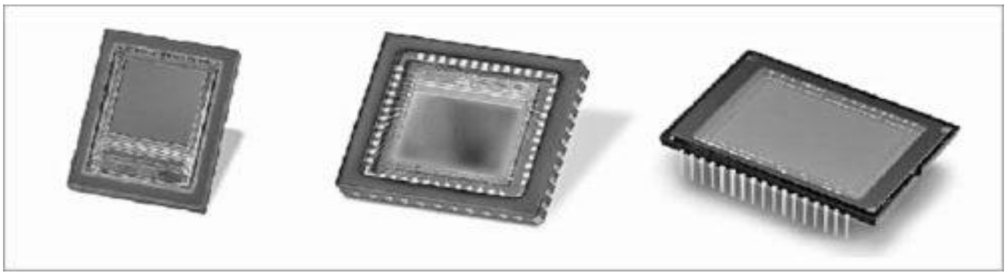


Fig. 2.28 Image Sensor

Accelerometer sensors: These sensors are used in smartphones, vehicles, aircrafts and other applications to detect orientation of an object, shake, tap, tilt, motion, positioning, shock or vibration. Different types of accelerometers include Hall-effect accelerometers, capacitive accelerometers and piezoelectric accelerometers.

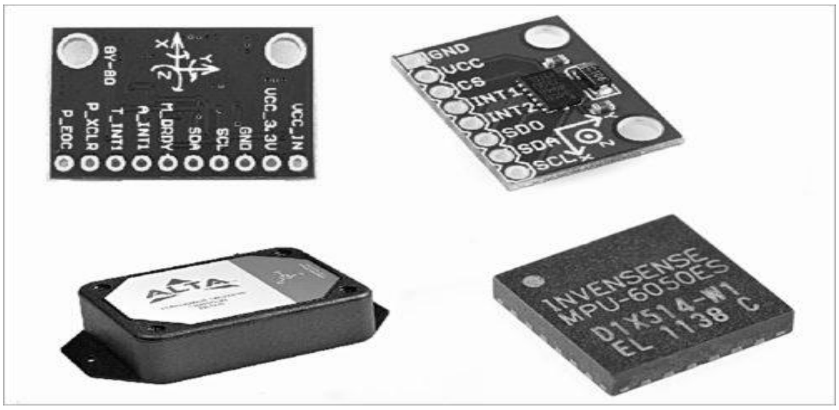


Fig. 2.29 Accelerator Sensors

IR sensors: These sensors can measure the heat emitted by objects. They are used in various IoT projects including healthcare to monitor blood flow and blood pressure, smartphones to use as remote control and other functions, wearable devices to detect amount of light, thermometers to monitor temperature and blind-spot detection in vehicles.

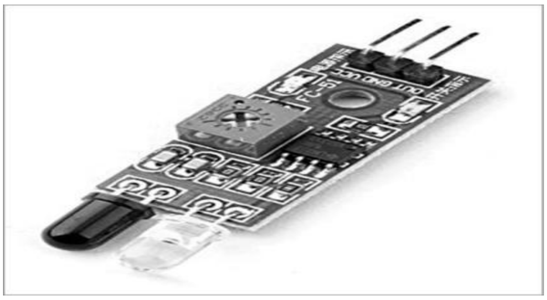
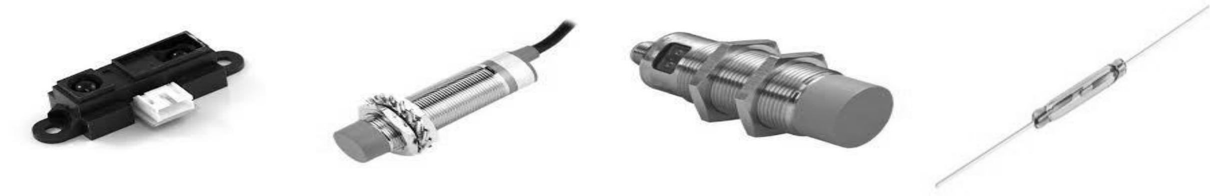


Fig. 2.30 IR Sensor

Proximity sensors: These sensors detect the presence or absence of a nearby object without any physical contact. Different types of proximity sensors are inductive, capacitive, photoelectric, ultrasonic and magnetic. These are mostly used in object counters, process monitoring and control.



IR Proximity Sensor

Inductive proximity sensor

Capacitive Sensor

Reed Switch

Fig. 2.31 Proximity sensors

Basic actuators you may use in your IoT projects

Servo motors: A Servo is a small device that incorporates a two wire DC motor, a gear train, a potentiometer, an integrated circuit, and a shaft (output spine). The shaft can be positioned to specific angular positions by sending the servo a coded signal. Of the three wires that stick out from the servo casing, one is for power, one is for ground, and one is a control input line. It uses the position-sensing device to determine the rotational position of the shaft, so it knows which way the motor must turn to move the shaft to the commanded position.

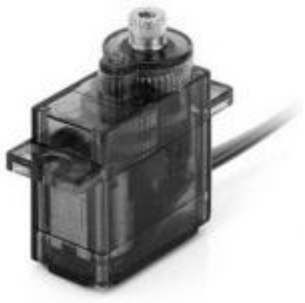


Fig. 2.32 Servo Motor

Stepper Motor: Stepper motors are DC motors that move in discrete steps. They have multiple coils that are organized in groups called “phases”. By energizing each phase in sequence, the motor will rotate, one step at a time. With a computer controlled stepping, you can achieve very precise positioning and/or speed control.

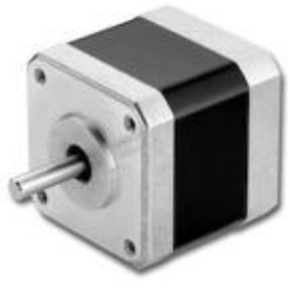


Fig. 2.33 Stepper Motor

DC motors: Direct Current (DC) motor is the most common actuator used in electronics projects. They are simple, cheap, and easy to use. DC motors convert electrical into mechanical energy. They consist of permanent magnets and loops of wire inside. When current is applied, the wire loops generate a magnetic field, which reacts against the outside field of the static magnets.

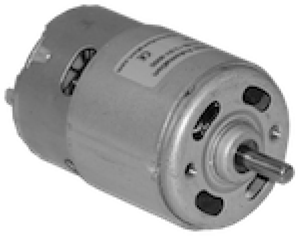


Fig. 2.34 DC Motor

Linear Actuator: A linear actuator is an actuator that creates motion in a straight line, in contrast to the circular motion of a conventional electric motor. Linear actuators are used in machine tools and industrial machinery, in computer peripherals such as disk drives and printers, in valves and dampers, and in many other places where linear motion is required.

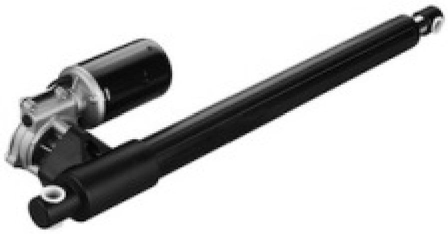


Fig. 2.35 Linear Actuator

Relay: A relay is an electrically operated switch. Many relays use an electromagnet to mechanically operate a switch, but other operating principles are also used, such as solid-state relays. The advantage of relays is that it takes a relatively small amount of power to operate the relay coil, but the relay itself can be used to control motors, heaters, lamps or AC circuits which themselves can draw a lot more electrical power.

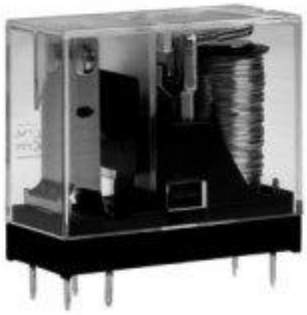


Fig. 2.36 Relay

Solenoid: A solenoid is simply a specially designed electromagnet. Solenoids are inexpensive, and their use is primarily limited to on-off applications such as latching, locking, and triggering. They are frequently used in home appliances (e.g. washing machine valves), office equipment (e.g. copy machines), automobiles (e.g. door latches and the starter solenoid), pinball machines (e.g., plungers and bumpers), and factory automation.

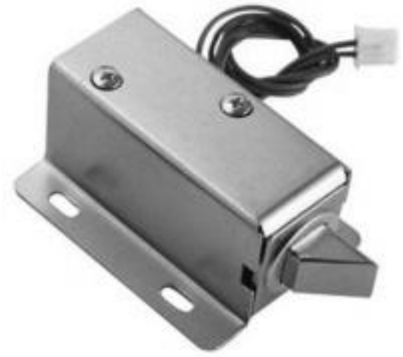


Fig. 2.37Solenoid

References:

- https://data-flair.training/blogs/iot-applications/
- https://books.google.co.in/books?id=JPKGBAAAQBAJ&pg=PA45&source=gbs_toc_r&cad=2#v=onepage&q&f=false
- https://www.tutorialspoint.com/arduino/arduino_board_description.htm#
- https://kainjan1.files.wordpress.com/2018/01/chapter-1_iot.pdf
- https://www.tutorialspoint.com/internet_of_things/internet_of_things_tutorial.pdf
- https://www.iare.ac.in/sites/default/files/lecture_notes/IOT%20LECTURE%20NOTES_IT.pdf
- https://components101.com/microcontrollers/arduino-uno
- https://computer.howstuffworks.com/raspberry-pi2.htm
- https://www2.deloitte.com/content/dam/insights/us/articles/iot-primer-iot-technologies-applications/DUP_1102_InsideTheInternetOfThings.pdf
- https://techdifferences.com/difference-between-sensors-and-actuators.html
- https://electronicsforu.com/technology-trends/tech-focus/iot-sensors
- https://iotbytes.wordpress.com/basic-iot-actuators/
- https://en.wikipedia.org/wiki/NodeMCU
- https://www.electronicwings.com/nodemcu/introduction-to-nodemcu
- https://www.instructables.com/id/Programming-ESP8266-ESP-12E-NodeMCU-Using-Arduino-/
- https://datafloq.com/read/3-major-challenges-facing-future-iot/2729

Sample Multiple Choice Questions:

1. IoT stands for
    a. Internet of Technology
    b. Intranet of Things
    c. Internet of Things
    d. Information of Things
2. Which is not the Feature of IoT
    a. Connectivity

b. Self-Configuring
c. Endpoint Management
d. Artificial Intelligence

3. Which not anIoT Communication model
   a. Request-Response
   b. Publish-Subscribe
   c. Push-Producer
   d. Exclusive Pair
4. WSN Stands for
   a. Wide Sensor Network
   b. Wireless Sensor Network
   c. Wired Sensor Network
   d. None of these
5. Devices that transforms electrical signals into physical movements.
   a. Sensors
   b. Actuators
   c. Switches
   d. display

Unit-3 Basics of Digital Forensic

Content

3.1 Digital forensics

- Introduction to digital forensic
- History of forensic
- Rules of digital forensic
- Definition of digital forensic
- Digital forensics investigation and its goal

3.2 Models of Digital Forensic Investigation

- Digital Forensic Research Workshop Group (DFRWS) Investigative Model
- Abstract Digital Forensics Model (ADFM)
- Integrated Digital Investigation Process (IDIP)
- End to End digital investigation process (EEDIP)
- An extended model for cybercrime investigation
- UML modeling of digital forensic process model (UMDFPM)

3.3 Ethical issues in digital forensic

- General ethical norms for investigators
- Unethical norms for investigation

3.1 Digital Forensics

3.1.1 Introduction to Digital Forensics

Forensics science is a well-established science that pays vital role in criminal justice systems. It is applied to both criminal and civil action. Digital forensics sometimes known as digital forensic science, is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

Digital forensics includes the identification, recovery, investigation, validation, and presentation of facts regarding digital evidence found on computers or similar digital storage media devices.

3.1.2 History of Forensic

1. Field of pc forensics began in 1980s when personal computers became a viable possibility for the buyer.
2. In 1984, an associate Federal Bureau of Investigation program was created, which was referred to as magnet media program.
3. It is currently referred to as Computer Analysis and Response Team (CART).
4. Michael Anderson, the Father of Computer Forensics, came into limelight during this period.
5. International Organization on Computer Evidence (IOCE) was formed in 1995.
6. In 1997, the great countries declared that law enforcement personnel should be trained and equipped to deal with sophisticated crimes.

7. In 1998, INTERPOL Forensic Science symposium was apprehended.
8. In 1999, the FBI CART case load goes beyond 2000 case examining, 17 terabytes of information.
9. In 2000, the first FBI Regional Computer Forensic Laboratory was recognized.
10. In 2003, the FBI CART case load exceeds 6500 cases, examining 782 terabytes of information.

3.1.3 Rule of Digital Forensics

While performing digital forensics investigation, the investigator should follow the given rules:

Rule 1. An examination should never be performed on the original media.
Rule 2. A copy is made onto forensically sterile media. New media should always be used if available.
Rule 3. The copy of the evidence must be an exact, bit-by-bit copy. (Sometimes referred to as a bit-stream copy).
Rule 4. The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified.
Rule 5. The examination must be conducted in such a way as to prevent any modification of the evidence.
Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

3.1.4 Definition of Digital Forensics

Digital forensics is a series of steps to uncover and analyses electronic data through scientific method. Major goal of the process is to duplicate original data and preserve original evidence and then performing the series of investigation by collecting, identifying and validating digital information for the purpose of restructuring past events.

3.1.5 Digital Forensic Investigation

Digital forensic investigation (DFI) is a special type of investigation where the scientific procedures and techniques used will be allowed to view the result- digital evidence- to be admissible in a court of law.

3.1.6 Goals of Digital Forensic Investigation:

The main objective computer forensic investigation is to examine digital evidences and to ensure that they have not been tampered in any manner. To achieve this goal investigation must be able to handle all below obstacles:

1. Handle and locate certain amount of valid data from large amount of files stored in computer system.
2. It is viable that the information has been deleted, I such situation searching inside the file is worthless.

3. If the files are secured by some passwords, investigators must find a way to read the protected data in an unauthorized manner.
4. Data may be stored in damaged device but the investigator searches the data in working devices.
5. Major obstacle is that, each and every case is different identifying the techniques and tools will take long time.
6. The digital data found should be protected from being modified. It is very tedious to prove that data under examination is unaltered.
7. Common procedure for investigation and standard techniques for collecting and preserving digital evidences are desired.

3.2 Models of Digital Forensics

3.2.1 Road map for Digital Forensic Research (RMDFR)

Palmar designed a framework with the following indexed processes shown in Figure 3.1.

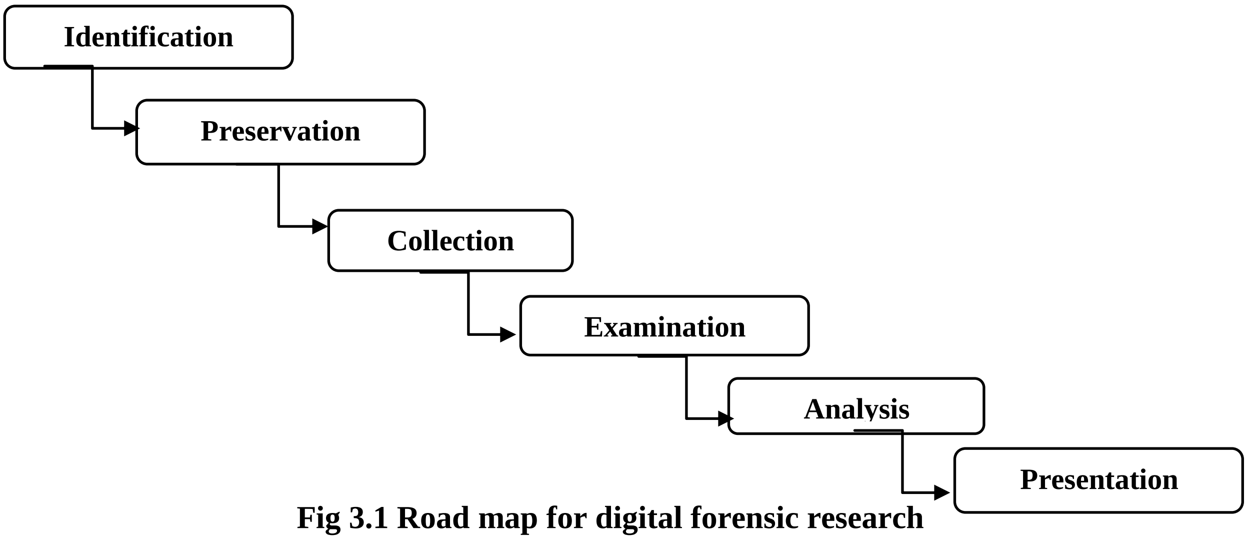


Fig 3.1 Road map for digital forensic research

Six Phases of RMDFR are as follows:

1. **Identification**: It recognizes an incident from indicators and determines its type.
2. **Preservation**: Preservation stage corresponds to \freezing the crime scene". It consists in stopping or preventing any activities that can damage digital information being collected. Preservation involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.
3. **Collection**: Collection stage consists in finding and collecting digital information that may be relevant to the investigation. Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium. Collection may involve removal of personal computers from the crime scene, copying or printing out contents of files from a server, recording of network traffic, and so on.

4. **Examination**: Examination stage consists in a \in-depth systematic search of evidence" relating to the incident being investigated. The outputs of examination are data objects found in the collected information. They may include logfiles, data files containing specific phrases, times-stamps, and so on.
5. **Analysis**: The aim of analysis is to "draw conclusions based on evidence found".
6. **Reporting**: This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

3.2.2 Abstract Digital Forensic Model (ADFM)

Reith, Carr, Gunsh proposed Abstract Digital Forensic model in 2002.

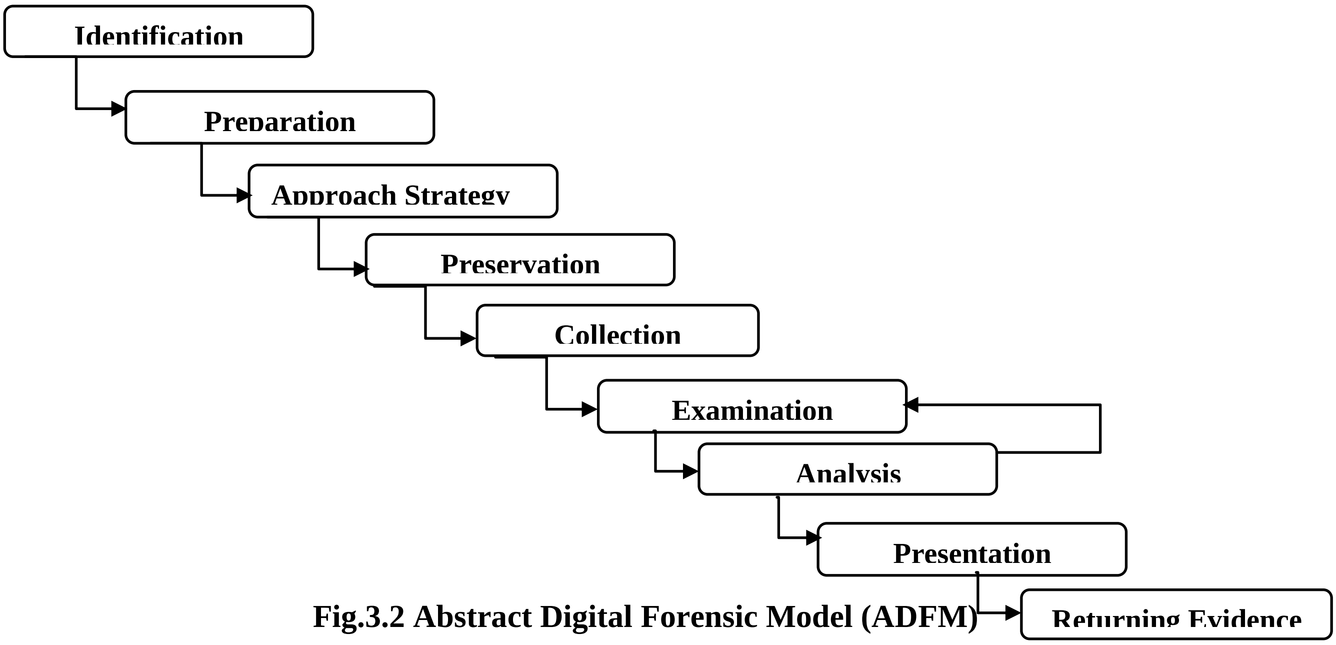


Fig.3.2 Abstract Digital Forensic Model (ADFM)

Phases of ADFM model are as follows:

1. **Identification** –it recognizes an incident from indicators and determines its type.
2. **Preparation** –it involves the preparation of tools, techniques, search warrants and monitoring authorization and management support
3. **Approach strategy** –formulating procedures and approach to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim
4. **Preservation**–it involves the isolation, securing and preserving the state of physical and digital evidence
5. **Collection** –This is to record the physical scene and duplicate digital evidence using standardized and accepted procedures
6. **Examination** –An in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence.
7. **Analysis** –This determines importance and probative value to the case of the examined product
8. **Presentation** -Summary and explanation of conclusion
9. **Returning Evidence** –Physical and digital property returned to proper owner

3.2.3 Integrated Digital Investigation Process (IDIP)

DFPM along with5 groups and 17 phases are proposed by Carrier and Safford. DFPM is named the Integrated Digital Investigation Process (IDIP). The groups are indexed as shown in following Figure 2.3.

