Security and Privacy for Internet of Things (IoT): Issues and Solutions

Sindhu Rajendran[1*], Surabhi Chaudhari[2],Varsha Kulkarni[1]
Department of Electronics and Communication[1],Department of Biotechnology[2]
R. V. College of Engineering Bangalore-560059

Abstract:*Due to digitalization, there is a need for a smart system; Internet of Things (IoT) is a collection of interconnected computer systems, mechanical and physical systems capable of transmitting data over a network without any human interference. There is no dearth for the new emerging technologies; we are surrounded by many smart devices in almost all the sectors, though the use of these technologies has made life convenient and easy, there is always a threat to our data because of the number of cyber-attacks. Hence, as the number of interrelated devices grows every day, the security and privacy issues magnify at the same rate. Though there are many algorithms for challenges from the security and vulnerability perspective, it is necessary to provide a holistic approach to overcoming these challenges. IoT has a three-layered and five-layered architecture and there are security threats associated with each of these layers.This chapter presents an analysis as per the security requirements emphasizing the threat and security issues for these IoT devices, different encryption techniques, and algorithms used for measurement. Also, this chapter will discuss the emerging and most widely used or proposed IoT technologies and their applications in real-time.*

Keywords: Internet of Thing(IoT), Security threat, Privacy, Encryption

1. Introduction [1]

Internet can be defined as a networking platform that links individuals to data whereas IOT which is Internet of Things is an integrated system of distinctly addressable physical objects with various degrees of computing, sensing, and actuation capability that share the capacity to interoperate and interact using the Internet as their shared forum. Thus, the key aim of the Internet of Things is to link objects to other objects, entities, via any network, route, or device at any time or location. The Internet of Things is increasingly termed as the following step of the development of the Internet. IoT would allow ordinary devices to be connected to the internet to accomplish myriad different goals.

All devices related to the internet may be grouped into three sections in Internet of Things [2]:

1. Things in collecting and sending information
2. Things in receiving information and acting on it
3. Things doing both

1. Collecting and sending information

Such tools are called Sensors. These devices detect changes in the environment and send information to other electronic devices. RFID sensors, Motion sensors, Light sensors, Sound/Acoustic sensors, Humidity/Moisture sensors, Temperature sensors, etc. are some examples of such devices. These sensors, together with a connection, allow data from the environment to be collected automatically which, in turn, leads to smarter decisions.

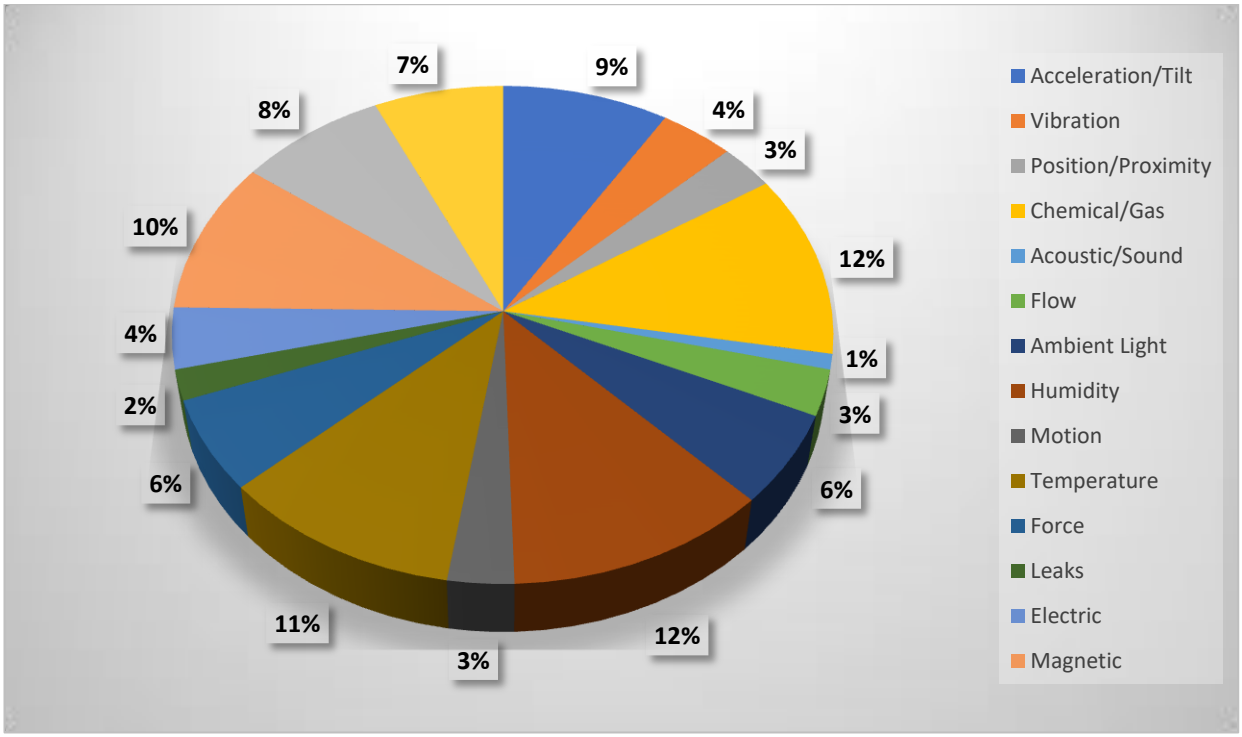

Fig 1: Sensors in IoT [3]

2. Receiving and acting on Information
   As discussed above, there are a set of devices that can collect the information and send it to other devices. These devices receive information and act based on the information received.