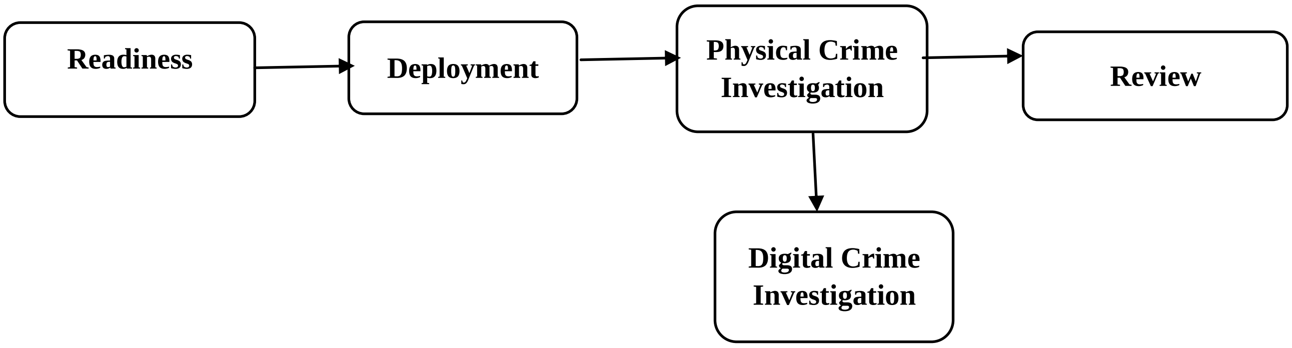


Fig. 3.3An Integrated Digital Investigation Process

The phases of IDIP are as follows:

1. **Readiness phase**The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:
2. •Operations Readiness phase
   • Infrastructure Readiness phase
3. **Deployment phase** The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

- Detection and Notification phase; where the incident is detected and then appropriate people notified.
- Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

4. **Physical Crime Investigation phase** The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident.
   It includes six phases:

- Preservation phase; which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
- Survey phase; that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
- Documentation phase; which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
- Search and collection phase; that entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin

- Reconstruction phase; which involves organizing the results from the analysis done and using them to develop a theory for the incident.
- Presentation phase; that presents the physical and digital evidence to a court or corporate management.

5. **Digital Crime Investigation phase**The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are:
   - Preservation phase; which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.
   - Survey phase; whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.
   - Documentation phase; which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
   - Search and collection phase; whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user's activities and identity.
   - Reconstruction phase; which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses.
   - Presentation phase; that involves presenting the digital evidence that was found to the physical investigative team.

It is noteworthy that this DFPM facilitates concurrent execution of physical and digital investigation.

6. **Review phase** this entails a review of the whole investigation and identifies areas of improvement. The IDIP model does well at illustrating the forensic process, and also conforms to the cyber terrorism capabilities which require a digital investigation to address issues of data protection, data acquisition, imaging, extraction, interrogation, ingestion/normalization, analysis and reporting. It also highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

3.2.4 End to End Digital Investigation Process (EEDIP)

This model is proposed by Stephenson comprises of six major mechanism within framework. EEDIP stands for End-to-End Digital Investigation Process which ensures investigation operation from beginning to end.

The phases of EEDIP are as follows:

1. Identification phase involves identifying the nature of incident from possible known indicators. Indicators are experience investigator.

2. The preservation phase includes condensing the investigation and finding till date.
3. The collection phase includes documentation of the physical scene and replication of the digital evidence using approved standard procedure.
4. Examination phase involves obtaining and studying the digital evidence .Method of extraction is used for reconstructing data from the media.
5. In the analysis phase the vitally of the documented evidence is explored and conclusions are drawn by integrating chunk of data.
6. The presentation phase involves summarizing the evidences found in the process of investigation.

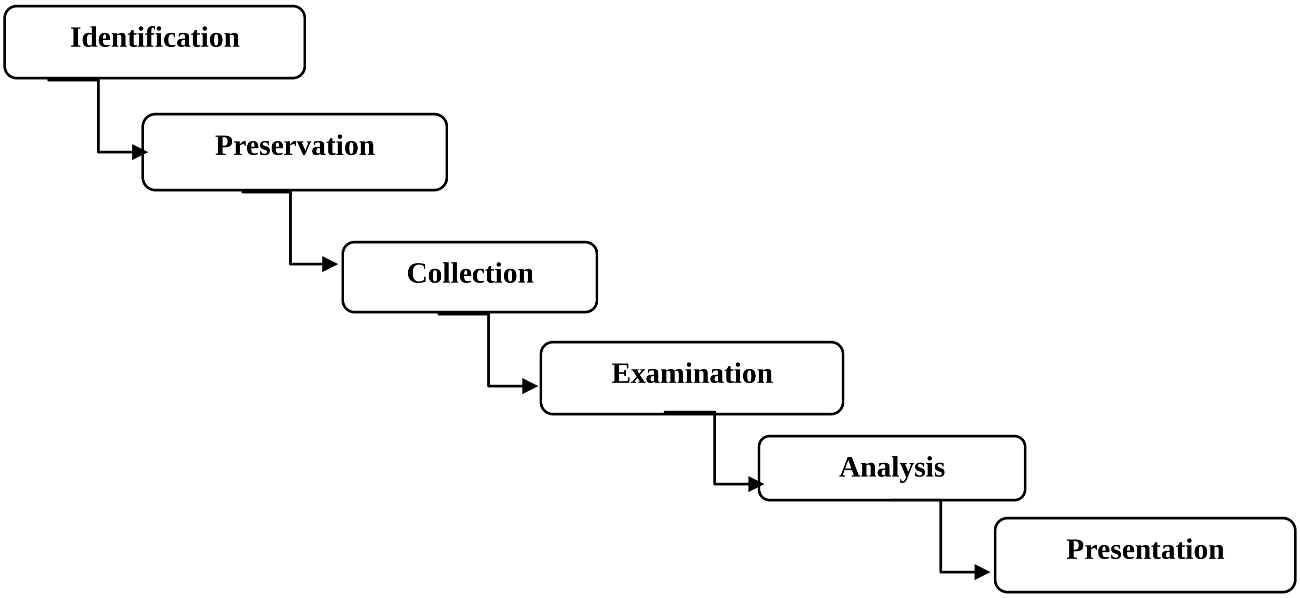


Fig 3.4 End to End Digital Investigation Process

3.2.5 An Extended Model of Cybercrime Investigation (EMCI)

The DFPM proposed by S. O. Ciardhuain- an Extended Model of Cybercrime Investigation (EMCI) - is more likely the most comprehensive till date.

Phases of EMCI: The EMCI follows waterfall model as every activity occurs in sequence. The sequence of examine, hypothesis, present, and prove/defend are bound to be repeated as the evidence heap increases during the investigation.

1. Awareness is the phase during which the investigator are informed that a crime has taken place; the crime is reported to some authority. An intrusion detection system may also triggered such awareness.
2. Authorization is the stage where the nature of investigation has been identified and the unplanned authorization may be required to proceed and the authorization is obtained internally or externally.
3. Planning is impacted by information from which and outside the organization that will affect the investigation. Internal factors are the organization policies, procedures, and former investigative knowledge while outside factors consist of legal and other requirements not known by the investigators.

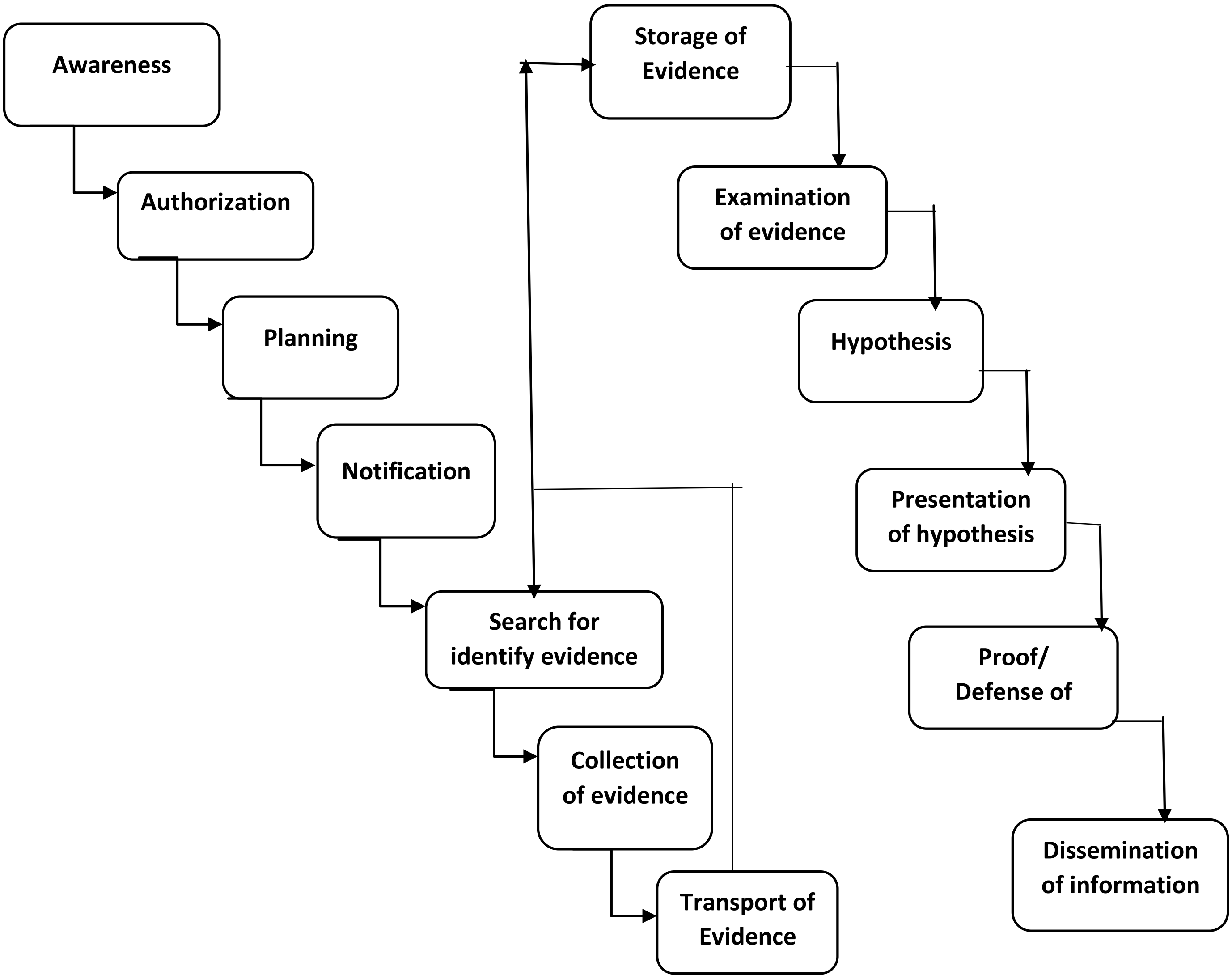


Figure 3.5 an Extended Model of Cybercrime Investigation

3.2.6 UML modeling of digital forensic process model(UMDFPM)

Kohn, Eloff, and Oliver proposed the UML Modeling of Digital Forensic Process Model, apt paradigm for modeling forensic processes.

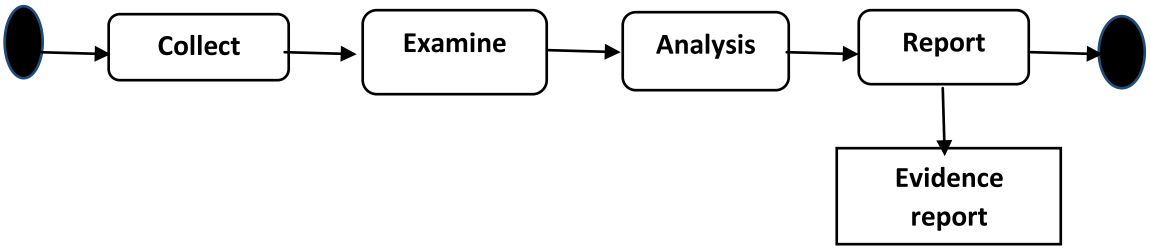


Fig 3.6 UML modeling of digital forensic process model

Phases of UMDFPM:

Kohn and Oliver made use of UML and case diagram (Figure 2.6) to demonstrate all the phases and its interaction with all investigators. Two processes have been added to the activity diagram to club with Kohn framework. These are “prepare” in the preparation phase and “present” in presentation phase.

1. The whole process is trigged by criminal activity, which constitutes of starting point. Prepare is the first step. The rest of the processes follow logically from prepare to collect, authenticate, examination and the analyze
2. Authentication is introduce between examination and collection phase to make sure that the data integrity of the data before the examination is started is preserved.
3. Examination can alter the contents of data such as in the case of compressed files, hidden files and other forms of data incomprehension.

The primary investigator will consider whether to analyze more data or to extract more data from the original source. After reaching this decision points an evidence report is compiled as part of the report procedure. Whole document is compiled during the investigation phase. The evidence document is the output of investigation phase.

3.3 Ethical issues in Digital Forensic

Ethics in digital forensic field can be defined as set of moral principles that regulate the use of computers. Ethical decision making in digital forensic work comprises of one or more of the following:

1. Honesty towards the investigation
2. Prudence means carefully handling the digital evidences
3. Compliance with the law and professional norms.

3.3.1 General ethical norms for investigator

Investigator should satisfy the following points:

1. To contribute to the society and human being
2. To avoid harm to others
3. To be honest and trustworthy
4. To be fair and take action not to discriminate
5. To honor property rights, including copyrights and patents
6. To give proper credit to intellectual property
7. To respect the privacy of others
8. To honor confidentiality
9.

3.3.2 Unethical norms for Digital Forensic Investigation

Investigator should not:

1. Uphold any relevant evidence
2. Declare any confidential matters or knowledge
3. Express an opinion on the guilt or innocence belonging to any party

4. Engage or involve in any kind of unethical or illegal conduct
5. Deliberately or knowingly undertake an assignment beyond him or her capability
6. Distort or falsify education, training, credentials
7. Display bias or prejudice in findings or observation
8. Exceed or outpace authorization in conducting examination

References:

- Digital Forensic by Dr. Nilakshi Jain and Dr. DhanjayKalbande Wiley publication ISBN:978-81-265-6574-0
- 2.https://www.academia.edu/34925415/Computer_Forensics_Digital_Forensic_Analysis_Methodology
- http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0C1681D4A48C19E12DFD96B781B18532?doi=10.1.1.258.7882&rep=rep1&type=pdf

Sample Multiple Choice Questions:

1. Digital forensics is all of them except:
   a) Extraction of computer data
   b) Preservation of computer data
   c) Interpretation of computer data
   d) Manipulation of computer data

2. IDIP stands for
   a) Integrated Digital Investigation Process
   b) Integrated Data Investigation Process
   c) Integrated Digital Investigator Process
   d) Independent Digital Investigator Process

3. Who proposed Road map model?
   a) G. Gunsh
   b) S. Ciardhuain
   c)J. Korn
   d)G. Palmar

4. Investigator should satisfy the following point:
   a) Contribute to the society and human being
   b) Avoid harm to others
   c) Honest and trustworthy
   d) All of the above

Unit-4 Digital Evidences

4.1 Digital Evidences:

The field of computer security includes events that provide a successful courtroom experience, which are both worthwhile and satisfactory. Investigation of a computer security incident leads to legal proceeding, such as court proceeding, where the digital evidence and documents obtained are likely used as exhibits in the trial.

To meet the requirements of the judging body and to withstand or face any challenges, it is essential to follow the evidence-handling procedure. Also, it is necessary to ensure that the evidence-handling procedures chosen are not difficult to implement at your organization as this can sometimes become an overhead for an organization.

While investigating a computer security incident, we are sometimes unsure and indecisive whether an item(viz. a chip, floppy disk, etc)should be considered as an evidence or an attachment or an addendum.

Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital evidence.

Digital Evidences: (Electronic evidence)

- **Evidence:** Any information that can be confident or trusted and can prove something related to a case in trial that is, indicating that a certain substance or condition is present.
- **Relevant Evidence**: An information which has a positive impact on the action occurred, such as the information supporting an incident.
- **Digital Evidence:** Digital evidence is any information or data that can be confident or trusted and can prove something related to a case trial, that is, indicating that a certain substance or condition is present. It is safe to use to use such information as evidence during an investigation.

4.1.1 Digital evidence or **Electronic evidence** is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.

Digital evidence is also defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired when electronic devices are seized and secured for examination. Digital evidence:

- Is latent (hidden), like fingerprints or DNA evidence
- Crosses jurisdictional borders quickly and easily
- Can be altered, damaged or destroyed with little effort
- Can be time sensitive

There are many sources of digital evidence; the topic is divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence-gathering processes, tools and concerns, and different types of crimes tend to lend themselves to one device or the other.

Some of the popular electronic devices which are potential digital evidence are: HDD, CD/DVD media, backup tapes, USB drive, biometric scanner, digital camera, smart phone, smart card, PDA, etc.

Forms of digital evidence: Text message, emails, pictures, videos and internet searches are most common types of Digital evidences.

The digital evidence are used to establish a credible link between the attacker, victim, and the crime scene. Some of the information stored in the victim's system can be potential digital evidence, are IP address, system log-in & remote log-in details, browsing history, log files, emails, images, etc.

Digital Evidences may be in the form:

- Email Messages (may be deleted one also)
- Office file
- Deleted files of all kinds

- Encrypted file
- Compressed files
- Temp files
- Recycle Bin
- Web History
- Cache files
- Cookies
- Registry
- Unallocated Space
- Slack Space
- Web/E-Mail server access Logs
- Domain access Logs

4.1.2 Best Evidence Rule:

The original or true writing or recording must be confessed in court to prove its contents without any expectations. An original copy of the document is considered as superior evidence.

One of the rules states that if evidence is readable by sight or reflects the data accurately, such as any printout or data stored in a computer or similar devices or any other output, it is considered as "original".

It states that multiple copies of electronic files may be a part of the "original" or equivalent to the "original". The collected electronic evidence is mostly transferred to different media. Hence, many computer security professionals are dependent on this rule.

Best Evidence: The most complete copy or a copy which includes all necessary parts of evidence, which is closely related to the original evidence.

Example-A client has a copy of the original evidence media.

The "Best Evidence Rule" says that an original writing must be offered as evidence unless it is unavailable, in which case other evidence, like copies, notes, or other testimony can be used. Since the rules concerning evidence on a computer are fairly reasonable (what you can see on the monitor is what the computer contains, computer printouts are best evidence) computer records and records obtained from a computer are best evidence.

4.1.3 Original Evidence:

The procedure adopted to deal with a situation or case takes it outside the control of the client/victim. A case with proper diligence or a case with persistence work will end up in a judicial proceeding, and we will handle the evidences accordingly.

For this purpose original evidence as the truth or real (original) copy of the evidence media which is given by victim/client.

We define best incidence as the most complete copy, which includes all the necessary parts of the evidence that are closely related to the original evidence. It is also called as duplication of the evidence media. There should be an evidence protector which will store either the best evidence or original evidence for every investigation in the evidence safe.

4.2 Rules of Digital Evidence:

Rule of evidence is also called as Law of evidence. It surrounds the rules and legal principles that govern all the proof of facts. This rule helps us to determine what evidence must or must not be considered by a trier of fact. The rule of evidence is also concerned with the amount, quantity and type of proof which helps us to prove in litigation. The rules may vary according to the criminal court, civil court etc.