3. Doing Both
   The real potential of IoT is that the devices can do above mentioned both i.e. collection & sending information and receiving & acting on the information.

1.1 Data Flow in IoT

In any given IoT device, the sensors on the other end of the line collect information and start putting it onto the network that makes it available through the internet. All of this information is stored depending upon the network it is allocated to. The sensor data can be accessed by accessing the network and the

server. Usually, all data of sensors, records, databases are stored in the form of Big Data. Big Data is the next step after IoT. All of this data is retrieved according to the requirement. An analysis is performed on the structure of the data and is then provided to any user.

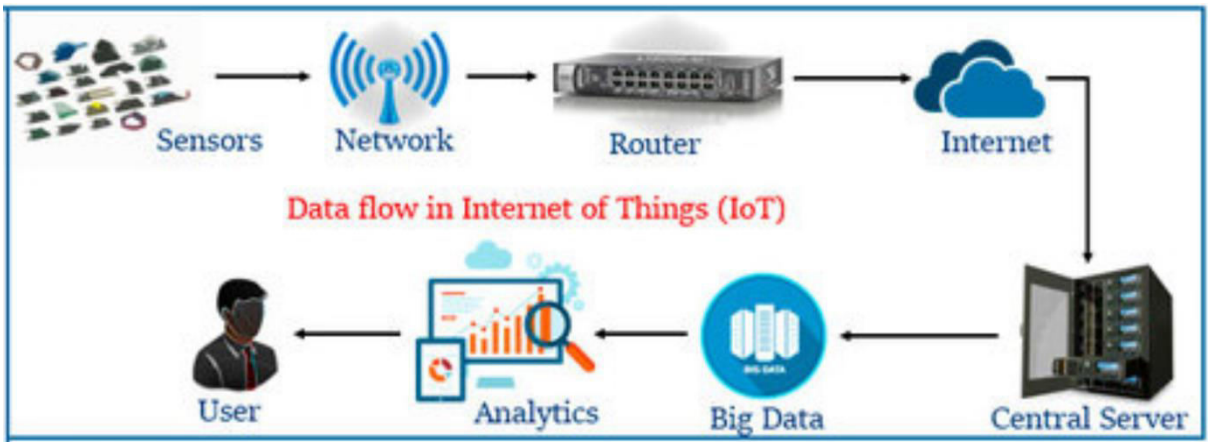

Fig 2: Data Flow in IoT [4]

2. Applications of IoT [5,6]

2.1 Consumer applications

- Smart Home: IoT is an important part of home automation. It involves applications like increasing energy efficiency, security, monitoring the temperature, interconnection between all the devices inside the house. Energy-efficient devices work on two parameters which are the number of the people in the house and the external (weather) conditions. So these devices count the number of people in the house and light up the lights in their respective places rather than lighting up the whole house. It also analyses the weather conditions and decides the number of lights required. Under security, various devices such as cameras, gas sensors, smoke detectors, motion detectors, etc are used [7].
- Eldercare: one important application of IoT is making the life of the disabled easier. Few examples are, IoT enables the person to control the devices in the house by their voice rather than physically doing it. The security alerts are connected to their cochlear implants which can be heard by them.

2.2 Commercial applications

- Medical and Healthcare: IoT in medicine and healthcare facilitates "remote health monitoring" and "emergency notification" systems. Such health monitoring gadgets can be pacemakers, Fitbit, hearing aids. Smart beds have been in various hospitals to monitor if a patient attempts to get up. As we know that many medical items like vaccines, medicines, and organic material are stored in the freezer, the conditions inside these medical fridges can be controlled by IoT [8].

- Media and Entertainment: The real benefit of IoT in the media and entertainment industry is creating high-quality data and creating targeted advertisements are more inclined towards the needs of the people.
- Transportation: The IoT has a significant role in the incorporation of communication, monitoring, or transmission of information across the transport system. It can be used in maintaining the vehicle health, curbing traffic, smart parking, improving fleet logistics, smart control traffic, safety assistance, electronic toll collectors, etc. This required incorporation of V2X communications which takes place in three ways: "Vehicle-to-vehicle communication; vehicle-to-infrastructure communication and vehicle-to-pedestrian communication".
- Building and Home automation: Various applications of IoT are measuring home conditions where the house is equipped with sensors to measure temperature, humidity, proximity, motion, or light. These sensors store the data and allow the user to access it anytime and anywhere. The next application is managing home appliances where the on/off commands for lamps, fans, air conditioners from anywhere and anytime. One of the most important applications is controlling home access which is basically comparing the identification attributes of the people with the identification attributes stored in the database and in turn deciding to give access or deny it.

2.3 Industrial application

- Manufacturing: The IoT enables easy manufacture of innovative goods and to automate output and delivery in real-time by utilizing networking equipment, sensors, and control devices together.
- Agriculture: In agriculture, various IoT applications, like collecting data on rainfall, temperature, wind speed, humidity, pest infestation, and soil quality are there. Such information may be utilized to simplify agricultural practices, take educated decisions to increase quality and quantity, mitigate danger or loss, and reduce crop management efforts. Farmers can now track the temperature and humidity of the soil beforehand and also apply IoT-acquired data to precision fertilization programs.

2.4 Infrastructure

- Energy management: The introduction of sensing and actuation technologies connecting to the internet is anticipated to optimize energy use. It is predicted that IoT sensors would be integrated into all sorts of energy utilizing equipment and would be able to interface with power production.
- Environmental monitoring: The IoT's environmental surveillance systems usually use sensors to help safeguard the atmosphere by tracking environmental situations like animal movements and their habitats. Emergency responders may often utilize the electronic equipment connecting to the Internet and are used as alert systems to offer more effective assistance.

2.5 Military applications

Another application of IoT is the Internet of Military Things (IoMT) in the military realm for monitoring, surveillance, and other purposes relevant to the war. This is highly inspired by potential combat possibilities in an urban world and includes the usage of sensors, weapons, vehicles, drones, robots, human-wearable biometrics, and many more related advanced technologies on the battlefield.

3. Architecture of IoT [9,10]

Internet of things consists of two types of architecture. Three-layered and Five layered.

The three layers of the IoT Three-layered Architecture are as follows:

1. Perception layer: It is the bottom-most layer of IoT architecture. It is the physical layer of sensors that aid in the sensing and collection of data from any environment. Hence, examples of devices in this layer are sensor networks, embedded systems, RFID tags, GPRS, etc. which sense the physical parameters and detect the smart objects present in the surrounding.
2. Network layer: It is the middle layer between the perception and application layer. It transfers the data collected by the sensors to further layers. It is essential for maintaining connectivity with other network devices, smart objects, and servers. It transmits and processes the data received from various sensors. For this, it should follow a standard universal protocol for transmitting information from various sensor nodes (heterogeneous devices).
3. Application layer: It is the topmost layer of the IoT architecture. It is required to provide application-specific services to users. This layer gives a user interface to different users to access various applications. It describes multiple applications such as smart homes, cities, smart health.

This architecture provides the reader with an abstract of IoT. However, it is not enough to understand all the communication that takes place and does not provide much information for research purposes.
Therefore, Five-layered architecture is preferred by research and development departments.
The layers of the Five-layered architecture are as follows:

1. Perception layer: Same role as the Three-layered architecture to gather information about any environment.
2. Transport layer: It sends sensor information through networks such as LAN, 3G, RFID, NFC, Ethernet, Wi-Fi, etc. It is a link between the perception and the processing layers.
3. Processing layer: It is the middle layer. It holds, analyses, and manages enormous data from the transportation layer. It manages the lower layers and delivers a wide range of services. It can use technologies like databases, cloud computing, and data processing modules.
4. Application layer: Same role as in the Three-layered architecture to determine the types of applications of IoT which are more authenticated and safer.
5. Business layer: It effectively governs the whole network, including applications, business and benefit structures, and user privacy.