The rule must be:

- **Admissible:** The evidence must be usable in the court.
- **Authentic:** The evidence should act positively to an incident.
- **Complete:** A proof that covers all perspectives.
- **Reliable:** There ought to be no doubt about the reality of the specialist’s decision.
- **Believable:** The evidence should be understandable and believable to the jury.

Rule 103: Rule of evidence

1. Maintaining a claim of error.
2. No renewal of objection or proof.
3. Aim an offer of proof.
4. Plain error taken as notice.

Evidence collection should also be performed to ensure that it will withstand legal proceedings. Key criteria for handling such evidence are as outlined as follows:

1. The proper protocol should be followed for acquisition of the evidence irrespective of whether it physical or digital. Gentle handling should be exercised for those situations where the device may be damaged(eg. Dropped or wet).
2. Special handling may be required for some situations. For example, when the device is actively destroying data through disk formatting, it may need to be shut down immediately to preserve the evidence. On the other hand, in some situations, it would not be appropriate to shut down the device so that the digital forensics expert can examine the device’s temporary memory.
3. All artifacts, physical and/or digital should be collected, retained and transferred using a preserved chain of custody.
4. All materials should be date and time stamped, identifying who collected the evidence and the location it is being transported to after initial collection.
5. Proper logs should be maintained when transferring possession.
6. When storing evidence, suitable access controls should be implemented and tracked to certify the evidence has only been accessed by authorized individual.

4.3 Characteristics of Digital Evidence:

Characteristics of digital evidences can help and challenge investigators during an investigation. The main goals in any investigation are to follow the trails that offenders leave during the commission of a crime and to tie perpetrators to the victims and crime scenes. Although witnesses may identify a suspect, tangible evidence of an individual's involvement is usually more compelling and reliable. Forensic analysts are employed to uncover compelling links between the offender, victim, and crime scene.

1. Locard's Exchange Principle:

According to Edmond Locard's principle, when two items make contact, there will be an interchange. The Locard principle is often cited in forensic sciences and is relevant in digital forensics investigations.

When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint evidence from the scene. This alteration is known as the Locard exchange principle. Many methods have been suggested in conventional forensic sciences to strongly prosecute criminals. Techniques used consists of blood analysis, DNA matching and fingerprint verification. These techniques are used to certify the existence of a suspected person at a physical scene. Based on this principle, Culley suggests that where there is a communication with a computer system, clues will be left.

According to Locard's Exchange Principle, contact between two items will result in an exchange. This principle applies to any contact at a crime scene, including between an offender and victim, between a person with a weapon, and between people and the crime scene itself. In short, there will always be evidence of the interaction, although in some cases it may not be detected easily (note that absence of evidence is not evidence of absence). This transfer occurs in both the physical and digital realms and can provide links between them as depicted in Figure 1. In the physical world, an offender might inadvertently leave fingerprints or hair at the scene and take a fiber from the scene. For instance, in a homicide case the offender may attempt to misdirect investigators by creating a suicide note on the victim's computer, and in the process leave fingerprints on the keyboard. With one such piece of evidence, investigators can demonstrate the strong possibility that the offender was at the crime scene. With two pieces of evidence the link between the offender and crime scene becomes stronger and easier to demonstrate. Digital evidence can reveal communications between suspects and the victim, online activities at key times, and other information that provides a digital dimension to the investigation.

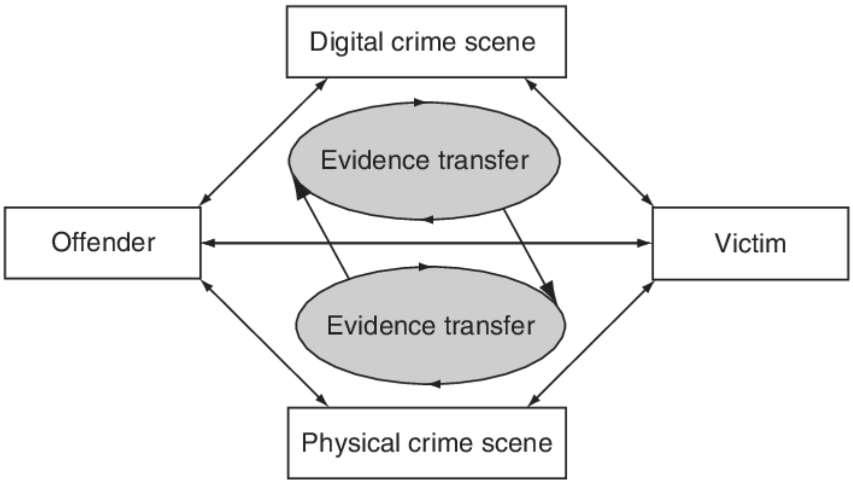


Fig.4.1: Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes.

In computer intrusions, the attackers will leave multiple traces of their presence throughout the environment, including in the file systems, registry, system logs, and network-level logs. Furthermore, the attackers could transfer elements of the crime scene back with them, such as stolen user passwords or PII in a file or database. Such evidence can be useful to link an individual to an intrusion.

In an e-mail harassment case, the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces. The Web browser used to send messages will store files, links, and other information on the sender's hard drive along with date-time–related information. Therefore, forensic analysts may find an abundance of information relating to the sent message on the offender's hard drive, including the original message contents. Additionally, investigators may be able to obtain related information from Hotmail, including Web server access logs, IP addresses, and possibly the entire message in the sent mail folder of the offender's e-mail account.

2. Digital Stream of Bits :

Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays to display the information. The information in continuous bits will rarely make scene and tools are needed to show these structures logically so that it is readable.

The circumstance in which digital evidence are found also helps the investigator during the inspection. Metadata is used to portray data more specifically and is helpful in determining the background of digital evidence.

4.4 Types of Evidences:

There are many types of Evidences, each with their own specific or unique characteristics. Some major types of evidences are :

1. Illustrative evidence: Illustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is common form of proof. For example , photographs , videos , sound recordings , X-rays , maps , drawing , graphs , charts , simulations , sculptors , and model.

2. Electronic Evidence: Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased .The evidences or proof that can be obtained from the electronic source is called the digital evidence.(viz. Email , hard drives etc.)

3. Documented Evidence: Documented evidence is same as demonstrative evidence. However, in documentary evidence , the proof is presented in writing (Viz. Contracts , wills , invoices etc.).

4. Explainable Evidence: This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case. It is also referred to as exculpatory.

5. Substantial Evidence: A proof that is introduced in the form of a physical object, whether whole or in part is referred to as substantial evidence. It is also called as physical evidence.

Such evidence might consist of dried blood, fingerprint, and DNA samples, casts of footprints or tries at the scene of crime.

6. Testimonial: It is the kind of evidence spoken by the spectator under the oath , or written evidence given under the oath by an official declaration that is affidavit. This is the common forms of evidence in the system.

4.5 Challenges in Evidence handling:

While responding to a computer security incident, a failure to adequately document is one of the most common mistakes made by computer security professional's .Analytical data might never be collected, critical data may be lost or data's origin or meaning may become unknown. As there are many evidences collected based on technical complexity is the fact that the properly retrieved evidence requires a paper trial.

Such documentations give an impression of having a certain quality against the natural instincts of the technical practical knowledge of individuals, who often investigate computer security incidents.

The challenges faced in the evidence handling must be properly understood by all the investigators. They should also understand how to meet these challenges. Therefore, it is essential for every organization to have formal evidence handling procedures that support computer security investigation. The most difficult task for an evidence handler is to substantiate the collected evidence at the judicial proceedings. Maintaining the chain of custody is also necessary. You must have both power and skill to validate your evidence.

4.5.1 Authentication of Evidence:

The laws of many state jurisdictions define data as Written Works and Record keeping .Before introducing them as evidence, documents and recorded material must be authenticated.

The evidence that are collected by any person/investigator should be collected using authenticate methods and techniques because during court proceedings these will become major evidences to prove the crime. In other words, for providing a piece of evidence of the testimony, it is necessary to have an authenticated evidence by a spectator who has a personal knowledge to its origin.

For an evidence to be admissible, it is necessary that it should be authenticated, otherwise the information cannot be presented to judging only. The matter of record is that the evidence collected by any person should meet the demand of authentication. The evidence collected must have some sort of internal documentation that records the manner of collected information.

4.5.2 Chain of Custody:

What Is the Chain of Custody in Computer Forensics?

The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It indicates the collection, sequence of control, transfer, and analysis. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Why Is It Important to Maintain the Chain of Custody?

It is important to maintain the chain of custody to preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible.

Importance to the Examiner:

Suppose that, as the examiner, you obtain metadata for a piece of evidence. However, you are unable to extract meaningful information from it. The fact that there is no meaningful information within the metadata does not mean that the evidence is insufficient. The chain of custody in this case helps show where the possible evidence might lie, where it came from, who created it, and the type of equipment that was used. That way, if you want to create an exemplar, you can get that equipment, create the exemplar, and compare it to the evidence to confirm the evidence properties.

Importance to the Court:

It is possible to have the evidence presented in court dismissed if there is a missing link in the chain of custody. It is therefore important to ensure that a wholesome and meaningful chain of custody is presented along with the evidence at the court.

What Is the Procedure to Establish the Chain of Custody?

In order to ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that, the more information a forensic expert obtains concerning the evidence at hand, the more authentic is the created chain of custody. Due to this, it is important to obtain administrator information about the evidence: for instance, the administrative log, date and file info, and who accessed the files. You should ensure the following procedure is followed according to the chain of custody for electronic evidence:

- **Save the original materials:** You should always work on copies of the digital evidence as opposed to the original. This ensures that you are able to compare your work products to the original that you preserved unmodified.
- **Take photos of physical evidence**: Photos of physical (electronic) evidence establish the chain of custody and make it more authentic.
- **Take screenshots of digital evidence content:** In cases where the evidence is intangible, taking screenshots is an effective way of establishing the chain of custody.
- **Document date, time, and any other information of receipt**. Recording the timestamps of whoever has had the evidence allows investigators to build a reliable timeline of where the evidence was prior to being obtained. In the event that there is a hole in the timeline, further investigation may be necessary.
- **Inject a bit-for-bit clone of digital evidence content into our forensic computers.** This ensures that we obtain a complete duplicate of the digital evidence in question.
- **Perform a hash test analysis to further authenticate the working clone**. Performing a hash test ensures that the data we obtain from the previous bit-by-bit copy procedure

is not corrupt and reflects the true nature of the original evidence. If this is not the case, then the forensic analysis may be flawed and may result in problems, thus rendering the copy non-authentic.

The procedure of the chain of custody might be different. depending on the jurisdiction in which the evidence resides; however, the steps are largely identical to the ones outlined above.

What Considerations Are Involved with Digital Evidence?

A couple of considerations are involved when dealing with digital evidence. We shall take a look at the most common and discuss globally accepted best practices.

1. **Never work with the original evidence to develop procedures:** The biggest consideration with digital evidence is that the forensic expert has to make a complete copy of the evidence for forensic analysis. This cannot be overlooked because, when errors are made to working copies or comparisons are required, it will be necessary to compare the original and copies.
2. **Use clean collecting media:** It is important to ensure that the examiner's storage device is forensically clean when acquiring the evidence. This prevents the original copies from damage. Think of a situation where the examiner's data evidence collecting media is infected by malware. If the malware escapes into the machine being examined, all of the evidence can become compromised.
3. **Document any extra scope:** During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. It is recommended that this information be documented and brought to the attention of the case agent because the information may be needed to obtain additional search authorities. A comprehensive report must contain the following sections:
   - Identity of the reporting agency
   - Case identifier or submission number
   - Case investigator
   - Identity of the submitter
   - Date of receipt
   - Date of report
   - Descriptive list of items submitted for examination, including serial number, make, and model
   - Identity and signature of the examiner
   - Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files
   - Results/conclusions
4. **Consider safety of personnel at the scene**. It is advisable to always ensure the scene is properly secured before and during the search. In some cases, the examiner may only have the opportunity to do the following while onsite:
   - Identify the number and type of computers.
   - Determine if a network is present.
   - Interview the system administrator and users.

- Identify and document the types and volume of media, including removable media.
- Document the location from which the media was removed.
- Identify offsite storage areas and/or remote computing locations.
- Identify proprietary software.
- Determine the operating system in question.

The considerations above need to be taken into account when dealing with digital evidence due to the fragile nature of the task at hand.

Chain of custody prevents evidence from being tainted; it thus establishes trustworthiness of items brought into evidence. The U.S. legal system wants the proponent of evidence to be able to demonstrate an unbroken chain of custody for items, he wants to have admitted.

Often, there is a stipulation,for example, when there is an agreement between the parties or a concession by the opponent of the evidence that allows it to be admitted without requiring testimony to prove the foundational elements. The purpose of stipulation is to move the trial quickly forward, without pondering idle questions.

If there is a break in the chain of custody brought to the attention of the court, then the court has to decide whether the breach is so severe as to meet exclusion of the item from trial. Alternatively, the court can decide that the Trier (trial judge or jury) need to decide the value of the evidence. To prevent a breach, a forensic investigation should follow a written policy, so that necessary deviations of the policy can be argued. The policy itself should take all reasonable (or arguably reasonable) precautions against tampering.

For example, assume that a PDA is seized from a suspected drug dealer. In the case of an PDA, there is no hard drive image to mirror, that is, the examination will have to be done on the powered-on original. The PDA can lose data, for example by disconnecting it from its battery. On seizure, the device should not be switched on. If it is seized switched on, it should be switched off in order to preserve battery power. It needs to be put into an evidence bag that does not allow access to the PDA without breaking the seal (no clear plastic bag!). The evidence needs to be tagged with all pertinent data, including the serial number of the PDA and the circumstances of the seizure. The PDA should never be returned to the accused at the scene, because the device can lose data if reset. To maintain the data in the PDA, it needs to be kept in a continuously charged mode. It should only be used to extract evidence by a competent person who can testify in court. As long as the PDA could be evidence, it needs to be kept in an evidence locker, with check-out logs, so that it can be determined who had access to the PDA at any time.

4.5.3 Evidence Validation: The challenge is to ensure that providing or obtaining the data that you have collected is similar to the data provided or presented in court. Several years pass between the collection of evidence and the production of evidence at a judiciary proceeding, which is very common. To meet the challenge of validation, it is necessary to ensure that the original media matches the forensic duplication by using MD5 hashes. The evidence for every file is nothing but the MD5 hash values that are generated for every file that contributes to the case.

The verify function within the Encase application can be used while duplicating a hard drive with Encase. To perform a forensic duplication using dd , you must record MD5 hash for both the original evidence media and binary files or the files which compose the forensic duplication.

Note: Evidence collection calculated by MD5 after 6 months may not be helpful.MD5 hashes should be performed when the evidence is obtained.

4.6 Volatile Evidence: Not all the evidence on a system is going to last very long. Some evidence is residing in storage that requires a consistent power supply; other evidence may be stored in information that is continuously changing. When collecting evidence, you should always try to proceed from the most volatile to the least. Of course, you should still take the individual circumstances into account—you shouldn't waste time extracting information from an unimportant/unaffected machine's main memory when an important or affected machine's secondary memory hasn't been examined.

You need to respond to the target system at the console during the collection of volatile data rather than access it over the network. This way the possibility of the attacker monitoring your responses is eliminated, ensuring that you are running trust commands. If you are creating a forensic duplication of the targeted system, you should focus on obtaining the volatile system data before shutting down the system.

To determine what evidence to collect first, you should draw up an Order of Volatility—a list of evidence sources ordered by relative volatility. An example an Order of Volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

Note: Once you have collected the raw data from volatile sources you may be able to shutdown the system.{Matthew Braid, "Collecting Electronic Evidence After A System Compromise," Australian Computer Emergency Response Team}

Registers, Cache: The contents of CPU cache and registers are extremely volatile, since they are changing all of the time. Literally, nanoseconds make the difference here. An examiner needs to get to the cache and register immediately and extract that evidence before it is lost.
Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory: Some of these items, like the routing table and the process table, have data located on network devices. In other words, that data can change quickly while the system is in operation, so evidence must be gathered quickly. Also, kernel statistics are moving back and forth between cache and main memory, which make them highly volatile. Finally, the information located on random access memory (RAM) can be lost if there is a power spike or if power goes out. Clearly, that information must be obtained quickly.

Temporary File Systems: Even though the contents of temporary file systems have the potential to become an important part of future legal proceedings, the volatility concern is not as high here. Temporary file systems usually stick around for awhile.

Disk: Even though we think that the data we place on a disk will be around forever, that is not always the case (see the SSD Forensic Analysis post from June 21). However, the likelihood that data on a disk cannot be extracted is very low.

Remote Logging and Monitoring Data that is Relevant to the System in Question: The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital. So, even though the volatility of the data is higher here, we still want that hard drive data first.

Physical Configuration, Network Topology, and Archival Media: Here we have items that are either not that vital in terms of the data or are not at all volatile. The physical configuration and network topology is information that could help an investigation, but is likely not going to have a tremendous impact. Finally, archived data is usually going to be located on a DVD or tape, so it isn’t going anywhere anytime soon. It is great digital evidence to gather, but it is not volatile.

4.7 Case Studies:

Case-1: Credit Card Fraud

State	:	Tamil Nadu
City	:	Chennai
Sections of Law	:	Section of Law: 66 of Information Technology Act
		2000 & 120(B), 420,467,468,471 IPC.

Background:

The assistant manager (the complainant) with the fraud control unit of a large business process outsourcing (BPO) organization filed a complaint alleging that two of its employees had conspired with a credit card holder to manipulate the credit limit and as a result cheated the company of INR 0.72 million.

The BPO facility had about 350 employees. Their primary function was to issue the bank's credit cards as well as attend to customer and merchant queries. Each employee was assigned to a specific task and was only allowed to access the computer system for that specific task. The employees were not allowed to make any changes in the credit-card holder's account unless they received specific approvals.

Each of the employees was given a unique individual password. In case they entered an incorrect password three consecutive times then their password would get blocked and they would be issued a temporary password.

The company suspected that its employees conspired with the son (holding an add-on card) of one of the credit card holders. The modus operandi suspected by the client is as follows.

The BPO employee deliberately keyed in the wrong password three consecutive times (so that his password would get blocked) and obtained a temporary password to access the computer system. He manually reversed the transactions of the card so that it appeared that payment for the transaction has taken place. The suspect also changed the credit card holder's address so that the statement of account would never be delivered to the primary card holder.

Investigation: A procedure to find the Digital Evidence

The investigating team visited the premises of the BPO and conducted detailed examination of various persons to understand the computer system used. They learnt that in certain situations the system allowed the user to increase the financial limits placed on a credit card. The system also allowed the user to change the customer's address, blocking and unblocking of the address, authorisations for cash transactions etc.

The team analysed the attendance register which showed that the accused was present at all the times when the fraudulent entries had been entered in the system. They also analysed the system logs that showed that the accuser's ID had been used to make the changes in the system.

The team also visited the merchant establishments from where some of the transactions had taken place. The owners of these establishments identified the holder of the add-on card.

Current status: The BPO was informed of the security lapse in the software utilised. Armed with this evidence the investigating team arrested all the accused and recovered, on their confession, six mobile phones, costly imported wrist watches, jewels, electronic items, leather accessories, credit cards, all worth INR 0. 3 million and cash INR 25000. The investigating team informed the company of the security lapses in their software so that instances like this could be avoided in the future.

This case won the second runner-up position for the India Cyber Cop Award, for its investigating officer Mr S. Balu, Assistant Commissioner of Police, Crime, Chennai Police. The case was remarkable for the excellent understanding displayed by the investigating team, of the business processes and its use in collecting digital evidence.

Case-2: Hosting Obscene Profiles

State	:	Tamil Nadu
City	:	Chennai
Sections of Law	:	67 of Information Technology
		Act 2000 469, 509 of the Indian Penal code

Background: The complainant stated that some unknown person had created an e-mail ID using her name and had used this ID to post messages on five Web pages describing her as a call-girl along with her contact numbers.

As a result she started receiving a lot of offending calls from men.

Investigation: A procedure to find the Digital Evidence
After the complainant heard about the Web pages with her contact details, she created a username to access and view these pages.

Using the same log-in details, the investigating team accessed the Web pages where these profiles were uploaded. The message had been posted on five groups, one of which was a public group. The investigating team obtained the access logs of the public group and the message to identify the IP addresses used to post the message. Two IP addresses were identified.

The ISP was identified with the help of publicly available Internet sites. A request was made to the ISPs to provide the details of the computer with the IP addresses at the time the messages were posted. They provided the names and addresses of two cyber cafes located in Mumbai to the police.

The investigating team scrutinised the registers maintained by the cyber cafes and found that in one case the complainant's name had been signed into the register.

The team also cross-examined the complainant in great detail. During one of the meetings she revealed that she had refused a former college mate who had proposed marriage.

In view of the above the former college mate became the prime suspect. Using this information the investigating team, with the help of Mumbai police, arrested the suspect and seized a mobile phone from him. After the forensic examination of the SIM card and the phone, it was observed that phone had the complainant's telephone number that was posted on the internet. The owner of the cyber cafes also identified the suspect as the one who had visited the cyber cafes.

Based on the facts available with the police and the sustained interrogation the suspect confessed to the crime.

Current status: The suspect was convicted of the crime and sentenced to two years of imprisonment as well as a fine.

Case - 3: Illegal money transfer

State	:	Maharashtra
City	:	Pune
Sections of Law	:	467,468, 471, 379,419, 420, 34 of IPC & 66 of IT ACT

Background: The accused in the case were working in a BPO, that was handling the business of a multinational bank. The accused, during the course of their work had obtained the personal identification numbers (PIN) and other confidential information of the bank's customers. Using these the accused and their accomplices, through different cyber cafes, transferred huge sums of money from the accounts of different customers to fake accounts.

Investigation: A procedure to find the Digital Evidence

On receiving the complaint the entire business process of the complainant firm was studied and a systems analysis was conducted to establish the possible source of the data theft.

The investigators were successful in arresting two people as they laid a trap in a local bank where the accused had fake accounts for illegally transferring money.

During the investigation the system server logs of the BPO were collected. The IP addresses were traced to the Internet service provider and ultimately to the cyber cafes through which illegal transfers were made.

The registers maintained in cyber cafes and the owners of cyber cafes assisted in identifying the other accused in the case. The e-mail IDs and phone call print outs were also procured and studied to establish the identity of the accused. The e-mail accounts of the arrested accused were scanned which revealed vital information to identify the other accused. Some e-mail accounts of the accused contained swift codes, which were required for internet money transfer.

All the 17 accused in the case were arrested in a short span of time. The charge sheet was submitted in the court within the stipulated time. In the entire wire transfer scam, an amount to the tune of about INR 19 million was transferred, out of this INR 9 million was blocked in transit due to timely intimation by police, INR 2 million was held in balance in one of the bank accounts opened by the accused which was frozen. In addition the police recovered cash, ornaments, vehicles and other articles amounting to INR 3 million.

During the investigation the investigating officer learned the process of wire transfer, the banking procedures and weakness in the system. The investigating officer suggested measures to rectify the weakness in the present security systems of the call centre. This has helped the local BPO industry in taking appropriate security measures.

Current status: Pending trial in the court.

This case won the India Cyber Cop Award, for its investigating officer Mr Sanjay Jadhav, Assistant Commissioner of Police, Crime, Pune Police. The panel of judges felt that this case was the most significant one for the Indian IT industry during 2005 and was investigated in a professional manner, with substantial portion of the swindled funds being immobilised, a large number of persons were arrested and the case was sent to the court for trial within 90 days.

Case-4: Fake Travel Agent

State	:	Maharashtra
City	:	Mumbai
Sections of Law	:	420, 465, 467, 468, 471, 34 of IPC r/w 143 of Indian Railway Act 1989.

Background: The accused in this case was posing to be a genuine railway ticket agent and had been purchasing tickets online by using stolen credit cards of non residents. The accused created fraudulent electronic records/ profiles, which he used to carry out the transactions.The tickets so purchased were sold for cash to other passengers. Such events occurred for a period of about four months.

The online ticket booking service provider took notice of this and lodged a complaint with the cyber crime investigation cell.

Investigation: A procedure to find the Digital Evidence

The service provider gave the IP addresses, which were used for the fraudulent online bookings, to the investigating team. IP addresses were traced to cyber cafes in two locations.

The investigating team visited the cyber cafŽs but was not able to get the desired logs as they were not maintained by the cyber cafŽ owners. The investigating team was able to short list the persons present at cyber cafes when the bookings were made. The respective owners of the cyber cafes were able to identify two persons who would regularly book railway tickets.

The investigating team then examined the passengers who had travelled on these tickets. They stated that they had received the tickets from the accused and identified the delivery boy who delivered the tickets to them. On the basis of this evidence the investigating team arrested two persons who were identified in an identification parade.

Current status: The charge sheet has been submitted in the court.

Case-5: Creating Fake Profile

State	:	Andhra Pradesh
City	:	Hyderabad
Sections of Law	:	67 Information Technology Act 2000 507, 509 of the Indian Penal Code

Background: The complainant received an obscene e-mail from an unknown e-mail ID. The complainant also noticed that obscene profiles along with photographs of his daughter had been uploaded on matrimonial sites.

Investigation: A procedure to find the Digital Evidence

The investigating officer examined and recorded the statements of the complainant and his daughter. The complainant stated that his daughter was divorced and her husband had developed a grudge against them due to the failure of the marriage.

The investigating officer took the original e-mail from the complainant and extracted the IP address of the same. From the IP address he could ascertain the Internet service provider.

The IP address was traced to a cable Internet service provider in the city area of Hyderabad. The said IP address was allotted to the former husband sometime back and his house was traced with the help of the staff of ISP.

A search warrant was obtained and the house of the accused was searched. During the search operation, a desktop computer and a handicam were seized from the premises. A forensic IT specialist assisted the investigation officer in recovering e-mails (which were sent to the complainant), using a specialised disk search tool as well as photographs (which had been posted on the Internet) from the computer and the handicam respectively. The seized computer and the handicam were sent to the forensic security laboratory for further analysis.

The experts of the forensic security laboratory analysed the material and issued a report stating that: the hard disk of the seized computer contained text that was identical to that of the obscene e-mail; the computer had been used to access the matrimonial websites on which the obscene profiles were posted; the computer had been used to access the e-mail account that was used to send the obscene e-mail; the handicam seized from the accused contained images identical to the ones posted on the matrimonial Websites. Based on the report of the FSL it was clearly established that the accused had: created a fictitious e-mail ID and had sent the obscene e-mail to the complainant; posted the profiles of the victim along with her photographs on the matrimonial sites.

Current status: Based on the material and oral evidence, a charge sheet has been filed against the accused and the case is currently pending for trial.

References

1. http://www.forensicsciencesimplified.org/digital/
2. http://www.forensicsciencesimplified.org/digital/
3. https://www.helpnetsecurity.com/2007/07/20/the-rules-for-computer-forensics/ as on 28 August 2019
4. Digital Evidence and Computer Crime, Third Edition © 2011 Eoghan Casey. Published by Elsevier Inc.
5. www.cse.scu.edu/~tschwarz/COEN252_13/LN/legalissues.html

Sample Multiple Choice Questions

1. The digital evidence are used to establish a credible link between____
   a. Attacker and victim and the crime scene
   b. Attacker and the crime scene
   c. victim and the crime scene
   d. Attacker and Information

2. Digital evidences must follow the requirements of the ______________.
   a. Ideal Evidence rule
   b. Best Evidence Rule
   c. Exchange Rule
   d. All of the mentioned

3. From the two given statements 1 and 2 , select the correct options from a-d.
   1): Original media can be used to carry out digital investigation process.
   2): By default, every part of the victim’s computer is considered unreliable.
   a. a and b both are true
   b. a is true and b is false
   c. a and b both are false
   d. a is false and b is true

4. The evidences or proof that can be obtained from the electronic source is called the_______
   a. digital evidence
   b. demonstrative evidence
   c. Explainable Evidence
   d. substantial evidence

5. Which of the following is not a type of volatile evidence?
   a. Routing Tables
   b. Main Memory
   c. Log files
   d. Cached Data

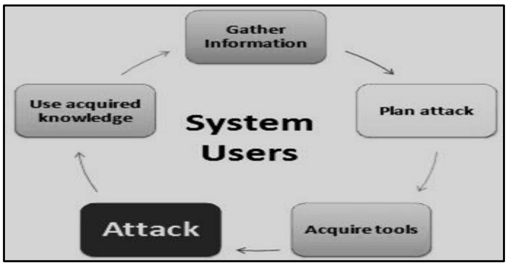
Unit-5 Basics of Hacking

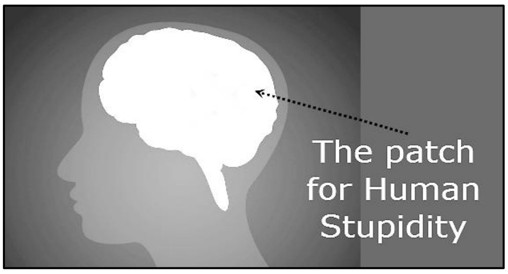
Contents

5.1 Ethical Hacking: History

Hacking developed alongside "Phone Phreaking", a term referred to exploration of the phone network without authorization, and there has often been overlap between both technology and participants.

Ethical hacking is the science of testing computers and network for security vulnerabilities and plugging the holes found before the unauthorized people get a chance to exploit them.





Social Engineering Cycle **Social Engineering Counter Measures**

Fig. 5.1

- **Gather Information**: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.
- **Plan Attack**: The attackers outline how he/she intends to execute the attack
- **Acquire Tools**: These include computer programs that an attacker will use when launching the attack.
- **Attack**: Exploit the weaknesses in the target system.
- **Use acquired knowledge**: Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

Most techniques employed by social engineers involve manipulating human biases. To counter such techniques, an organization can;

- ✓ **To counter the familiarity exploit**
- ✓ **To counter intimidating circumstances attacks**
- ✓ **To counter phishing techniques**
- ✓ **To counter tailgating attacks**
- ✓ **To counter human curiosity**
- ✓ **To counter techniques that exploit human greed**

Summary

- Social engineering is the art of exploiting the human elements to gain access to un-authorized resources.
- Social engineers use a number of techniques to fool the users into revealing sensitive information.
- Organizations must have security policies that have social engineering countermeasures.

Hacker's attitude:

A hacker-cracker separation give more emphasis to a range of different categories, such as white hat (ethical hacking), grey hat, black hat and script kiddie. The term cracker refer to black hat hackers, or more generally hackers with unlawful intentions.

Hackers are problem solvers. They get extract from understanding a problem and sorting out a solution. Their motivation to meet challenges is internal. Hackers do what they do because it's extremely satisfying to solve puzzles and fix the up-until-now unfixable. The pleasure derived is both intellectual and practical but one don't have to be a geek to be a hacker. Being a hacker is a mind-set. In Raymond's dissertation, "How to Become a Hacker", he describes the fundamentals of a hacker attitude.

These are very same principles apply to being innovative which are explained as below:

The world is full of fascinating problems waiting to be solved.

Innovation happens because hackers like to solve the problem rather than complaining. If one happen to find these problems fascinating and exciting, then it won't even feel like hard work.

No Problem should ever have to be solved twice.

Hackers are perfectionists for clarifying the problem before they start generating ideas. It's easy to jump to solutions, but sometimes that means wrong problems are solved. A little bit of accuracy on the front end of a problem solving process means one tackles the right and real problem, so one only have to do it once.

Boredom and drudgery (more and more work) are evil.

The best way to lose touch with innovation is to become too repetitive. Innovation requires constant and vigilant creativity. It may not be broken enough to fix, but there's no reason not to squeeze it and cut boredom off at the pass.

Freedom is good.

Hackers need freedom to work upon their ideas.

Attitude is no substitute for competence.

They are open-minded and they see problems as interesting opportunities. Innovators are seeking to understand a problem more deeply, puzzling at how an unworkable idea might become workable, increasing their skill set so that they are better problem solvers and can better execute their ideas.

Hackers are the innovators of the Internet. Overall hackers are who have got that relentless, curious, problem-solving attitude.

Computer Hacking

Computer Hackers have been in existence for more than a century. Originally, "hacker" did not carry the negative implications. In the late 1950s and early 1960s, computers were much different than the desktop or laptop systems most people are familiar with. In those days, most companies and universities used mainframe computers: giant, slow-moving hunks of metal locked away in temperature-controlled glass cages. It cost thousands of dollars to maintain and operate those machines, and programmers had to fight for access time.

Because of the time and money involved, computer programmers began looking for ways to get the most out of the machines. The best and brightest of those programmers created what they called "hacks" - shortcuts that would modify and improve the performance of a computer's operating system or applications and allow more tasks to be completed in a shorter time.

Still, for all the negative things hackers have done, they provide a necessary (and even valuable) service, which is elaborated on after a brief timeline in the history of computer hacking

- **How Hackers Beget Ethical Hackers**

  Hacker is a word that has two meanings:

- ✓ Traditionally, a hacker is someone who likes to tamper with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.
- ✓ Recently, hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

The good-guy (white-hat) hackers don't like being in the same category as the bad-guy (black-hat) hackers. Whatever the case, most people give hacker a negative meaning. Many malicious hackers claim that they don't cause damage but instead are selflessly helping others. In other words, many malicious hackers are electronic thieves.

Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases their status in hacker circles.

If one need protection from hacker troubles; one has to become as savvy as the guys trying to attack systems. A true security assessment professional possesses the skills, mind-set, and tools of a hacker but is also trustworthy. He or she performs the hacks as security tests against systems based on how hackers might work.

Ethical hacker's attitude encompasses formal and methodical penetration testing, white hat hacking, and vulnerability testing ,which involves the same tools, tricks, and techniques that criminal hackers use, but with one major difference: Ethical hacking is performed with the target's permission in a professional setting.

The intent of ethical hacking is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems. Ethical hacking is part of an overall information risk management program that allows for on-going security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are genuine.

Ethical hacking versus auditing

Many people confuse security testing via the ethical hacking approach with security auditing, but there are big differences, namely in the objectives.

Security auditing involves comparing a company's security policies (or compliance requirements) to what's actually taking place. The intent of security auditing is to validate that security controls exist using a risk-based approach.

Auditing often involves reviewing business processes and, in many cases, might not be very technical. Security audits are usually based on checklists.

Equally, security assessments based around ethical hacking focus on vulnerabilities that can be exploited. This testing approach validates that security controls do not exist or are incompetent at best.

Ethical hacking can be both highly technical and nontechnical, and although one can use a formal methodology, it tends to be a bit less structured than formal auditing.

Policy considerations

If it is chosen to make ethical hacking an important part of business's information risk management program, one really need to have a documented security testing policy. Such a policy outlines who's doing the testing, the general type of testing that is performed, and how often the testing takes place.

What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.

Example of Hacking:

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses.

- ✓ Using password cracking algorithm to gain access to a system.
- ✓ This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.
- ✓ Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming up with countermeasures that protect the weaknesses.

Ethical hacking is a branch of information security or information assurance which tests an organization's information systems against a variety of attacks. Ethical hackers are also sometimes known as **White Hats.**

Many people are confused when the terms "Ethical" and "Hacking" are used together. Usually the term "hacker" has a negative connotation due to media reports using incorrect terminology.

Ethical hackers must abide by the following rules:

- ✓ Get **written permission** from the owner of the computer system and/or computer network before hacking.
- ✓ **Protect the privacy of the organization** been hacked.
- ✓ **Transparently report** all the identified weaknesses in the computer system to the organization.
- ✓ **Inform** hardware and software vendors of the **identified weaknesses**.

Definition

Ethical hacking:

- ✓ Refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers.
- ✓ known as **penetration testing, intrusion testing**, or **red teaming.**

An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems.

By conducting penetration tests, an ethical hacker looks to answer the following four basic questions:

1. What information/locations/systems can an attacker gain access?
2. What can an attacker see on the target?
3. What can an attacker do with available information?
4. Does anyone at the target system notice the attempts?

An ethical hacker operates with the knowledge and permission of the organization for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

Defining hacker, Malicious users

Definition of Hacker: A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

An **Ethical Hacker**, also known as a whitehat hacker, or simply a whitehat, is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems.

Nowadays, certified ethical hackers are among the most sought after information security employees in large organizations such as Wipro, Infosys, IBM, Airtel and Reliance among others.

What Is a Malicious User?

Malicious users (or internal attackers) try to compromise computers and sensitive information from the inside as authorized and “trusted” users. Malicious users go for systems they believe they can compromise for fraudulent gains or revenge.

- ✓ Malicious attackers are, generally known as both, hackers and malicious users.
- ✓ Malicious user means a rogue employee, contractor, intern, or other user who abuses his or her trusted privileges .It is a common term in security circles.

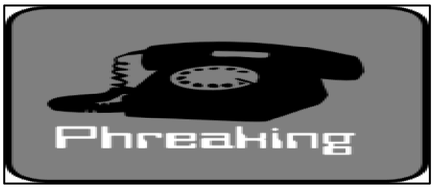
Users search through critical database systems to collect sensitive information, e-mail confidential client information to the competition or elsewhere to the cloud, or delete sensitive files from servers that they probably do not have access.

There’s also the occasional ignorant insider whose intent is not malicious but who still causes security problems by moving, deleting, or corrupting sensitive information. Even an innocent “fat-finger” on the keyboard can have terrible consequences in the business world.

Malicious users are often the worst enemies of IT and information security professionals because they know exactly where to go to get the goods and don’t need to be computer savvy to compromise sensitive information. These users have the access they need and the management trusts them, often without question. In short they take the undue advantage of the trust of the management.

Hackers are classified according to the intent of their actions.

Table 5.1 Classifications of hackers according to their intent.

Symbol	Description
	Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	Script kiddies: A non-skilled person who gains access to computer systems using already made tools.
Knowledge Is Free. We Are Anonymous. We Are Legion. We Do Not Forgive. We Do Not Forget. Expect Us.	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
	**Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secured can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated as above. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

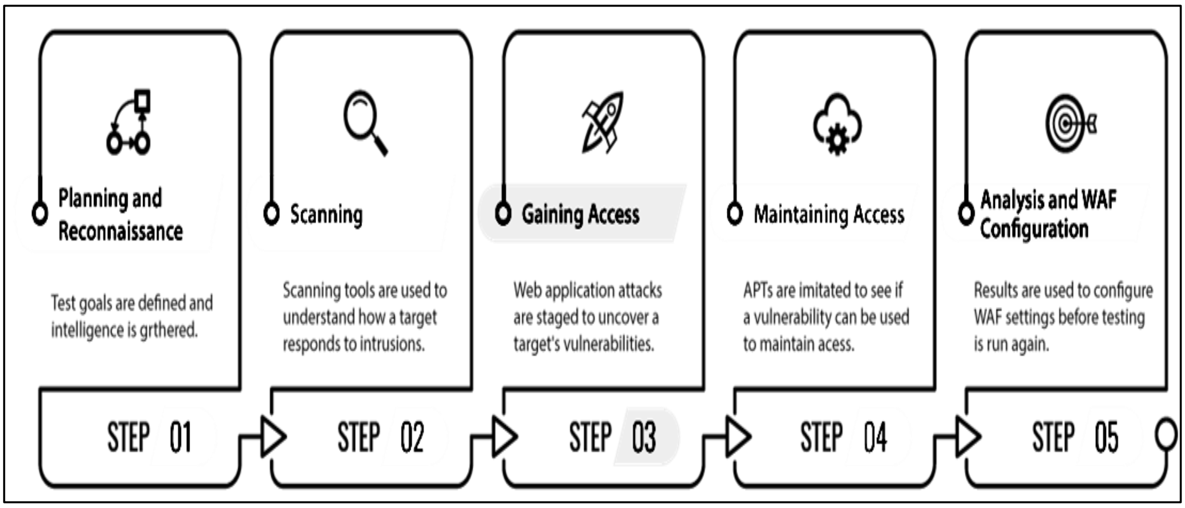

Planning and Reconnaissance
Test goals are defined and intelligence is grthered.
STEP 01
Scanning
Scanning tools are used to understand how a target responds to intrusions.
STEP 02
Gaining Access
Web application attacks are staged to uncover a target's vulnerabilities.
STEP 03
Maintaining Access
APTs are imitated to see if a vulnerability can be used to maintain acess.
STEP 04
Analysis and WAF Configuration
Results are used to configure WAF settings before testing is run again.
STEP 05

Fig. 5.2 Penetration Testing Stages

5.2 Understanding the need to hack your own systems

To catch a thief, think like a thief. That's the basis for ethical hacking.

The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting your systems from the bad guys and not just the generic vulnerabilities that everyone knows about is absolutely critical. When the hacker tricks are known, one can see how vulnerable the systems are.

Hacking targets on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPNs) can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking your own systems to discover vulnerabilities is a step to making them more secure.