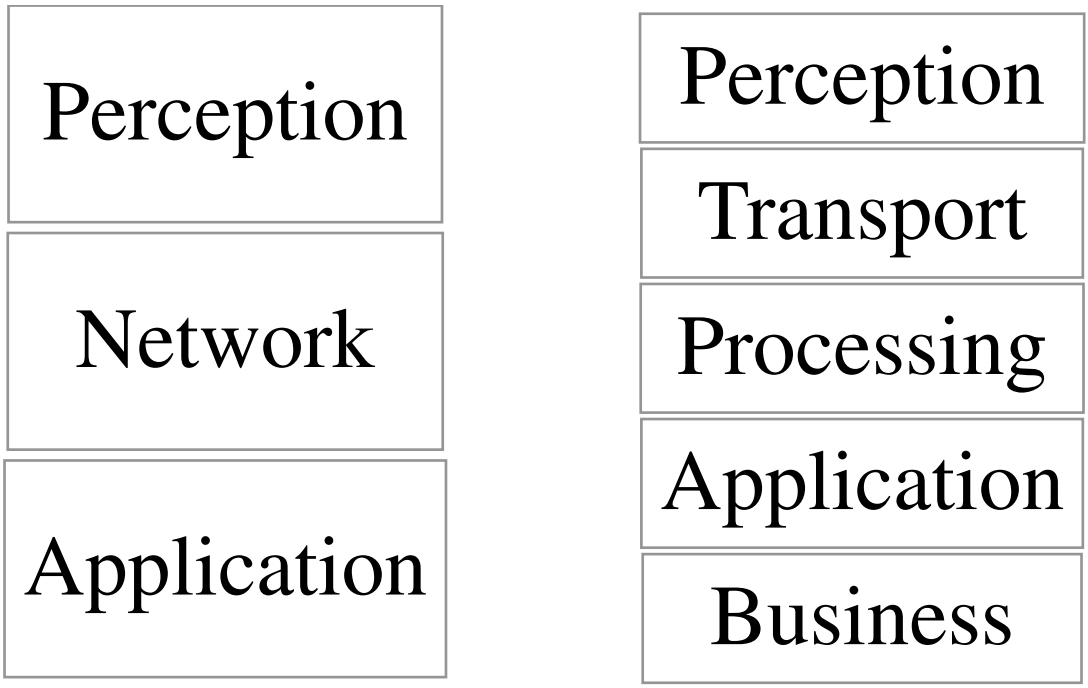

Fig 3: (i) Three-layered architecture; (ii) Five-layered architecture

4. Threats Involved [11,12]

In several places around us, information and networking systems are utilized in considerable detail. Technology innovation is pushing expanded automation in various ways. Tasks carried out by humans are increasingly done by computers. As this technology is cheap, simple devices with minimal computing capacity also can be connected to each other. Even though all these devices entail the high potential for expansion and flexibility, they are not free from the risk of security problems. This section gives a layered approach to security threats.

4.1 SECURITY THREATS IN PERCEPTION LAYER

This layer faces security threats due to the vulnerability of sensors from direct physical attacks like tampering etc.

1. Tampering: It is an event where an attacker makes physical alterations to the computer or the communication channel. This physical layer offers an excellent surface for an attack. In this, the attacker physically takes control of the sensors and actuators. It can then be stolen, replaced, or accessed which violates the integrity and privacy of the system.
2. Denial of Service (DoS): It involves changing the physical link between the communication nodes. Since most of the IoT devices interact in the physical layer via radio access technology, such kind of Denial of Service (DoS) attacks are commonly seen in wireless communication.
3. Signal/Radio jamming: A type of DoS taking place by signal distortion or jamming.

4. Spoofing: This type of attack occurs when the attacker initially sends a fake relay message to the network resulting in the node taking its identity wrongly and having it look from the original source. In this case, the attacker is most frequently granted complete access to the network, resulting in it becoming exposed.
5. Node outage: This attack is related to the network technically or physically; interruption implies a lack of connection and tends to halt the network feature functionality. Because of this attack, most of the Node resources or activities are halted.
6. Eavesdropping: It's a kind of threat when an individual intercepts encrypted messages. It's possible because of the wireless features of the RFID device that lets the attacker delete sensitive details such as a password or any other data that leaves the network insecure in effect.

4.2 SECURITY THREATS IN NETWORK LAYER

Threats in the network layer are

A) Denial of Service (DoS) attacks

1. Collision: Collision that has been intentionally produced may be called a jamming-type attack because it particularly targets the network layer which involves the wireless component of the information flow. While the attackers are not jamming the complete signal, they are reducing the network's efficiency, or even making the contact impossible.
2. Exhaustion: Targeted resource attack, i.e. of a given node, can consume networking resources such as buffers, storage capacity, and throughput.
3. Unfairness: Data Connection layer attacks also strike at corrupting WSN's fairness mechanisms. Their approach involves depletion, or collision, of intended WSN tools. Then, such approaches contribute to poor Denial of Service; but the effect is magnified by the number of nodes involved.
4. Spoofed routing information: While packet load information is generally covered in the channel, it does not provide routing and other header data. Attackers may spoof or modify, delete, or replay IP or transportation protocol details (UDP, TCP channel, etc) to interrupt network traffic. It could lead to routing loops, extended routes, fake errors, and much more.
5. Selective Forwarding: Some of the messages are not sent by a malicious node in this attack, so they are discarded selectively, meaning they cannot spread later. The individual responsible for changing or deleting packets comes from a few chosen nodes and often forwards the residual traffic in order not to expose their illegal activity.
6. Sinkhole attack: Many nodes or destinations are created more desirable to traffic in such forms of attacks (e.g. by tampering details on routing management) than some usual nodes. The messages may be lost (selective forwarding) after entering the sinkhole node, which can be distributed via modified information, otherwise modified.
7. Wormhole attack: Maliciously designed wormhole, low latency connection, which enables the attacker to replay messages. An attacker at one point in the network collects packets utilizing a wormhole attack and "tunnels" them to another place in the network, which is then replayed over the network.
8. Sybil attack: Sybil type attacker uses multi-identity nodes or computers. These produce traffic which tends to be multi-source or also distributed. This approach corrupts the usage of services for fairness, redundancy, or voting concepts that were initially present in the system.