This is the only proven method of greatly hardening your systems from attack. If weaknesses are not identified, it's a matter of time before the vulnerabilities are exploited.

As hackers expand their knowledge, one should also gain the required knowledge of it. You must think like them to protect your systems from them. As the ethical hacker, one must know activities hackers carry out and how to stop their efforts. One should know what to look for and how to use that information to spoil hackers' efforts.

One cannot protect the systems from everything. The only protection against everything is to unplug computer systems and lock them away so no one can touch them , not even you.

That's not the best approach to information security. What's important is to protect your systems from known vulnerabilities and common hacker attacks. It's impossible to support all possible vulnerabilities on all systems. One can't plan for all possible attacks, especially the ones that are currently unknown.

However, the more combinations you try — the more you test whole systems instead of individual units ,the better your chances of discovering vulnerabilities that affect everything as a whole.

Building the Foundation for Ethical Hacking

One should not forget about insider threats from malicious employees. One's overall goals as an ethical hacker should be as follows:

- ✓ Hack your systems in a non-destructive fashion.
- ✓ Enumerate vulnerabilities and, if necessary, prove to upper management that vulnerabilities exist.
- ✓ Apply results to remove vulnerabilities and better secure your systems.

5.3 Understanding the dangers your systems face

Systems are generally under fire from hackers around the world. It's another to understand specific attacks against your systems that are possible.

There are some well-known attacks. Many information-security vulnerabilities aren't critical by themselves. However, exploiting several vulnerabilities at the same time can take its toll.

For example, a default Windows OS configuration, a weak SQL Server administrator password, and a server hosted on a wireless network may not be major security concerns separately. But exploiting all three of these vulnerabilities at the same time can be a serious issue as:

- Nontechnical attacks
- Network-infrastructure attacks
- Operating-system attacks
- Application and other specialized attacks

- **Nontechnical attacks**

Exploits that involve manipulating people or end users and even yourself are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property. Physical attacks can include dumpster diving (searching through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

- **Network-infrastructure attacks**

Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet.

Here are some examples of network-infrastructure attacks:

- ✓ Connecting into a network through a rogue modem attached to a computer behind a firewall
- ✓ Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- ✓ Flooding a network with too many requests, creating a Denial of Service (DoS) for legitimate requests
- ✓ Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text
- ✓ Piggybacking onto a network through an insecure wireless configuration.

- **Operating-system attacks Hacking**

Operating Systems (OSs) is a preferred method of the bad guys(hackers). Operating systems comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them.

Occasionally, some operating systems that are more secure out of the box, such as Novell NetWare and the flavor's of BSD UNIX are attacked, and vulnerabilities turn up.

But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities.

Here are some examples of attacks on operating systems:

- ✓ Exploiting specific protocol implementations
- ✓ Attacking built-in authentication systems
- ✓ Breaking file-system security
- ✓ Cracking passwords and encryption mechanisms

- **Application and other specialized attacks**

Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down:

- ✓ Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.
- ✓ Malicious software (malware) includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.
- ✓ Spam (junk e-mail) is wreaking havoc on system availability and storage space. And it can carry malware. Ethical hacking helps reveal such attacks against computer systems.

5.4. Obeying the Ethical Hacking Commandments

Every ethical hacker must abide by a few basic commandments. If not, bad things can happen.

- **Working ethically**

The word ethical in this context can be defined as working with high professional morals and principles. While performing ethical hacking tests against own systems or for someone who has hired for, everything one need to do as an ethical hacker must be above board and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate principle. The misuse of information is absolutely forbidden. That's what the bad guys or hackers do.

- **Respecting privacy**

Treat the information gathered with the greatest respect. All information obtained during testing from Web-application log files to clear-text passwords must be kept private. This information shall not be used to watch into confidential corporate information or private lives. If you sense or feel that someone should know there's a problem, consider sharing that information with the appropriate manager.

Involve others in process. This is a "watch the watcher" system that can build trust and support ethical hacking projects.

- **Not crashing your systems**

One of the biggest mistakes seen when people try to hack their own systems is inadvertently crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.

DoS-Denial of Service conditions on the systems are easily created when testing. Running too many tests too quickly on a system causes many system lockups. Things should not be rushed and assumed that a network or specific host can handle the beating that network scanners and vulnerability assessment tools can be useless .

Many security-assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if one needs to run the tests on production systems during regular business hours. One can even create an account or system lockout condition by social engineering, changing a password, not realizing that doing so might create a system lockout condition.

5.5 The Ethical Hacking Process

Like practically any IT or security project, ethical hacking needs to be planned in advance. Strategic and tactical issues in the ethical hacking process should be determined and agreed upon. Planning is important for any amount of testing from a simple password-cracking test to an all-out penetration test on a Web application.

- **Formulating your plan**

Approval for ethical hacking is essential. What isbeing done should be known and visible at least to the decision makers. Obtaining sponsorship of the project is the first step. This could be the manager, an executive, a customer, or even the boss. Someone is needed to back up and sign off on the plan. Otherwise, testing may be called off unexpectedly if someone claims they never authorized one to perform the tests.

The authorization can be as simple as an internal memo from the senior-most person or boss if one is performing these tests on own systems. If the testing is for a customer, one should have a signed contract in place, stating the customer's support and authorization. Get written approval on this sponsorship as soon as possible to ensure that none of the time or effort is wasted. This documentation works as a proof as what one is doing when someone asks or demands.

A detailed plan is needed, but that doesn't mean that it needs volumes of testing procedures. One slip can crash your systems.

A **well-defined scope** includes the following information:

- ✓ Specific systems to be tested
- ✓ Risks that are involved
- ✓ When the tests are performed and your overall timeline
- ✓ How the tests are performed
- ✓ How much knowledge of the systems you have before you start testing
- ✓ What is done when a major vulnerability is discovered
- ✓ The specific deliverables — this includes security-assessment reports and a higher-level report outlining the general vulnerabilities to be addressed, along with countermeasures that should be implemented.
- ✓ When selecting systems to test, start with the most critical or vulnerable systems. For instance, one can test computer passwords or attempt social engineering attacks before drilling down into more detailed systems.

  What if one is assessing the firewall or Web application, and one takes it down? This can cause system unavailability, which can reduce system performance or employee productivity. Even worse, it could cause loss of data integrity, loss of data, and bad publicity.

  Handle social-engineering and denial-of-service attacks carefully. Determine how they can affect the systems you're testing and entire organization.

  Determining when the tests are performed is something that one must think long and hard about. Do the tester test during normal business hours? How about late at night or early in the morning so that production systems aren't affected? Involve others to make sure they approve tester's timing.

  The best approach is an unlimited attack, wherein any type of test is possible. The hackers aren't hacking the systems within a limited scope. Some exceptions to this approach are performing DoS, social engineering, and physical-security tests.

  One should not stop with one security hole. This can lead to a false sense of security. One should keep going to see what else he/she can discover. It's not like to keep hacking until the end of time or until one crash all his/ her systems. Simply pursue the path he/she is going down until he//she can't hack it any longer.

  One of the goals may be to perform the tests without being detected.
  For example, one may be performing his/her tests on remote systems or on a remote office, and he/she doesn't want the users to be aware of what they are doing. Otherwise, the users may be on to him/her and be on their best behaviour.

Extensive knowledge of the systems is not needed for testing . Just a basic understanding is required to protect the tested systems.

Understanding the systems which are being tested shouldn't be difficult if one is hacking his/her own in-house systems. If hacking a customer's systems, one may have to dig deeper. In fact, Most people are scared of these assessments. Base the type of test one will perform on his/her organization's or customer's needs.

- **Selecting tools**

  If one don't have the right tools for ethical hacking, to accomplish the task is effectively difficult. just using the right tools doesn't mean that all vulnerabilities will be discovered.

  Know the personal and technical limitations.

  Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities). Some tools may miss vulnerabilities. Many tools focus on specific tests, but no one tool can test for everything. This is why a set of specific tools are required that can call on for the task at hand. The more are the tools , the easier ethical hacking efforts are.

  Make sure the right tool is being used for the task :
- To crack passwords, one needs a cracking tool such as LC4, John the Ripper, or pwdump.

  A general port scanner, such as SuperScan, may not crack passwords.
- For an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or WebInspect) is more appropriate than a network analyzer (such as Ethereal).

  When selecting the right security tool for the task, ask around. Get advice from the colleagues and from other people online. A simple Groups search on Google (www.google.com) or perusal of security portals, such as SecurityFocus.com, SearchSecurity.com, and ITsecurity.com, often produces great feedback from other security experts.

  Some of the widely used commercial, freeware, and open-source security tools:
  - Nmap
  - EtherPeek
  - SuperScan
  - QualysGuard
  - WebInspect
  - LC4 (formerly called L0phtcrack)
  - LANguard Network Security Scanner
  - Network Stumbler
  - ToneLoc

  Here are some other popular tools:
  - Internet Scanner
  - Ethereal
  - Nessus

- Nikto
- Kismet
- THC-Scan

The capabilities of many security and hacking tools are often misunderstood. This misunderstanding has shed negative light on some excellent tools, such as **SATAN** (**S**ecurity **A**dministrator **T**ool for **A**nalysing **N**etworks) and **Nmap** (**N**etwork **map**per).

Some of these tools are complex. Whichever tools are being used, one should be familiarized with them before starting to use them.

Here are ways to do that:

- ✓ Read the readme and/or online help files for tools.
- ✓ Study the user’s guide for commercial tools.
- ✓ Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.
- ✓ One should Look for these characteristics in tools for ethical hacking:
- ✓ Adequate documentation.
- ✓ Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
- ✓ Updates and support when needed.
- ✓ High-level reports that can be presented to managers or non-techie types.
- ✓ These features can save time and effort when writing the report.

- **Executing the plan**

  Ethical hacking can take persistence. Time and patience are important. One should be careful when performing ethical hacking tests. A hacker in network or a seemingly gentle employee looking over one’s shoulder may watch what’s going on. This person could use this information against tester.

  It’s not practical to make sure that no hackers are on one’s systems before starting. Just one has to make sure to keep everything as quiet and private as possible. This is especially critical when transmitting and storing own test results. If possible, one should encrypt these e-mails and files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them.

  In an investigation mission, attach as much information as possible about the organization and systems, which is what malicious hackers do.

  Start with a broad view and narrow down the focus:

1. Search the Internet for own organization’s name, computer and network system names, and the IP addresses.
   Google is a great place to start for this.
2. Narrow the scope, targeting the specific systems to be tested or being tested.
   Whether physical-security structures or Web applications, a casual assessment can turn up much information about the systems.
3. Further narrow down focus with a more critical eye. Perform actual scans and other detailed tests on the systems.

4. Perform the attacks, if that's what one choose to do.

- **Evaluating results**

  Assess the results to see what has been uncovered, assuming that the vulnerabilities haven't been made obvious before now. This is where knowledge counts. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience. One will end up knowing his/her own systems as well as anyone else. This makes the evaluation process much simpler moving forward.

  Submit a formal report to upper management or to the customer, outlining results. Keep these other parties in the loop to show that efforts and their money are well spent.

- **Moving on**

  When finished with ethical hacking tests, one still need to implement his/her analysis and recommendations to make sure that the systems are secure.

  New security vulnerabilities continually appear. Information systems constantly change and become more complex. New hacker exploits and security vulnerabilities are regularly uncovered. Security tests are a snapshot of the security posture of the systems.

  At any time, everything can change, especially after software upgrades, adding computer systems, or applying patches. Plan to test regularly (for example, once a week or once a month).

5.6 Cracking the Hacker Mindset

Before assessing the security of systems, one may want to understand something about the hackers mind-set. Many information security product vendors and other professionals claim that one should protect the systems from the bad guys , both internal(Insiders) and external(Outsiders).

Knowing what hackers and malicious users want helps understand how they work. Understanding how they work helps to look at your information systems in a whole new way. This understanding better prepares for ethical hacking tests.

- **What You're Up Against**

Thanks to sensationalism in the media, public perception of hacker has transformed from harmless tamperer to malicious criminal. Hackers often state that the public misunderstands them, which is mostly true. It's easy to prejudge what is not understood. Unfortunately, many hacker stereotypes are based on misunderstanding rather than fact, and that misunderstanding fuels a constant debate.

Hackers can be classified by both their abilities and their underlying motivations. Some are skilled, and their motivations are benign; they're merely seeking more knowledge. At the other end of the spectrum, hackers with malicious intent seek some form of personal gain. Unfortunately, the negative aspects of hacking usually overshadow the positive aspects and promote the negative stereotypes.

Hackers hacked for the pursuit of knowledge and the thrill of the challenge. Hackers see what others often overlook. They wonder what would happen if a cable was unplugged, a switch was flipped, or lines of code were changed in a program. These old-school hackers

mat think they can improve electronic and mechanical devices by “rewiring them.” More recent evidence shows that many hackers may also hack for political, social, competitive, and even financial purposes, so times are changing.
Hackers who perform malicious acts don’t really think about the fact that human beings are behind the firewalls, wireless networks, and web applications they’re attacking. They ignore that their actions often affect those human beings in negative ways, such as put in danger their job security and putting their personal safety at risk.

These people don’t hack in the way people normally suppose. Instead, they root around in files on server shares; probe into databases they know they shouldn’t be in; and sometimes steal, modify, and delete sensitive information to which they have access. This behaviour is often very hard to detect . This activity is continued if these users passed their criminal background and credit checks before they were hired. Past behaviour is often the best predictor of future behaviour, but just because someone has a clean record and authorization to access sensitive systems doesn’t mean he or she won’t do anything bad. Criminals may have to start from somewhere.
As negative as breaking into computer systems often can be, hackers and malicious users play key roles in the advancement of technology. In a world without hackers, odds are good that the latest intrusion prevention technology, data leakage protection, or vulnerability scanning tools would not exist. Such a world may not be bad, but technology does keep security professionals employed and keep the field moving forward. Unfortunately, the technical security solutions can’t ward off all malicious attacks and unauthorized use because hackers and (sometimes) malicious users are usually a few steps ahead of the technology designed to protect against their disobedient actions.

However when the stereotypical hacker or malicious user is being viewed, one thing is certain: Somebody will always try to take down computer systems and compromise information by poking and prodding where he or she shouldn’t, through denial of service attacks or by creating and launching malware. One must take the appropriate steps to protect his/her systems against this kind of intrusion.

- **Thinking like the bad guys**

Malicious attackers often think and work just like thieves, kidnappers, and other organized criminals you hear about in the news every day. The smart ones constantly devise ways to fly under the radar and exploit even the smallest weaknesses that lead them to their target. The following are examples of how hackers and malicious users think and work :

- ✓ **Evading an intrusion prevention system** by changing their MAC address or IP address every few minutes to get further into a network without being completely blocked
- ✓ **Exploiting a physical security weakness** by being aware of offices that have already been cleaned by the cleaning crew and are unoccupied (and thus easy to access with little chance of getting caught), which might be made obvious by, for instance, the fact that the office blinds are opened and the curtains are pulled shut in the early morning

- ✓ **Bypassing web access controls** by changing a malicious site's URL to its dotted decimal IP address equivalent and then converting it to hexadecimal for use in the web browser
- ✓ **Using unauthorized software that would otherwise be blocked at the firewall** by changing the default TCP port that it runs on
- ✓ **Setting up a wireless "evil twin"** near a local Wi-Fi hotspot to entice unsuspecting Internet surfers onto a rogue network where their information can be captured and easily manipulated
- ✓ **Using an overly trusting colleague's user ID and password** to gain access to sensitive information that would otherwise be highly improbable to obtain
- ✓ **Unplugging the power cord or Ethernet connection to a networked security camera**that monitors access to the computer room or other sensitive areas and subsequently gaining unmonitored access
- ✓ **Performing SQL injection or password cracking against a website** via a neighbor's unprotected wireless network in order to hide the malicious user's own identity

- **Who Breaks into Computer Systems**

In a world of black and white, describing the typical hacker is easy. A general stereotype of a hacker is an antisocial, unpleasant mind-set personality. But the world has many shades of gray and many types of hackers. Hackers are unique individuals, so an exact profile is hard to outline. The best broad description of hackers is that all hackers aren't equal. Each hacker has his or her own unique motives, methods, and skills. Hacker skill levels fall into three general categories:

- ✓ **Script kiddies:** These are computer beginners who take advantage of the hacker tools, vulnerability scanners, and documentation available free on the Internet but who don't have any real knowledge of what's really going on behind the scenes. They know just enough to cause headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind.
- ✓ **Criminal hackers:** These are skilled criminal experts and nation states who write some of the hacking tools, including the scripts and other programs that the script kiddies and ethical hackers use. These people also write such malware as viruses and worms. They can break into systems and cover their tracks.

Advanced hackers are often members of collectives that prefer to remain nameless. These hackers are very secretive and share information with their subordinates only when they are deemed worthy. Typically, for lower-ranked hackers to be considered worthy, they must possess some unique information or prove themselves through a high-profile hack.

These hackers are possibly some of the worst enemies in information security.

- ✓ **Security researchers:** These uber-hackers are highly technical and publicly known IT professionals who not only monitor and track computer, network, and application vulnerabilities but also write the tools and other code to exploit them. If these guys didn't exist, ethical hackers wouldn't have much in the way of open source and even certain commercial security-testing tools.

There are good-guy (white hat) and bad-guy (black hat) hackers. Gray hat hackers are a little bit of both. There are also blue-hat hackers who are invited by software vendors to find security flaws in their systems.

A recent study at the Black Hat security conference found that everyday IT professionals even engage in malicious and criminal activity against others. And people wonder why IT doesn’t get the respect it deserves? Perhaps this group will evolve into a fourth general category of hackers in the coming years.
Perhaps more important than a hacker’s skill level is his or her motivation.

- ✓ **Hacktivists** try to distribute political or social messages through their work. A hacktivist wants to raise public awareness of an issue. In many situations, criminal hackers will try to take the person down if he/she expresses a view that’s contrary to theirs. Examples of hacktivism include messages about legalizing drugs, protests against the war in Iraq, protests centered around wealth envy and big corporations, and just about any other social and political issues.
- ✓ **Cyber-terrorists** (both organized and unorganized) attack government computers or public utility infrastructures, such as power grids and air-traffic control towers. They crash critical systems or steal classified government information. Countries take the threats these cyber-terrorists pose so seriously that many mandate information security controls in crucial industries, such as the power industry, to protect essential systems against these attacks.
- ✓ **Hackers for hire** are part of organized crime on the Internet. Many of these hackers hire out themselves or their botnets for money and lots of it.

These criminal hackers are in the minority. Like the spam kings of the world, many of the wicked acts from members of collectives that prefer to remain nameless are carried out by a small number of criminals. Many other hackers just love to tinker and only seek knowledge of how computer systems work. One of the greatest threats works inside premises and has an access badge to the building and a valid network account, so don’t discount the insider threat.

- **Why They Do It?**
  Reasons:
  - ✓ Hacking is a casual hobby for some hackers. They hack just to see what they can and can’t break into, usually testing only their own systems.
  - ✓ Many hackers get a kick out of outsmarting corporate and government IT and security administrators. They thrive on making headlines and being notorious cyber outlaws.
  - ✓ Hackers often promote individualism or at least the decentralization of information because many believe that all information should be free.
  - ✓ They think cyber-attacks are different from attacks in the real world. Hackers may easily ignore or misunderstand their victims and the consequences of hacking.
  - ✓ They don’t think long-term about the choices they’re making today. Many hackers say they don’t intend to harm or profit through their bad deeds, a belief that helps them justify their work.

- ✓ Some common motives are revenge, basic bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, corporate intelligence, and just generally speaking out against “the man.” Hackers regularly cite these motives to explain their behavior, but these motivations tend to be cited more commonly during difficult economic conditions.
- ✓ Many business owners and managers — even some network and security administrators believe that they don’t have anything that a hacker wants or that hackers can’t do much damage if they break in. This indifferent kind of thinking helps support the bad guys and promote their objectives.
- ✓ Hackers can compromise a seemingly unimportant system to access the network and use it as a launching pad for attacks on other systems, and many people would be none the wiser because they don’t have the proper controls to prevent and detect malicious use.
- ✓ Hackers often hack just because they can. Some hackers go for high-profile systems, but hacking into anyone’s system helps them fit into hacker circles. Hackers exploit many people’s false sense of security and go for almost any system they think they can compromise. Electronic information can be in more than one place at the same time, so if hackers merely copy information from the systems they break into, it’s tough to prove that hackers possess that information.