9. Flooding: The network flooding and its potential prevention have a broad variety of literature, owing to their complexity and their influence on our system's life. Nowadays the most disturbing is the DDoS flooding attacks.
10. Replication of nodes: An attacker can replicate the identity of a node and create an identity-like (virtual) node. It then sends fake data in his name so that the network can be interrupted by random routes.

B) Man-in-the-middle attacks

Man-in – the middle attack happens when an attacker has access to and may use information that is transferred between nodes. Data protection must be enforced to reduce the probability of this threat.

1. Replay attack: An attacker catches the signed packet, and while he/she cannot decipher it, he/she will re-send it to the planned party later. The replay risks can be eliminated by message sequence numbers and message authentication code (MAC).
2. Eavesdropping: An attacker will enter a communication path. This is a passive attack until the attacker changes the received packets marginally and returns them to every user. The method is known as a replay attack, a common spoofing subtype.
3. Routing Attack: Since routing information is not authenticated typically, an attacker can modify the routing information to create routing loops that significantly affect service efficiency.

4.3 SECURITY THREATS IN APPLICATION LAYER

Custom designed modules are used in the application layer depending on the user requirements; e.g. user interface to monitor devices in IoT. The security threats are mentioned below:

1. Sniffer / Loggers: In order to extract valuable details from the network traffic, attackers may insert sniffer/logger programs into the framework. The sniffer takes all sorts of passwords, directories (FTP directories, e-mail files), and reads email text. Many protocols are vulnerable to sniffing.
2. Injection: Attackers can inject code directly into the server-running program. This is a very simple attack, quick to use, and can contribute to some horrible consequences such as data destruction, data theft, and lack of transparency.
3. Session Hijacking: Personal identity is revealed in this attack by taking advantage of protection vulnerabilities in authentication and user control. This kind of attack is really normal and the assault results are very important. With someone else's identity, the attacker can do anything that the real user can do.
4. Distributed Denial of Service (DDoS): It’s a method of attack where multiple infected systems are used to damage a particular device. It is a traditional Denial of Service assault as it is conducted at the time by other users.
5. Social Engineering: This is a challenge to the application layer because attackers will obtain user knowledge and data through knowing each other, texting, etc.

5. Need for Privacy and Security

The Internet is a massive open publishing platform and as a result, has become troublesome concerning the notion of privacy. Everything one writes might be visible to anyone online: from when you wake up to posts on your day to day activities, from articles about your hobbies to posts about recreation with family. The story told online comes with the price of one's persona. it defines someone concerning friends and family and potential employers [13].

Need for privacy:

1. Data being visible to an abusive relative.
2. As any data can be obtained, there is a risk of assassination for citizens.
3. The group is targeted by people (religion, sexuality, political party, journalists).

Actions that reduce privacy [14]:

1. Indulging in someone's personal affairs and disturbing their wish for alone time
2. Disclosure of personal information of anyone can cause misrepresentation and is embarrassing for them.
3. Infringing the rights of someone and using their similarities to promote not your own interests.

Security is required to prevent Cyber Crimes such as [15]:

1. Backdoor
2. Denial of service attack
3. Direct-access attacks
4. Eavesdropping
5. Multi-vector, polymorphic attacks
6. Phishing
7. Privilege escalation
8. Social engineering
9. Spoofing
10. Tampering

It is necessary to implement security methods to protect users' privacy and prevent it from being misused, easily accessed. No security implies that any given data can be sold or brought by illegal organizations to favor them with strength such as blackmailing, belie, and supporting attacks on the people in the subject.[16]

In short, Privacy is necessary as it defines who people are as individuals, and what decisions they make daily. It gives space to be oneself without judgement, allows us to think without discrimination, and is an important element of giving us control over who knows what about us.

Precautions require keeping up-to-date security updates. Patches of software usually close a vulnerable path into the access code of a device. The wise precautionary defense is always the usage of two-factor authentication (2FA). 2FA involves an authorization of a secondary account using an add-on-time access code to the mobile device or e-mail of the customer.

6. Security Issues in IoT Devices [15]

The IoT devices are not the only tools we have in matters of trust. The confidentiality of individuals who come in contact with sensor paths through accident or design should be considered when more sensors and devices monitor and report data to the Internet. Such issues would be closely considered by IoT designers. Keeping information safe for things like healthcare is an obvious problem.

Cybercriminals have entered the black-market rate for data in recent years in electronic medical registers, which is significantly higher than bank account passwords. This trend is seemingly obvious. [13]

One is incapable of trusting any device as even seemingly harmless applications can leak private details. Hence, one must be ready to take precautions to avoid such a situation.

This can be shown with a small example of a parking lot in front of a shopping mall. Each parking bay is looked after by a sensor that makes use of a camera to tell if space is occupied. The sensors are all connected to a network and can provide data to the one who owns that parking lot. A light on the sensor helps guide the drivers to a free slot. This seems innocuous. This shopping mall came up with a mobile application for visitors to download so that they are more informed about the facilities. One of the features of this application is "find my car". This asked the user for the first characters on the license plate after which the app returns four potential matches of the cars by making use of optical character recognition from the mall's data server.