Computer openings continue to get easier to execute yet harder to prevent for several reasons:

- ✓ Widespread use of networks and Internet connectivity
- ✓ Anonymity provided by computer systems working over the Internet and often on the internal network (because, effectively, logging and especially log monitoring rarely takes place)
- ✓ Greater number and availability of hacking tools
- ✓ Large number of open wireless networks that help hackers cover their tracks
- ✓ Greater complexity and size of the codebase in the applications and databases being developed today
- ✓ Computer-savvy children
- ✓ Unlikelihood **that attackers will be investigated or prosecuted if caught**

A malicious hacker only needs to find one security hole **whereas IT professionals and business owners must find and block them all**.

Although many attacks go unnoticed or unreported, criminals who are discovered are often not pursued or prosecuted. When they’re caught, hackers often rationalize their services as being unselfish and a benefit to society: They’re merely pointing out vulnerabilities before someone else does.

The same goes for malicious users. Typically, their troubles go unnoticed, but if they’re trapped, the security breach may be kept secret in the name of shareholder value or not wanting to disturb any customer or business partner. However, recent information security and privacy laws and regulations are changing this because in most situations breach notification is required. Sometimes, the person is fired or asked to resign. Although public cases of internal breaches are becoming more common, these cases don’t give a full picture of what’s really taking place in the average organization.

Hacking in the name of liberty?

Many hackers exhibit behaviours that contradict their stated purposes. They fight for civil liberties and want to be left alone, while at the same time, they love prying into the business of others and controlling them in any way possible.

Many hackers call themselves civil libertarians and claim to support the principles of personal privacy and freedom. However, they contradict their words by intruding on the privacy and property of others. They often steal the property and violate the rights of others, but are willing to go to great lengths to get their own rights back from anyone who threatens them.

This applies to external hacks, internal breaches, and even something as seemingly gentle as a lost mobile device or backup tapes.

- **Planning and Performing Attacks**

  Attack styles vary widely:

  - ✓ **Some hackers prepare far in advance of an attack.** They gather small bits of information and methodically carry out their hacks. These hackers are the most difficult to track.
  - ✓ **Other hackers — usually the inexperienced script kiddies — act before they think through the consequences.** Such hackers may try, for example, to telnet directly into an organization’s router without hiding their identities. Other hackers may try to launch a DoS attack against a Microsoft Exchange server without first determining the version of Exchange or the patches that are installed. These hackers usually are caught.
  - ✓ **Malicious users are all over the map.** Some can be quite savvy based on their knowledge of the network and of how IT operates inside the organization.

    Many of the hackers, especially advanced hackers don’t share information with the crowd. Most hackers do much of their work independently in order to remain anonymous.

  Hackers who network with one another use private message boards, anonymous e-mail addresses, hacker websites, and **Internet Relay Chat (IRC).**One can log in to many of these sites to see what hackers are doing.

  Following are the aspects of real-world security:

  - ✓ **The majority of computer systems aren’t managed properly.** The computer systems aren’t properly patched, hardened, or monitored. Attackers can often fly below the radar of the average firewall, an Intrusion prevention system (IPS), or an access control system. This is especially true for malicious users whose actions are often not monitored at all while, at the same time, they have full access to the very environment they can exploit.

- ✓ **Most network and security administrators simply can't keep up with the deluge of new vulnerabilities and attack methods.** These people often have too many tasks to stay on top of and too many other fires to put out. Network and security administrators may also fail to notice or respond to security events because of poor time management and goal setting, but that's for another discussion.
- ✓ **Information systems grow more complex every year.** This is yet another reason why overburdened administrators find it difficult to know what's happening across the wire and on the hard drives of all their systems. Mobile devices such as laptops, tablets, and phones are making things exponentially worse.

Time is an attacker's friend and it's almost always on his or her side. By attacking through computers rather than in person, hackers have more control over the timing for their attacks:

- ✓ **Attacks can be carried out slowly, making them hard to detect.**
- ✓ **Attacks are frequently carried out after typical business hours,** often in the middle of the night, and from home, in the case of malicious users.

If one wants detailed information on how some hackers work or want to keep up with the latest hacker methods, several magazines are worth checking out:

- ✓ 2600 — The Hacker Quarterly magazine
- ✓ Magazine
- ✓ Hackin9
- ✓ PHRACK

Malicious attackers usually learn from their mistakes. Every mistake moves them one step closer to breaking into someone's system. They use this knowledge when carrying out future attacks. As an ethical hacker, one needs to do the same.

- **Maintaining Anonymity**

Smart attackers want to remain as low-key as possible. Covering their tracks is a priority, and many times their success depends on them remaining unnoticed. They want to avoid raising suspicion so they can come back and access the systems in the future.

Hackers often remain anonymous by using one of the following resources:

- ✓ Borrowed or stolen remote desktop and VPN accounts from friends or previous employers
- ✓ Public computers at libraries, schools, or kiosks at the local mall
- ✓ Open wireless networks
- ✓ Internet proxy servers
- ✓ Anonymous or disposable e-mail accounts from free e-mail services
- ✓ Open e-mail relays
- ✓ Infected computers also called zombies or bots at other organizations
- ✓ Workstations or servers on the victim's own network

If hackers use enough stepping stones for their attacks, they are hard to trace.

Ethical Hacker: Job Description, Requirements

Ethical hackers are trained hackers who use their skills to identify security problems with computer networks.

Career Definition of an Ethical Hacker

Ethical hackers are cyber security professionals who are capable of breeching security systems. They conduct tests on computer networks and try to hack into the networks to access information without authorization. The purpose of this is to identify weaknesses in the security systems that are in place and help determine how to improve Internet security.

The primary objective of an ethical hacker is to ensure that the computer systems they work with are safe and cannot be accessed without authorization.

They need to be aware of new software and hardware that can improve computer security since they play a key role in determining the security needs of their employer or clients. When they attempt to hack into the system, they produce reports detailing their attempts and the conclusions they've reached about the effectiveness of the security systems that are in place.

Educational Requirements	Bachelor's degree and certification
Job Skills	Analytical skills, interpersonal skills, communication skills, customer service skills, attention to detail, problem-solving skills
Job Outlook (2016-2026)	28% (*information security analysts*)

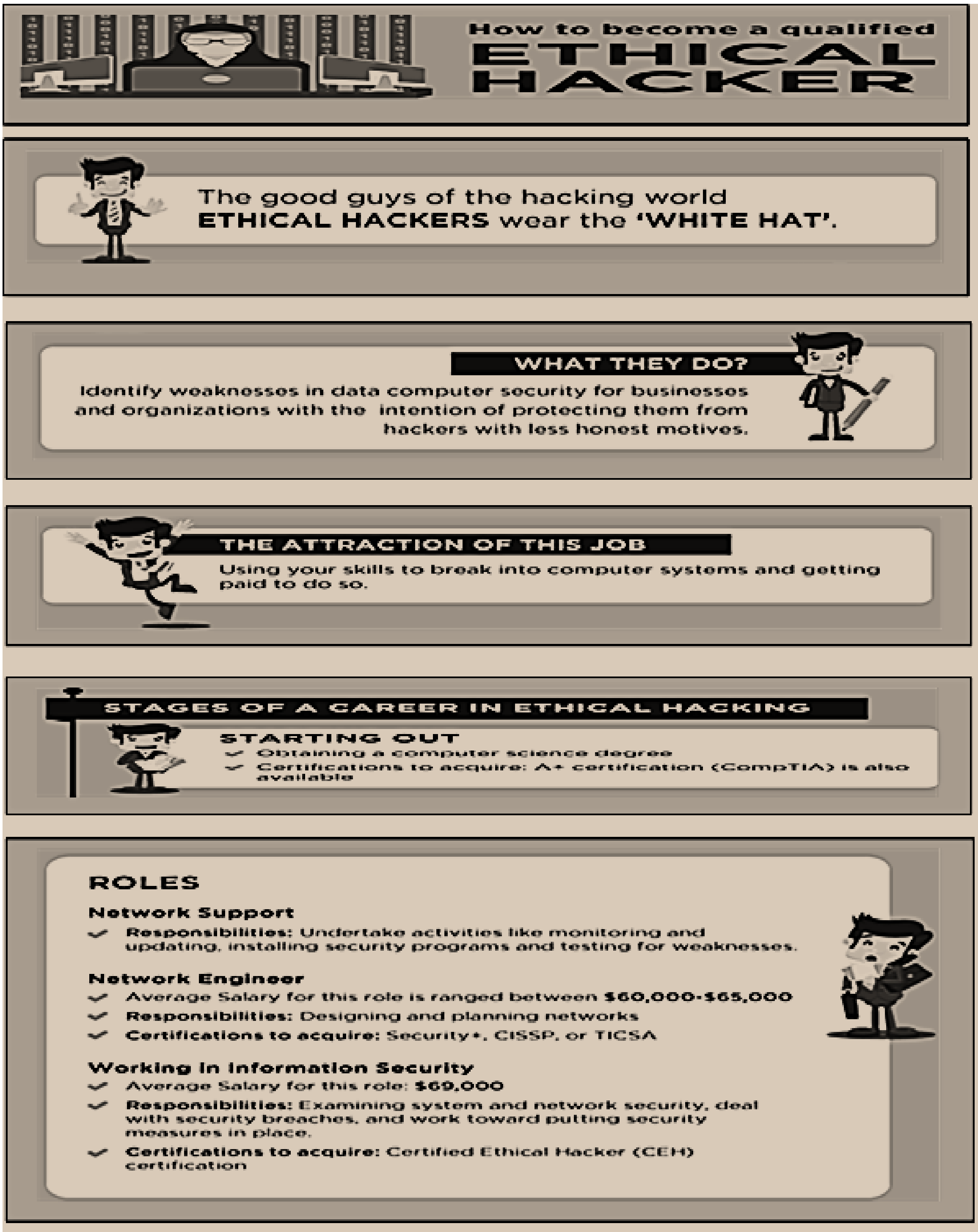
Required Education

In order to become an ethical hacker it's necessary to have a bachelor's degree in a related field, such as computer science. Ethical hackers need to have computer programming experience and familiarity with a range of different programming languages. It's common for employers to require ethical hackers to have **Certified Ethical Hacker(CEH)** certification and other recognized certifications, such as CompTIA, that prepare them to work as experts in cyber security.

Required Skills

Ethical hackers need to have:

- ✓ Strong analytical skills because their work involves reviewing a lot of data to identify potential issues with computer network security.
- ✓ Consulting with clients, explaining their findings to managers or clients, and collaborating with other professionals who are involved with information security.
- ✓ Excellent customer service skills and strong interpersonal skills.
- ✓ Communication skills are also important so that they can effectively explain their test results to clients and co-workers.
- ✓ Exceptional problem-solving skills and attention to detail are fundamental since ethical hackers need to be thorough in their attempts to breech the security systems in place.
- ✓ Develop new and often innovative strategies that enable them to identify problems with the security systems they work on.



How to become a qualified
ETHICAL HACKER

The good guys of the hacking world
ETHICAL HACKERS wear the 'WHITE HAT'.

WHAT THEY DO?

Identify weaknesses in data computer security for businesses and organizations with the intention of protecting them from hackers with less honest motives.

THE ATTRACTION OF THIS JOB

Using your skills to break into computer systems and getting paid to do so.

STAGES OF A CAREER IN ETHICAL HACKING

STARTING OUT

✓ Obtaining a computer science degree

✓ Certifications to acquire: A+ certification (CompTIA) is also available

ROLES

Network Support

✓ Responsibilities: Undertake activities like monitoring and updating, installing security programs and testing for weaknesses.

Network Engineer

✓ Average Salary for this role is ranged between $60,000-$65,000

✓ Responsibilities: Designing and planning networks

✓ Certifications to acquire: Security+, CISSP, or TICSA

Working in Information Security

✓ Average Salary for this role: $69,000

✓ Responsibilities: Examining system and network security, deal with security breaches, and work toward putting security measures in place.

✓ Certifications to acquire: Certified Ethical Hacker (CEH) certification

Fig. 5.3 What knowledge is required to become an ethical hacker?

Steps to become A Hacker:

Step 0: Read the Hacking

Step 1: Learn To Program In C

Step 2: Learn More Than One Programming Language

Step 3: Learn UNIX

Step 4: Learn More Than One Operating Systems

Step 5: Learn Networking Concepts

Step 6: Start Simple: Read Some Tutorials About Hacking
Step 7: Learn Cryptography
Step 8: Experiment A Lot

Some of the things you may need to keep in mind when doing experiments

- ✓ Keep a backup before any experiment.
- ✓ Start small and have check points.
- ✓ Know when to stop.
- ✓ Document your progress
- ✓ Keep improvising
- ✓ Automate repetitive tasks

Step 9: Read Some Good Books From Experts

Step 10: Participate In Hacking Challenges: Apart from that, there are some websites listed below that regularly offer hacking challenges online.

- ✓ hackquest.de
- ✓ Page on hacktissite.org
- ✓ www.trythis0ne.com
- ✓ www.hackchallenge.net
- ✓ Home : Hacking-Lab.com

Step 11: Go Next Level: Write Vulnerability
Step 12: Contribute To Open Source Security Projects
Step 13: Continue Learning And Keep Listening To Security Talks

Above are few exhaustive steps that can teach how to be a hacker and help to walk the road of being an expert hacker. However, one should be a responsible citizen and be selective, ensuring one don’t use this skill to breach the security of important institutions, as it may land you in dire straits. One should always remember, for every hacking tool, there is always a counter hacking tool. Therefore, be a smart hacker and more importantly, be a responsible hacker.

Ethical Hacking Related Careers

Ethical hackers spend most of their time working on computers and must be capable of writing computer programming code. Those interested in this career field may be interested in the other occupations linked to here that involve writing computer code, protecting data stored on computer networks and creating secure computer networks.

- Back-End Developer: Job Description & Salary
- Become a Software Developer: Education and Career Roadmap
- Computer Networking Specialist: Job Description and Requirements

Hacking Tools: are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There is a variety of such tools available on the market. Some of them are open source while others are commercial solution.

Tools for Ethical hacking of web applications, servers and networks:

- ✓ **Netsparker** is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SAAS solution.
- ✓ **Acunetix**is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.
- ✓ **Probely**continuously scans for vulnerabilities in your Web Applications. It allows its customers to manage the life cycle of vulnerabilities and provides them with some guidance on how to fix them. Probely is a security tool built having Developers in mind.
- ✓ **InsightVM**is a top-ranked vulnerability risk management solution focused on detecting, prioritizing, and remediating vulnerabilities. With InsightVM, you can automatically assess and understand security risk across your entire infrastructure.
- ✓ **SaferVPN**is an indispensable tool in an Ethical hacker’s arsenal. You may need it to check target in different geographies, simulate non-personalized browsing behavior, undiscovered file transfers, etc.
- ✓ **Burp Suite** is a useful platform for performing Security Testing of web applications. Its various tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.
- ✓ **Ettercap** is an ethical hacking tool. It supports active and passive dissection includes features for network and host analysis.
- ✓ **Aircrack** is a trustable ethical hacking tool. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.
- ✓ **Angry IP Scanner** is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.
- ✓ **GFI LanGuard** is an ethical tool that scans networks for vulnerabilities. It can acts as your 'virtual security consultant' on demand. It allows creating an asset inventory of every device.
- ✓ **Savvius:** It is an ethical hacking tool. It performance issues and reduces security risk with the deep visibility provided by Omnipeek. It can diagnose network issues faster and better with Savvius packet intelligence.
- ✓ **Qualys guard** helps businesses streamline their security and compliance solutions. It also builds security into their digital transformation initiatives. This tool can also check the performance vulnerability of the online cloud systems.
- ✓ **WebInspect** is automated dynamic application security testing that allows performing ethical hacking techniques. It provides comprehensive dynamic analysis of complex web applications and services.
- ✓ **Hashcat** is a robust password cracking ethical hacking tool. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

- ✓ **L0phtCrack 6** is useful password audit and recovery tool. It identifies and assesses password vulnerability over local machines and networks.
- ✓ **RainbowCrack** is a password cracking tool widely used for ethical hacking. It cracks hashes with rainbow tables. It uses time-memory tradeoff algorithm for this purpose.
- ✓ **Hashcat** is a robust password cracking ethical hacking tool. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.
- ✓ **IKECrack** is an open source authentication crack tool. This ethical hacking tool is designed to brute-force or dictionary attack. This tool also allows performing cryptography tasks.
- ✓ **IronWASP** is an open source software for ethical hacking too. It is web application vulnerability testing. It is designed to be customizable so that users can create their custom security scanners using it.
- ✓ **Medusa** is one of the best online brute-force, speedy, parallel password crackers ethical hacking tool. This tool is also widely used for ethical hacking.
- ✓ **NetStumble**r is used to detect wireless networks on the Windows platform.
- ✓ **SQLMap** automates the process of detecting and exploiting SQL Injection weaknesses. It is open source and cross platform. It supports the following database engines.
  - ✦ Recover MS Access passwords
  - ✦ Uncover password field
  - ✦ Sniffing networks
  - ✦ Cracking encrypted passwords using dictionary attacks, brute-force, and cryptanalysis attacks.
- ✓ **Nessus** can be used to perform:
  - ✦ Remote vulnerability scanner
  - ✦ Password dictionary attacks
  - ✦ Denial of service attacks.
  - ✦ It is closed source, cross platform and free for personal use.

References

- https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078)
- Hacking For Dummies, 5th Edition By Kevin Beaver
- http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies
- http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking
- https://www.dummies.com/programming/networking/what-is-a-malicious- user/
- https://www.guru99.com/what-is-hacking-an-introduction.html#2
- http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies.pdf
- 2600 — The Hacker Quarterly magazine (www.2600.com)
- (IN)SECURE Magazine (www.net-security.org/insecuremag.php)
- Hackin9 (http://hakin9.org)

- PHRACK (www.phrack.org/archives/)
- https://learning.oreilly.com/library/view/hacking-for-dummies/9781118380956/06_9781118380956-ch02.html
- https://www.quora.com/What-knowledge-is-required-to-become-an-ethical-hacker

Sample Multiple Choice Questions:

1) Ethical Hacking is also known as______

a. Black Hat hacking
b. White hat hacking
c. Encrypting
d. None of these

2) Tool(s) used by ethical hackers ______

a. Scanner
b. Decoder
c. Proxy
d. All of these

3) Vulnerability scanning in Ethical hacking finds________

a. Strengths
b. Weakness
c. a&b
d. None of these

4) Ethical hacking will allow to________ all the massive security breaches.

a. remove
b. measure
c. reject
d. None of these

5) Sequential steps hackers use are: __, ___, __, __

A) Maintaining Access
B) Reconnaissance
C) Scanning
D) Gaining Access

a. B, C, D, A
b. B, A, C, D
c. A, B, C, D
d. D, C, B, A

Unit-6 Types of Hacking

Contents

6.1 Network Hacking

- Computer Network is one of the most fundamental communications systems in your organization. Network consists of such devices as routers, firewalls, and even generic hosts (including servers and workstations) that you must assess as part of the ethical hacking process.
- There are thousands of possible network vulnerabilities, equally as many tools, and even more testing techniques. We don’t need to test our network for every possible vulnerability, using every tool available.
- We can eliminate many well-known network vulnerabilities by simply patch-ing your network hosts with the latest vendor software and firmware patches. We can eliminate many other vulnerabilities by following some security best practices on our network.

6.1.2 Network Infrastructure Vulnerabilities

- Network infrastructure vulnerabilities are the foundation for all technical security issues in your information systems. These lower-level vulnerabilities affect everything running on your network. That's why you need to test for them and eliminate them whenever possible.
- Your focus for ethical hacking tests on your network infrastructure should be to find weaknesses that others can see in your network so you can quantify your level of exposure.
- Many issues are related to the security of your network infrastructure. Some issues are more technical and require you to use various tools to assess them properly. You can assess others with a good pair of eyes and some logical thinking. Some issues are easy to see from outside the network, and others are easier to detect from inside your network
- Network infrastructure security involves assessing such areas as
  - ✓ Where such devices as a firewall or IDS (intrusion detection system) are placed on the network and how they are configured
  - ✓ What hackers see when they perform port scans and how they can exploit vulnerabilities in your network hosts
  - ✓ Network design, such as Internet connections, remote-access capabilities, layered defenses, and placement of hosts on the network
  - ✓ Interaction of installed security devices
  - ✓ Protocols in use
  - ✓ Commonly attacked ports that are unprotected
  - ✓ Network host configuration
  - ✓ Network monitoring and maintenance
- If any of these network security issues is exploited, such things can happen:
  - ✓ A DoS attack can take down your Internet connection or even your entire network.
  - ✓ A hacker using a network analyzer can steal confidential information in e-mails and files being transferred.
  - ✓ Backdoors into your network can be set up.
  - ✓ Specific hosts can be attacked by exploiting local vulnerabilities across the network.
- Always remember to do the following:
  - ✓ Test your systems from both the outside in and the inside out.
  - ✓ Obtain permission from partner networks that are connected to your network to check for vulnerabilities on their ends that can affect your network's security, such as open ports and lack of a firewall or a misconfigured router.

Network Testing and port scanning tools:

- **Sam Spade** for Windows for network queries from DNS lookups to trace routes
- **SuperScan** for ping sweeps and port scanning
- **NetScan**Tools Pro for dozens of network security-assessment functions, including ping sweeps, port scanning, and SMTP relay testing

- **Nmap or NMapWin** as a happy-clicky-GUI front end for host-port probing and operating-system fingerprinting
- **Netcat** the most versatile security tool for such security checks as port scanning and firewall testing
- **WildPacketsEtherPeek** for network analysis.

6.1.3 Scanning-Ports

- A port scanner is a software tool that basically scans the network to see who’s there. Port scanners provide basic views of how the network is laid out. They can help identify unauthorized hosts or applications and network host configuration errors that can cause serious security vulnerabilities.
- The big-picture view from port scanners often uncovers security issues that may otherwise go unnoticed. Port scanners are easy to use and can test systems regardless of what operating systems and applications they’re running. The tests can be performed very quickly without having to touch individual network hosts, which would be a real pain otherwise.
- Port-scan tests take time. The length of time depends on the number of hosts you have, the number of ports you scan, the tools you use, and the speed of your network links. Also, perform the same tests with different utilities to see whether you get different results. Not all tools find the same open ports and vulnerabilities. This is unfortunate, but it’s a reality of ethical hacking tests.
- If your results don’t match after you run the tests using different tools, you may want to explore the issue further. If something doesn’t look right such as a strange set of open ports it probably isn’t. Test it again; if you’re in doubt, use another tool for a different perspective.
- As an ethical hacker, you should scan all 65,535 UDP and 65,535 TCP ports on each network host that’s found by your scanner. If you find questionable ports, look for documentation that the application is known and authorized. For speed and simplicity, you can scan commonly hacked ports.

Table 6.1: Commonly hacked ports

Port Nos.	Service	Protocols
7	Echo	TCP, UDP
19	Chargen	TCP, UDP
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP

Port Nos.	Service	Protocols
37	Daytime	TCP, UDP
53	DNS (Domain Name System)	UDP
69	TFTP (Trivial File Transfer Protocol)	UDP
79	Finger	TCP, UDP
80	HTTP (Hypertext Transfer Protocol)	TCP
110	POP3 (Post Office Protocol version 3)	TCP
111	SUN RPC (remote procedure calls)	TCP, UDP
135	RPC/DCE end point mapper for Microsoft networks	TCP, UDP
137, 138, 139	NetBIOS over TCP/IP	TCP, UDP
161	SNMP (Simple Network Management Protocol)	TCP, UDP
220	IMAP (Internet Message Access Protocol)	TCP
443	HTTPS (HTTP over SSL)	TCP
512, 513, 514	Berkeley r commands (such as rsh, rexec, and rlogin)	TCP
1214	Kazaa and Morpheus	TCP, UDP
1433	Microsoft SQL Server	TCP, UDP
1434	Microsoft SQL Monitor	TCP, UDP
3389	Windows Terminal Server	TCP
5631, 5632	pcAnywhere	TCP
6346, 6347	Gnutella	TCP, UDP
12345, 12346, 12631, 12632, 20034, 20035	NetBus	TCP
27444	Trinoo	UDP

Port Nos.	Service	Protocols
27665	Trinoo	TCP
31335	Trinoo	UDP
31337	Back Orifice	UDP
34555	Trinoo	UDP

Countermeasures (Port Scanning)

- You can implement various countermeasures to typical port scanning.

✓ Traffic restriction

- Enable only the traffic you need to access internal hosts preferably as far as possible from the hosts you're trying to protect. You apply these rules in two places: External router for inbound traffic & Firewall for outbound traffic .
- Configure firewalls to look for potentially malicious behavior over time (such as the number of packets received in a certain period of time), and have rules in place to cut off attacks if a certain threshold is reached, such as 100 port scans in one minute. Most firewalls, IDSs, andIDPs detect port scanning and cut it off in real time.

✓ **Gathering network information**

- NetScanTools Pro is a great tool for general network information, such as the -number of unique IP addresses, NetBIOS names, and MAC addresses found.
- The following report is an example of the NetScanner (network scanner) output of NetScanTools Pro 2000:
- Scan completion time = Sat, 7 Feb 2004 14:11:08
- Start IP address: 192.168.1.1
- End IP address: 192.168.1.254
- Number of target IP addresses: 254
- Number of IP addresses responding to pings: 13
- Number of IP addresses sent pings: 254
- Number of intermediate routers responding to pings: 0
- Number of successful NetBIOS queries: 13
- Number of IP addresses sent NetBIOS queries: 254
- Number of MAC addresses obtained by NetBIOS queries: 13
- Number of successful Subnet Mask queries: 0
- Number of IP addresses sent Subnet Mask queries: 254
- Number of successful Whois queries: 254

✓ **Traffic denial**

- Deny ICMP traffic to specific hosts you're trying to protect. Most hosts don't need to have ICMP enabled especially inbound ICMP requests unless it's needed for a network management system that monitors hosts using this protocol.
- You can break applications on your network, so make sure that you analyze what's going on, and understand how applications and protocols are working, before you disable such network traffic as ICMP.

6.1.4 Ping sweeping

- Port sweeping is regarded by certain systems experts to be different from port scanning.
- They point out that port scanning is executed through the searching of a single host for open ports. However, they state that port sweeping is executed through the searching of multiple hosts in order to target just one specific open port.
- While Port scanning and sweeping have legitimate uses with regard to network management, unfortunately, they are used almost as frequently for the purpose of criminal activity.

A Serious Threat

- Any times there are open ports on one's personal computer, there is potential for the loss of data, the occurrence of a virus, and at times, even complete system compromise.
- It is essential for one to protect his or her virtual files, as new security risks concerning personal computers are discovered every day.
- Computer protection should be the number one priority for those who use personal computers.
- Port scanning is considered a serious threat to one's PC, as it can occur without producing any outward signs to the owner that anything dangerous is taking place.

Firewall Protection

- Protection from port scanning is often achieved through the use of a firewall. A firewall monitors incoming and outgoing connections through one's personal computer.
- One technique used by firewall technology is the opening of all the ports at one time. This action stops port scans from returning any ports. This has worked in many situations in the past, however, most experts agree it is best to have all open ports investigated individually.
- Another approach is to filter all port scans going to one's computer. An individual can also choose to port scan his or her own system, which enables one to see the personal computer through the eyes of a hacker.
- Firewalls are the best protection one can invest in with regard to port scanning. Firewalls deny outside access to an individual's personal computer. With this type of protection, a personal computer is essentially hidden from unwelcome visitors and is also protected from a variety of other hacking techniques. With firewall software, an individual is assured that his or her sensitive and personal information remains protected.

- A ping sweep of all your network subnets and hosts is a good way to find out which hosts are alive and kicking on the network.
- A ping sweep is when you ping a range of addresses using Internet Control Message Protocol (ICMP) packets.
- Dozens of Nmap command-line options exist, which can be overwhelming when you just want to do a basic scan.
- You can just enter nmap on the command line to see all the options available.

- These command-line options can be used for an Nmap ping sweep:

- **sP** tells Nmap to perform a ping scan.
- **n**tellsNmap to not perform name resolution. You may want to omit this if you want to resolve hostnames to see which systems are responding. Name resolution may take slightly longer, though.
- -T 4 option tells Nmap to perform an aggressive (faster) scan.
- 192.168.1.1-254 tells Nmap to scan the entire 192.168.1.x subnet.

6.1.5 SNMP(Simple Network Management Protocol) scanning

- Networks are the backbone of every business. Even in small or enterprise-level businesses, the loss of productivity during a network outage can result in hefty damages.
- Network monitoring helps you anticipate potential outages and address network problems proactively. This helps in maintaining a congestion-free network that keeps your business up and running.
- A network monitoring software helps you to monitor the performance of any IP-based device and helps businesses remotely visualize their system performance and monitor network services, bandwidth utilization, switches, routers and traffic flow.

Vulnerabilities (SNMP)

- The problem is that most network hosts run SNMP that isn’t hardened or patched to prevent known security vulnerabilities. The majority of network devices have SNMP enabled and don’t even need it.
- If SNMP is compromised, a hacker can gather such network information as ARP tables and TCP connections to attack your systems. If SNMP shows up in port scans, you can bet that a hacker will try to compromise the system.

- **Countermeasures (SNMP)**

- Preventing SNMP attacks can be as simple as A-B-C:
- Always disable SNMP on hosts if you’re not using it period.
- Block the SNMP port (UDP port 161) at the network perimeter.
- Change the default SNMP community string from public to another value that’s more difficult to guess. This makes SNMP harder to hack.

6.1.6 Banner grabbing

- Banner grabbing is the act of capturing the information provided by banners, configurable text-based welcome screens from network hosts that generally display system information. Banners are intended for network administration
- Banner grabbing is often used for white hathacking endeavors like vulnerability analysis and penetration testing as well as gray hat activities and black hat hacking. Banner screens can be accessed through Telnet at the command prompt on the target system’s IP address.
- Other tools for banner grabbing include Nmap, Netcat and SuperScan. A login screen, often associated with the banner, is intended for administrative use but can also provide access to a hacker. Meanwhile, the banner data can yield information about vulnerable software and services running on the host system.

- For the sake of security, if banners are not a requirement of business or other software on a host system, the services that provide them may be disabled altogether. Banners can also be customized to present disinformation or even a warning message for hackers
- Banners are the welcome screens that divulge software version numbers and other host information to a network host. This banner information may identify the operating system, the version number, and the specific service packs, so hackers know possible vulnerabilities. **You can grab banners by using either plain old telnet or Netcat.**
- Telnet

✓ You can telnet to hosts on the default telnet port (TCP port 23) to see whether you're presented with a login prompt or any other information.

✓ Just enter the following line at the command prompt in Windows or UNIX:

✓ telnet ip_address

- Netcat

✓ Netcat can grab banner information from routers and other network hosts, such as a wireless access point or managed Ethernet switch.

- Countermeasures (Banner Grabbing)

✓ The following steps can reduce the chance of banner-grabbing attacks:

- If there is no business need for services that offer banner information, disable those unused services on the network host.
- If there is no business need for the default banners, or if you can customize the banners displayed, configure the network host's application or operating system to either disable the banners or remove information from the banners that could give an attacker a leg up.

6.1.7 Analysing Network Data and Network Analyzer

- A network analyzer is a tool that allows you to look into a network and analyze data going across the wire for network optimization, security, and/or troubleshooting purposes. Like a microscope for a lab scientist, a network analyzer is a must-have tool for any security professional.
- Network analyzers are often generically referred to as sniffers, though that's actually the name and trademark of a specific product from Network Associates, Sniffer (the original network-analysis tool).
- When assessing security and responding to security incidents, a network analyzer can help you
  - ✓ View anomalous network traffic and even track down an intruder.
  - ✓ Develop a baseline of network activity and performance before a security incident occurs, such as protocols in use, usage trends, and MAC addresses.
- A network analyzer is just software running on a computer with a network card. It works by placing the network card in promiscuous mode, which enables the card to see all the traffic on the network, even traffic not destined to the network-analyzer host.
- The network analyzer performs the following functions:
  - ✓ Captures all network traffic

- ✓ Interprets or decodes what is found into a human-readable format
- ✓ Displays it all in chronological order

- Here are a few caveats for using a network analyzer:
  - ✓ To capture all traffic, you must connect the analyzer to either
  - ✓ A hub on the network
  - ✓ A monitor/span/mirror port on a switch
  - ✓ What's entering your network before the firewall filters eliminates the junk traffic
  - ✓ What's leaving your network after the traffic goes past the firewall
- When your network behaves erratically, a network analyzer can help you in
  - ✓ Track and isolate malicious network usage
  - ✓ Detect malicious Trojan-horse applications
  - ✓ Monitor and track down DoS attacks
- Different network analysing tools are

Sr No	Name of Network Analyzer	Supporting Operating System
1	EtherPeek by WildPackets	Windows
2	Ethereal	Windows and UNIX
3	ettercap	Windows and UNIX
4	dsniff	UNIX

Countermeasures (Network Analyzer)

A network analyzer can be used for good or evil. All these tests can be used against you, too. A few countermeasures can help prevent someone from using an unauthorized network analyzer, but there's no way to completely prevent it.

- ✓ Physical security
  - Ensure that adequate physical security is in place to prevent a hacker from plugging into your network
  - Keep the bad guys out of your server room and wiring closet
  - A special monitor port on a switch where a hacker can plug in a network analyzer is especially sensitive. Make sure it's extra secure
  - Make sure that such unsupervised areas as unoccupied desks don't have live network connections.
- ✓ Network-analyzer detection

- You can use a network- or host-based utility to determine if someone is running an unauthorized network analyzer on your network
- Some Network analyzer detection tools are sniffdet, PromiscDetect. These tools enable us to monitor the network for Ethernet cards that are running in Promiscuous mode.

6.1.8 The MAC-daddy attack

- Hackers can use ARP Protocol that is running on the network to make their systems seem as your system or another allowed host on your network.

- A too much number of ARP (Address Resolution Protocol) requests can be a sign of an ARP poisoning or spoofing attack on your network. Anyone can run a program, such as dsniff tool or Cain & Abel tool, can modify the ARP tables, which are responsible for saving IP addresses to media access control (MAC) address mappings on network hosts.
- That makes the victim machines to think they require to forward traffic to the hacker's computer rather than to the correct destination machine when communicating on the network. And this is a type of man-in-the-middle (MITM) attacks. Spoofed ARP responses can be sent to a switch, which returns the switch to broadcast mode and basically turns it into a hub. When this happens, a hacker can sniff every packet going through the switch and capture anything and everything from the network.

ARP spoofing

- ✓ An excessive amount of ARP requests can be a sign of an *ARP poisoning* attack (or *ARP spoofing*) on your network.
- ✓ What happens is that a client running a program such as the UNIX-based dsniff or the UNIX- and DOS/Windows-based ettercap can change the ARP tables the tables that store IP addresses to *media access control (MAC)* mappings on network hosts.
- ✓ This causes the victim computers to think they need to send traffic to the attacker's computer, rather than the true destination computer, when communicating on the network. This is often referred to as a Man-in-the-Middle (MITM) attack.

MAC-address spoofing

- ✓ MAC-address spoofing tricks the *switch* into thinking you (actually, your computer) are someone else. You simply change your MAC address and masquerade as another user
- ✓ You can use this trick to test such access control systems as your IDS, fire-wall, and even operating-system login controls that check for specific MAC addresses.

Countermeasures (MAC-daddy attack)

- ✓ A few countermeasures on your network can minimize the effects of a hacker attack against ARP and MAC addresses on your network.

- You can prevent MAC-address spoofing if your switches can enable port security to prevent automatic changes to the switch MAC address tables.
- No realistic countermeasures for ARP poisoning exist. The only way to prevent ARP poisoning is to create and maintain static ARP entries in your switches for every host on the network. This is definitely something that no network administrator has time to do.

Detection

- ✓ You can detect these two types of hacks through either an IDS or a stand-alone MAC address monitoring utility.

- ✓ Arp watch is a UNIX-based program alerts you via e-mail if it detects changes in MAC addresses associated with specific IP addresses on the network.

Wireless LAN

- A wireless LAN (or WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 group of standards specify the technologies for wireless LANs 802.11 standards used the Ethernet Protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.

- **Implications of Wireless Network Vulnerabilities**

✓ WLANs are very susceptible to hacker attacks even more so than wired networks are.
✓ They have vulnerabilities that can allow a hacker to bring your network to its knees and allow your information to be gleaned right out of thin air.
✓ If a hacker comprises your WLAN, you can experience the following problems:

1. Loss of network access, including e-mail, Web, and other services that can cause business downtime
2. .Loss of confidential information, including passwords, customer data, intellectual property, and more.
3. Legal liabilities associated with unauthorized users

- Most of the wireless vulnerabilities are in the 802.11 protocol and within wireless access points the central hub like devices that allow wireless clients to connect to the network. Wireless clients have some vulnerability as well.
- Various fixes have come along in recent years to address these vulnerabilities, but most of these fixes have not been applied or are not enabled by default.
- You may also have employees installing rogue WLAN equipment on your network without your knowledge; this is the most serious threat to your wireless security and a difficult one to fight off. Even when WLANs are hardened and all the latest patches have been applied, you still may have some serious security problems, such as DoS and man-in-the-middle attacks (like you have on wired networks), that will likely be around for a while.
- Common Wireless Threats
  - There are a number of main threats that exist to wireless LANS, these include:

✓ Rogue Access Points/Ad-Hoc Networks
✓ Denial of Service
✓ Configuration Problems (Mis Configurations/Incomplete Configurations)
✓ Passive Capturing

Wireless Network Attacks

- Wi-Fi networks can be vulnerable to a variety of different attacks. Because of this, it’s important to be aware of them so you can take the necessary steps to prevent and reduce their impact.
- Different kinds of attacks are Encrypted traffic, Rogue networks, Physical security problems, Vulnerable wireless workstations, Default configuration settings

✓ **Encrypted traffic**

- Wireless traffic can be captured directly out of the airwaves, making this communications medium susceptible to malicious eavesdropping.
- Unless the traffic is encrypted, it’s sent and received in clear text just like on a standard wired network.
- On top of that, the 802.11 encryption protocol, Wired Equivalent Privacy (WEP), has its own weakness that allows hackers to crack the encryption keys and decrypt the captured traffic.

✓ **Rogue networks**

- Watch out for unauthorized Access Points and wireless clients attached to your network that are running in ad-hoc mode.
- Using NetStumbler or your client manager software, you can test for Access Points that don’t belong on your network.
- You can also use the network monitoring features in a WLAN analyzer such as AiroPeek.
- Walk around your building or campus to perform this test to see what you can find.
- Physically look for devices that don’t belong a well-placed Access Point or WLAN client that’s turned off won’t show up in your network analysis tools.
- Search near the outskirts of the building or near any publicly accessible areas.
- Scope out boardrooms and the offices of upper level managers for any unauthorized devices. These are places that are typically off limits but often are used as locations for hackers to set up rogue Access Points.

✓ **Physical-security problems**

- Various physical-security vulnerabilities can result in physical theft, the reconfiguration of wireless devices, and the capturing of confidential information.
- You should look for the security vulnerabilities when testing your systems such as Access Points mounted on the outside of a building and accessible to the public,Poorly mounted antennas or the wrong types of antennas that broadcast too strong a signal and that are accessible to the public.
- You can view the signal strength in NetStumbler or your wireless client manager.

✓ **Vulnerable wireless workstations**

- Wireless workstations have tons of security vulnerabilities from weak passwords to unpatched security holes to the storage of WEP(Wired Equivalent Privacy) keys locally.
- One serious vulnerability is for wireless clients using the Orinoco wireless card.
- The Orinoco Client Manager software stores encrypted WEP keys in the Windows Registry even for multiple networks.

✓ **Default configuration settings**

- Similar to wireless workstations, wireless Access Points have many known vulnerabilities.
- The most common ones are default SSIDs (Service Set IDentifier) and admin passwords. The more specific ones occur only on certain hardware and software versions that are posted in vulnerability databases and vendor Web sites.

- The one vulnerability that stands out above all others is that certain Access Poinits, including Linksys, D-Link, and more, are susceptible to a vulnerability that exposes any WEP key(s), MAC(Media Access Control) address filters, and even the admin password! All that hackers have to do to exploit this is to send a broadcast packet on UDP port 27155 with a string of gstsearch.

6.2 Operating system hacking

- An operating system is a program that acts as an interface between the software and the computer hardware. It is an integrated set of specialized programs used to manage overall resources and operations of the computer. It is specialized software that controls and monitors the execution of all other programs that reside in the computer, including application programs and other system software. Many Operating systems are available now days.
- Many security flaws in the headlines aren't new. They're variants of vulnerabilities that have been around for a long time in UNIX and Linux, such as the Remote Procedure Call vulnerabilities that the Blaster worm used.
- You've heard the saying "the more things change, the more they stay the same." That applies here, too.
- Most Windows attacks are prevented if the patches were properly applied. Thus, poor security management is often the real reason.