The returned images were thumbnails that were sufficient to recognize the car of interest, but the license plates were hardly clear. However, one security personnel had figured that the implementation was full of scope. With software, he was capable of accessing what information the app had sent requests from the server. He found that it was a simple unencrypted web request. The initial URL request consisted of several parameters, including a search string, number of results to be returned. It was easier for the creator of the service to return all available data than to restrict it. It included the license plate of every vehicle and the amount of time for which it had been parked. By making changes in the search parameters, he found that more than four matches could be requested and that license plate search could be removed. This meant a full list of license plates from all parking bays could be downloaded in a single web request at any time.

Although all the data is publicly available, there is a huge difference in ease of obtaining it between watching cars come and go at the entrance and scripting it on a computer at a regular time period. It has become a standard practice to never store passwords as cleartext. Applying standard mechanisms for password encryption is also considered these days to enhance protection.

The solution to this is by a method known as one-way hashing explained below.

ONE WAY HASHING [16]

It is a cryptographic method that is used to condense a random size chunk of data to fixed-sized, called the hash. It is known as one-way hashing as no easy way exists to recover the original data after the

hashing. Hashing algorithms are such that even a minute difference in input data is converted to a huge difference in the output hash. This is very useful for verifying if the two data are identical without having to store them for any comparison.

This is useful when the data to be compared is very large. Cryptographic hashes are widely used for password verification. Rather than store the password, the service provider stores a hash of the password which increases the security.

When the authentication is required, the hash is recalculated and if it is matched with the stored one, the service is sure that the password provided is correct. It is better to salt before applying a hash to the password. This adds random, extra text to the password before the hash is computed. The salt is stored with the hash, so the service can concatenate the two during verification. The salt prevents attackers who end up with a copy of the hash by easily comparing it with a dictionary of hashes to work out the password.

Making use of a one-way hashed version of the information instead which lets the originators find their data and allows statistics gathering and promotes no storing the data as recoverable.

7. Encryption Techniques

Encryption is the method of encoding information. Plain text is the original information which is converted to ciphertext after encryption. Only those with authorization can decipher and access the information. Encryption techniques make use of two variants, symmetric key, and public-key encryption. In the symmetric key, the encryption and decryption key are the same. However, in the public key, there is one key to encrypt the information which can be done by anyone, and a private key with the receiver to decrypt it. Encryption techniques have keys that are generated pseudo-randomly. This provides better security as it requires excessive computation to determine the key. Over the years, multiple algorithms have been developed to increase the complexity of the key and speed the computation for better performance. Below are the basic versions of all encryptions techniques that can be modified individually.

7.1 PUBLIC KEY INFRASTRUCTURE(PKI)[17]

PKI has a very efficientway to encrypt data as it is capable of providing an increased confidence levelto exchange information over any insecure surroundings, likeIoT. Mathematically linked keys are used by PK cryptography. Only a related key will be able to decode the information if the key were used to encrypt. Even if the public key is known, it is not possible to get the private key. Devices that validate patient details, apublic key can be used and the health monitoring devices can make use of a private key associated with it for decryption. The digital PKI certificates guarantee that the devices are correctly encrypted and the data is being transmitted securely.The Introduction of PKI in IoTdevicesgives rise to a major challenge. Even this encryption approach needs memory and computation resources which are not provided by the existing wireless sensor technologies, particularly when data is frequently transmitted. The proposed framework solves

this issue with the implementation of IoT-enabled gateways. The IoT 26 Gateways provide computer-like computational features which comprise of interconnected, robust operating systems such as Linux with other communication interfaces. The gateways can address another security problem for IoT devices: registration and key management of new sensor devices. Once a device that monitors that acts as a transmitter is added, it demands the public key for encryption. Thiscauses issues in key management and distribution. It is possible to manage the gateways by making use of keys. Through symmetrical encryption, the connection between the IoT gateway and the sensor device is secured. This is less complex than PKI on a computer basis. The gateway may even receive a new key if necessary because it is a central point of communication and is still connected to the internet.