Windows

- ✓ The Microsoft Windows OS is the most widely used OS in the world.
- ✓ It's also the most widely hacked, because Microsoft doesn't care as much about security as other OS vendors? The answer is no.Numerous security mistakes were unnoticed especially in the Windows NT days but because Microsoft products are so pervasive throughout networks. Microsoft is the easiest vendor to pick on, and often its Microsoft products that end up in the crosshairs of hackers. This is the same reason for many vulnerability alerts on Microsoft products. The one positive about hackers is that they're driving the requirement for better security!
- ✓ There are variants of vulnerabilities that have been around for a long time in UNIX and Linux, such as the RPC vulnerabilities that the Blaster worm used. Most Windows attacks are prevented if the patches were properly applied. Thus, poor security management is often the real reason Windows attacks are successful
  - Much vulnerability have been published for windows operating system.
  - Some of the common vulnerabilities found in all versions of windows are: DoS, Remote Code Execution, Memory Corruption, Overflow, Sql Injection, XSS, Http Response Splitting, Directory Traversal, Bypass something Gain Information /Privileges, CSRF File Inclusion etc.
  - The maximum number of vulnerabilities detected were of Gaining Privileges by which the confidentiality and integrity was highly impacted.

- **Windows Vulnerabilities**
    - ✓ Due to the ease of use of Windows, many organizations have moved to the Microsoft platform for their networking needs.
    - ✓ Many businesses especially the small to medium sized ones depend solely on the Windows OS for network usage.
    - ✓ Many large organizations run critical servers such as Web servers and database servers on the Windows platform.
    - ✓ If security vulnerabilities aren't addressed and managed properly, they can bring a network or an entire organization to its knees.
    - ✓ When Windows and other Microsoft software are attacked especially by a widespread Internet-based worm or virus hundreds of thousands of organizations and millions of computers are affected.
    - ✓ Many **well-known attacks against Windows** can lead to

- Leakage of confidential information, including files being copied and credit card numbers being stolen
- Passwords being cracked and used to carry out other attacks
- Systems taken completely offline by DoS attacks
- Entire databases being corrupted or deleted when insecure Windows-based systems are attacked, serious things can happen to a tremendous number of computers around the world.
- Autoplay feature came in Windows XP. This feature checks removable media/ devices then identifies and launches appropriate application based on its contents. This feature is useful for authentic users but is a gateway for an attacker.
- Clipboard vulnerability can allow attacker to get access to the sensitive clipboard data. In windows clipboard is common for all applications. This may lead to access and modification in the clipboard of all applications in the operating system.
- MS-Windows stores its configuration settings and options in a hierarchical database which is known as windows Registry. Registry is used for low level operating system settings and for settings of applications running on the platform.

- **LINUX**
    - ✓ It is the latest flavor of UNIX that has really taken off in corporate networks.
    - ✓ It is the competitor Operating System for Microsoft.
    - ✓ A common misunderstanding is that Windows is the most insecure operating system. However, Linux and most of its sister variants of UNIX are prone to the same security vulnerabilities as any other operating system.
    - ✓ Hackers are attacking Linux because of its popularity and growing usage in today's network environment, because some versions of Linux are free.
    - ✓ Many organizations are installing Linux for their Web servers and e-mail servers in expectations of saving money.
    - ✓ Linux has grown in popularity for other reasons, including the following:

- Ample resources available, including books, Web sites, and consultant expertise.
- Perception that Linux is more secure than Windows.

- Unlikeliness that Linux will get hit with as many viruses (not necessarily worms) as Windows and its applications do. This is an area where Linux excels when it comes to security, but it probably won't stay that way.
- Increased buy-in from other UNIX vendors, including IBM and Sun Micro systems
- Growing ease of use.

- **Linux Vulnerabilities**
    - ✓ Vulnerabilities and hacker attacks against Linux are affecting a growing number of organizations especially e-commerce companies and ISPs that rely on Linux for many of their systems.
    - ✓ When Linux systems are hacked, the victim organizations can experience the same side effects as if they were running Windows, including:
        - Leakage of confidential intellectual property and customer information
        - Passwords being cracked
        - Systems taken completely offline by DoS attacks
        - Corrupted or deleted databases

6.3 Applications Hacking:-

6.3.1 Messaging System

Messaging systems are those e-mail and instant messaging (IM) applications that we depend on are often hacked within a network. Why? Because messaging software both at the server and client level is vulnerable because network administrators forget about securing these systems, believe that antivirus software is all that's needed to keep trouble away, and ignore the existing security vulnerabilities.

- **Messaging system Vulnerabilities**
    - ✓ E-mail and instant-messaging applications are hacking targets on your network.
    - ✓ In fact, e-mail systems are some of the most targeted.
    - ✓ A ton of vulnerabilities are inherent in messaging systems.
    - ✓ The following factors can create **weaknesses**:
        - Security is rarely integrated into software development.
        - Convenience and usability often outweigh the need for security.
        - Many of the messaging protocols were not designed with security in mind.
        - Especially those developed several decades ago, when security wasn't nearly the issue it is today.
- ✓ Many hacker attacks against messaging systems are just minor nuisances. Others can inflict serious harm on your information and your organization's reputation. The **hacker attacks against messaging systems** include these:
    - Transmitting malware
    - Crashing servers
    - Obtaining remote control of workstations
    - Capturing and modifying confidential information as it travels across the network
    - Perusing e-mails in e-mail databases on servers and workstations
    - Perusing instant-messaging log files on workstation hard drives

  - Gathering messaging trend information, via log files or a network analyzer, that can tip off the hacker about conversations between people and organizations
  - Gathering internal network configuration information, such as hostname and IP addresses

✓ Hacker attacks like these can lead to such problems as lost business, unauthorized and potentially illegal disclosure of confidential information
and loss of information.

Email Attacks

- Many people rely on the Internet for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.
- Email is a universal service used by number of people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.
- The following e-mail attacks use the most common e-mail security vulnerabilities. Some of these attacks require the basic hacking methodologies, gathering public information, scanning and enumerating your systems, and attacking. Others can be carried out by sending e-mails or capturing network traffic.
- Different email attacks are email bomb, banner etc.

- **Email Bombs**
  - ✓ E-mail bombs can crash a server and provide unauthorized administrator access.
  - ✓ They attack by creating DoS conditions against your e-mail software and even your network and Internet connection by taking up so much bandwidth and requiring so much storage space.
  - ✓ An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.
  - ✓ An email bomb is also known as a **letter bomb.**
  - ✓ Different email bomb attacks are as attachment overloading attack, connection attack, autoresponder attack.

1. **Attachment Overloading Attack**
   - An attacker can create an **attachment-overloading attack** by sending hundreds or thousands of e-mails with very large attachments.
   - Attachment overloading attacks may have a couple of different goals
   - The whole e-mail server may be targeted for a complete interruption of service with these failures like **storage overload and bandwidth blocking.**

a. Storage overload

- Multiple large messages can quickly fill the total storage capacity of an e-mail server. If the messages aren't automatically deleted by the server or manually deleted by individual user accounts, the server will be unable to receive new messages.

- This can create a serious DoS problem for your e-mail system, either crashing it or requiring you take your system offline to clean up the junk that has accumulated. E.g. 100MB file attachment sent ten times to 80 users can take 80GB of storage space.

b. Bandwidth blocking

- An attacker can crash your e-mail service or bring it to a crawl by filling the incoming Internet connection with junk. Even if your system automatically identifies and discards obvious attachment attacks, the bogus messages eat resources and delay processing of valid messages

Countermeasures (Attachment-Overloading Attack)

These countermeasures can help prevent attachment-overloading attacks:

- **Limit the size of either e-mails or e-mail attachments.** Check for this option in e-mail server configuration options, e-mail content filtering, and e-mail clients. This is the best protection against attachment overloading.
- **Limit each user's space on the server**. This denies large attachments from being written to disk. Limit message sizes for inbound and even outbound messages if you want to prevent a user from launching this attack inside your network.

2. Connection Attack

- ✓ A hacker can send a huge amount of e-mails simultaneously to addresses on your network.
- ✓ These connection attacks can cause the server to give up on servicing any inbound or outbound TCP requests.
- ✓ This can lead to a complete server lockup or a crash, often resulting in a condition where the attacker is allowed administrator or root access to the system!
- ✓ This attack is often carried out as spam attack.

Countermeasures (Connection Attacks)

- ✓ Many e-mail servers allow you to limit the number of resources used for inbound connections.
- ✓ It can be impossible to completely stop an unlimited amount of inbound requests.
- ✓ However, you can minimize the impact of the attack. This setting limits the amount of server processor time, which can help prevent a DoS attack.
- ✓ Even in large companies, there's no reason that thousands of inbound e-mail deliveries should be necessary within a short time period.

3. Autoresponders Attack

- ✓ This is an interesting attack to find two or more users on the same or different e-mail systems that have autoresponder configured.
- ✓ Autoresponder is that annoying automatic e-mail response you often get back from random users when you're subscribing to a mailing list.

- ✓ A message goes to the mailing list of subscribers and then users have their e-mail configured to automatically respond back, saying they're out of the office or, on vacation.
- ✓ An autoresponder attack is a pretty easy hack.
- ✓ Many unsuspecting users and e-mail administrators never know what hit them!
- ✓ The hacker sends each of the two (or more) users an e-mail from the other simply by masquerading as that
- ✓ This attack can create a never-ending loop that bounces thousands of messages back and forth between users.
- ✓ This can create a DoS condition by filling either the user's individual disk space quota on the e-mail server or the e-mail server's entire disk space.

Countermeasures (Autoresponder attack)

- ✓ The best countermeasure for an autoresponder attack is to make policy that no one sets up an autoresponder message.
- ✓ Prevent e-mail attacks as far considering perimeter of your network.
- ✓ The more traffic or malicious behavior you keep off, your e-mail servers and clients are better.

- **Banners**
  - ✓ One of the first orders of business for a hacker when hacking an e-mail server is performing a basic banner grab to see whether he can tell what e-mail server Software is running
  - ✓ This is one of the most critical tests to find out what the World knows about your SMTP, POP3, and IMAP servers.
  - ✓ Gathering Information
  - when a basic telnet connection is made on port 25 (SMTP) banner displayed on an e-mail server.
  - To do this, at a command prompt, Simply enter telnet IP or hostname.
  - From that we get what e-mail software type and version of the server is running. This information can give hackers some ideas about possible attacks, especially if they search a vulnerability database for known vulnerabilities of that software version.
  - If you've changed your default SMTP banner, don't think that no one can figure out the version.
  - One Linux-based tool called smtpscan determines e-mail server version information based on how the server responds to malformed SMTP requests.

Countermeasures (Banners)

There is not a 100 percent secure way of disguising banner information.

Following are some banner security tips for SMTP, POP3, and IMAP servers:

- Change your default banners to cover up the information.
- Make sure that you're always running the latest software patches.
- Harden your server as much as possible by using well-known best practices

General Best Practices for minimizing email security risk

The following countermeasure helps to keep email messages as secure as possible: -

- ✓ Use of right software can neutralize many threats such as - Use malware protection software on the e-mail server better, Apply the latest operating system and e-mail application security patches consistently.
- ✓ Use of encrypted messages or messaging system.
- ✓ Put your e-mail server behind a firewall, preferably in a DMZ that's on a different network segment from the Internet and from your internal LAN.
- ✓ Disable unused protocols and services on your e-mail server.
- ✓ Run your e-mail server on a dedicated server, if possible, to help keep hackers out of other servers and information if the server is hacked.
- ✓ Log all transactions with the server in case you need to investigate malicious use in the future.
- ✓ If your server doesn't need e-mail services running (SMTP, POP3, and IMAP) disable them immediately.
- ✓ Email monitoring can detect and block messages sent from compromised accounts.
- ✓ Email filtering can block certain types of attachments that are known to carry malicious content.
- ✓ Secure email client configurations can also reduce the risk of malicious email.
- ✓ Checking to see if the email address of a questionable message matches the reply-to email address.
- ✓ Verifying that URLs in an email go to legitimate websites.

6.3.2 Web Applications

- Web applications, like e-mail are common hacker targets because they are everywhere and often open for anyone to poke around in.
- Basic Web sites used for marketing, contact information, document downloads and so on are a common target for hackers especially the script-kiddie's types to deface.
- However, for criminal hackers, Web sites that store valuable information, like credit-card and Social Security numbers, are especially attractive.
- Why are Web applications so vulnerable? The general consent is they're vulnerable because of poor software development and testing practices. Sound familiar? It should, because this is the same problem that affects operating systems and practically all computer systems.
- This is the side effect of relying on software compilers to perform error checking, lack of user demand for higher-quality software and emphasizing time-to-market instead of security and stability.

- **Web application Vulnerabilities**

- ✓ Hacker attacks against insecure Web applications via Hypertext Transfer Protocol (HTTP) make up the majority of all Internet-related attacks.
- ✓ Most of these attacks can be carried out even if the HTTP traffic is encrypted (via HTTPS or HTTP over SSL) because the communications medium has nothing to do with these attacks.

- ✓ The security vulnerabilities actually lie within either the Web applications themselves or the Web server and browser software that the applications run on and communicate with.
- ✓ Many attacks against Web applications are just minor nuisances or may not affect confidential information or system availability.
- ✓ However, some attacks can cause destruction on your systems. Whether the Web attack is against a basic brochure ware site or against the company's most critical customer server, these attacks can hurt your organization.
- ✓ Some other **web application security vulnerabilities** are as follows

SQL Injection

- Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.
- Injection occurs when the user input is sent to an interpreter as part of command or query and trick the interpreter into executing unintended commands and gives access to unauthorized data.

Cross site scripting

- Cross Site Scripting is also shortly known as XSS.
- XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather than at the server side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.
- Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious websites.
- XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

Security Misconfiguration

- Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these are properly configured, an attacker can have unauthorized access to sensitive data or functionality.
- Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security.

Directory Traversals

- ✓ A directory traversal is a really basic attack, but it can turn up interesting information about a Web site.
- ✓ This attack is basically browsing a site and looking for clues about the server's directory structure.
- ✓ Properly controlling access to web content is crucial for running a secure web server.

- ✓ Directory traversal or Path Traversal is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.
- ✓ Web servers provide two main levels of security mechanisms

Access Control Lists (ACLs)

- An Access Control List is used in the authorization process.
- It is a list which the web server's administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights

Root directory

- The root directory is the top-most directory on the server file System.
- User access is confined to the root directory, meaning users are unable to access directories or files outside of the root

Countermeasures (Directory Traversal Attack)

- ✓ There are two main countermeasures to having files compromised via Malicious directory traversals:
- o **Don't store old, sensitive, or otherwise nonpublic files on your Web server.**
- The only files that should be in your /htdocs or Document Root folder are those that are needed for the site to function properly.
- These files should not contain confidential information that you don't want the world to see.
- o **Ensure that your Web server is properly configured to allow public access only to those directories that are needed for the site to function.**
- Minimum necessary privileges are key here, so provide access only to the bare-minimum files and directories needed for the Web application to perform properly.

6.3.3 Database System Vulnerabilities

- ✓ Database management systems are nearly as complex as the operating systems on which they reside.
- ✓ As a security professional, there is need to assess and manage any potential security problems.
- ✓ Following are the Vulnerabilities in database management systems
    - ➢ **Loose access permissions.** Like applications and operating systems, database management systems have schemes of access controls that are often designed far too loosely, which permits more access to critical and sensitive information than is appropriate. This can also include failures to implement cryptography as an access control when appropriate.
    - ➢ **Excessive retention of sensitive data.** Keeping sensitive data longer than necessary increases the impact of a security breach.
    - ➢ **Aggregation of personally identifiable information.** The practice known as aggregation of data about citizens is a potentially risky undertaking that can result in an organization possessing sensitive personal information.

Sometimes, this happens when an organization deposits historic data from various sources into a data warehouse, where this disparate sensitive data is brought together for the first time. The result is a gold mine or a time bomb, depending on how you look at it.

Best practices for minimizing database security risks

- ✓ While some attackers still focus on denial of service attacks, cyber criminals often target the database because that is where the money is.
- ✓ The databases that power web sites hold a great deal of profitable information for someone looking to steal credit card information or personal identities.
- ✓ Database security on its own is an extremely in-depth topic that could never be covered in the course of one article; however there are a few best practices that can help even the smallest of businesses secure their database enough to make an attacker move on to an easier target.

Separate the Database and Web Servers

- Keep the database server separate from the web server.
- When installing most web software, the database is created for you. To make things easy, this database is created on the same server where the application itself is being installed, the web server. Unfortunately, this makes access to the data all too easy for an attacker to access.
- If they are able to crack the administrator account for the web server, the data is readily available to them.
- Instead, a database should reside on a separate database server located behind a firewall, not in the DMZ (Demiltarized Zone) with the web server. While this makes for a more complicated setup, the security benefits are well worth the effort.

Encrypt Stored Files

- Encrypt stored files.
- White Hat security estimates that 83 percent of all web sites are vulnerable to at least one form of attack.
- The stored files of a web application often contain information about the databases the software needs to connect to.
- This information, if stored in plain text like many default installations do, provide the keys an attacker needs to access sensitive data.

Encrypt Your Backups Too

- Encrypt back-up files.
- Not all data theft happens as a result of an outside attack. Sometimes, it’s the people we trust most that are the attackers.

Use a WAF

- Employ web application firewalls.
- The misconception here might be that protecting the web server has nothing to do with the database.

- Nothing could be further from the truth. In addition to protecting a site against cross-site scripting vulnerabilities and web site vandalism, a good application firewall can thwart SQL injection attacks as well.
- By preventing the injection of SQL queries by an attacker, the firewall can help keep sensitive information stored in the database away from prying eyes.

Keep Patches Current

- Keep patches current. This is one area where administrators often come up short.
- Web sites that are rich with third-party applications, widgets, components and various other plug-ins and add-ons can easily find themselves a target to an exploit that should have been patched.

Minimize Use of 3rd Party Apps

- Keep third-party applications to a minimum.
- We all want our web site to be filled with interactive widgets and sidebars filled with cool content, but any app that pulls from the database is a potential threat.
- Many of these applications are created by hobbyists or programmers who discontinue support for them.

Don't Use a Shared Server

- Avoid using a shared web server if your database holds sensitive information.
- While it may be easier, and cheaper, to host your site with a hosting provider you are essentially placing the security of your information in the hands of someone else.
- If you have no other choice, make sure to review their security policies and speak with them about what their responsibilities are should your data become compromised.

Enable Security Controls

- Enable security controls on your database.
- While most databases nowadays will enable security controls by default, it never hurts for you to go through and make sure you check the security controls to see if this was done.
- Keep in mind that securing your database means you have to shift your focus from web developer to database administrator. In small businesses, this may mean added responsibilities and additional buy in from management.
- However, getting everyone on the same page when it comes to security can make a difference between preventing an attack and responding to an attack.

References:

1. Hacking for Dummies (5th Edition), Kevin Beaver CISSP, Wiley Publishing Inc.
 ISBN: 978-81-265-6554-2
2. CISSP for Dummies(5th Edition),Lawrence C. Miller, Peter H. Gregory, ISBN: 978-1-119-21023-8
3. http://www.applicure.com/blog/database-security-best-practice
4. https://thecybersecurityplace.com/database-hacking-its-prevention
5. https://www.valencynetworks.com/blogs/cyber-attacks-explained-database-hacking
6. https://www.acunetix.com/websitesecurity/directory-traversal

7. https://www.veracode.com/security/directory-traversal

Sample Multiple Choice Questions:

1. SNMP stands for
    a. Simple Network Messaging Protocol
    b. Simple Network Mailing Protocol
    c. Simple Network Management Protocol
    d. Simple Network Master Protocol

2. Which of the following tool is used for Network Testing and port Scanning
    a. NetCat
    b. SuperScan
    c. NetScan
    d. All of Above

3. Banner grabbing is often used for
    a. White Hat Hacking
    b. Black Hat Hacking
    c. Gray Hat Hacking
    d. Script Kiddies

4. An attacker can create an……………………attack by sending hundreds or thousands of e-mails with very large attachments.
    a. Connection Attack
    b. Auto responder Attack
    c. Attachment Overloading Attack
    d. All of the above