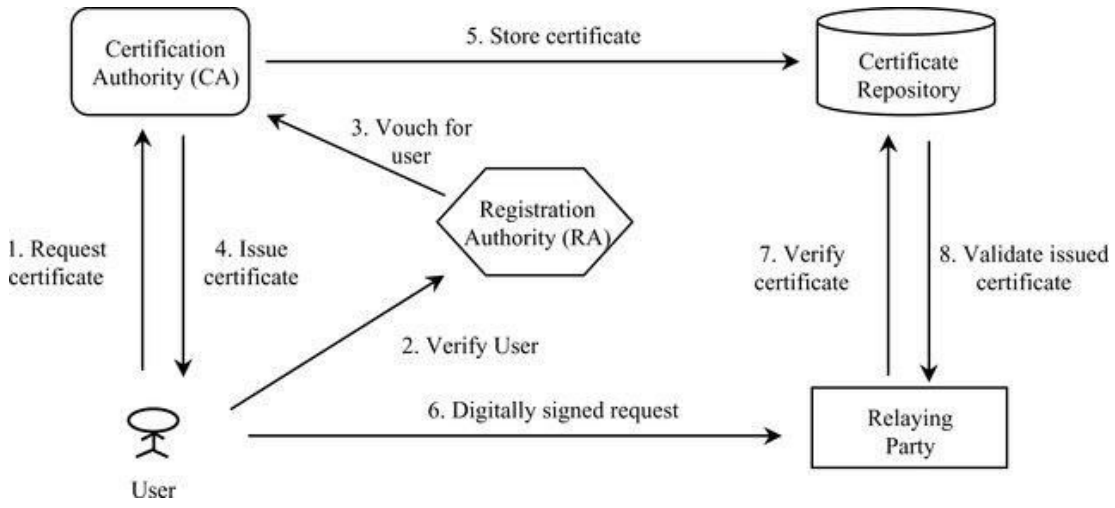

Fig 4: Public Key Infrastructure [18]

7.2 RSA ENCRYPTION [13]

The first asymmetrical cryptosystem that is commonly used for securing communication is Rivest – Shamir – Adleman or even known as RSA. This has a different decryption key that only the authorized may have. The key sizes vary from 1024 to 4096 bits, which makes it difficult to crack due to the huge number of permutations possible and hence it's more secure. It has computational speed limitations even if it's advantageous in terms of security. To mitigate this, data is not encrypted directly, and shared keys are used to speed up bulk encryption. This system has a contact interface and has an encoding and decoding framework coupled to at least one terminal. The message will be converted from a defined set into a ciphertext. This is consequently enhanced to the power of the receiver and further computed.

The steps of the RSA are explained below:

i) Key generation: Key is created by implementing mathematical rules to it.

ii) Key distribution: Only the public key is distributed to share the encrypted content. The

symmetric key is not distributed.

iii) Encryption: Once the public key is shared, the data is encrypted.

iv) Decryption: Decryption is done after receiving by making use of the private key.

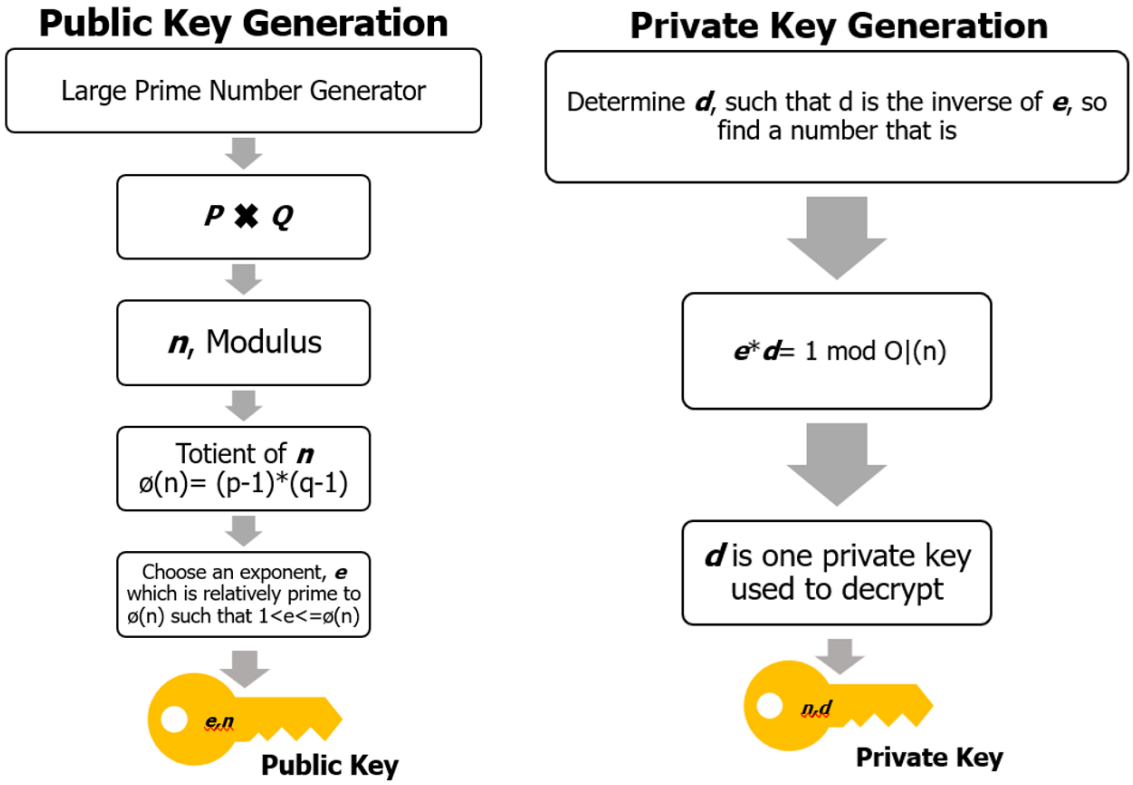

Fig 5: Public and Private Key Generation [13]

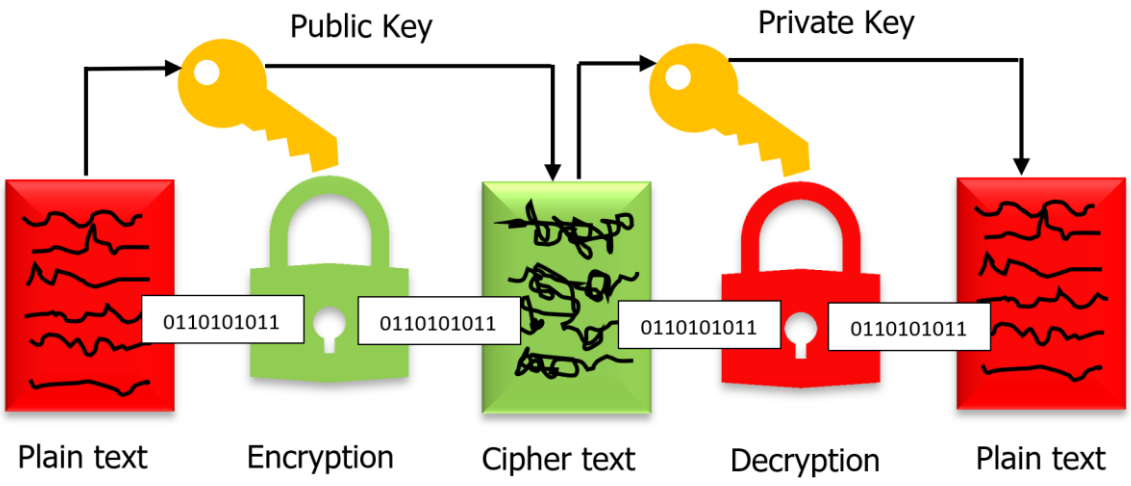

Fig 6: Encryption and Decryption processes in RSA [13]

7.3 TWO - FISH ALGORITHM [19]

This algorithm is a complex combination of both functions and matrices. First, the 128- bit plaintext is read in, split into four words, and whitened with the first four round subkeys, then the round function begins. Each round feeds the two left words into the F-function that moves the second block by 8, converting the two words into G-functions, executing and applying the pseudo-Hadamard transition to the 2 round subkeys. Once the F function words one and three are XORed and shifted right by one, word four is shifted right by one, and XORed with word two and finally they are shifted between words one and three, and two and four. G function is the heart of this algorithm. The word is divided into 4 bytes and each is fed into a different key-dependent s-Box and later recombined. It is supplied via the MDS matrix that generates the output text.
The criteria are that 16 rounds need to be executed before the terms are whitened with four to seven and then the entire 128-bit ciphertext combined.

It is a flexible design which means:

- It accepts lengths of keys even if extra.
- It is used on a variety of applications.
- It is appropriate for a stream cipher, MAC, and hash function.

Features include:

- Encrypt data on Intel Pentium, Pentium Pro, and Pentium II in less than 500 clock cycles a block for a fully optimized algorithm model.
- Able to set a 128-bit key (for optimal encryption speed) to encrypt 32 blocks on Pentium, Pentium Pro, and Pentium II in less than the required time.

Encrypt data on a Pentium, Pentium Pro, and Pentium II without key setup time in less than 5000 clock cycles per block.

7.4 TRIPLE DATA ENCRYPTION STANDARD

The cipher is a symmetric block type and is used on every data block by the DES algorithm three times. Compared to modern cryptanalytics and supercomputing power, the 56-bit DES key is considered insufficient. Triple DES nevertheless uses the same algorithm and increases the security of the adapted version of DES. This algorithm uses a 56-bit encoding and decoding of a 64-bit data set. The key is always a 64-bit block, which is not taken into account every 8th bit. However, each 8th bit is normally programmed to ensure that each 8th bit group has an odd number of bits programmed to 1. This algorithm is preferably used for hardware implementation as the software one is comparatively slow. However, in modern computers, the results of software implementation are satisfactory [20].

Triple DES uses multi-size keys in which three times DES is implemented. Considering a triple length key to consist of three 56-bit keys K1, K2, K3 then encipher is as follows:

- K1 for encipher
- K2 for decipher
- K3 for encipher

Deciphering will be inverse:

- K3 for decipher
- K2 for encipher
- K1 for decipher

If K3 is identical to K1 it results in a K1, K2 double-length key.

When all keys are equal, the effect is the same as a single 56-bit key. A system with triple-DES is therefore compatible with a single DES.

In general, Triple DES with three non-dependant keys has the length equal to 168 bits, but due to meet-in-the-middle attack, only 112 bits of security is provided. The key size of Keying option 2 is reduced to 112. It is quite vulnerable to both selected and known plaintext attacks and therefore only has 80 bits of security as designated by NIST. This can be considered insecure and therefore been disapproved by NIST in 2017 [5].

3DES is prone to block collision attacks by using a 64-bit short block size to encrypt massive numbers of data using the same key.

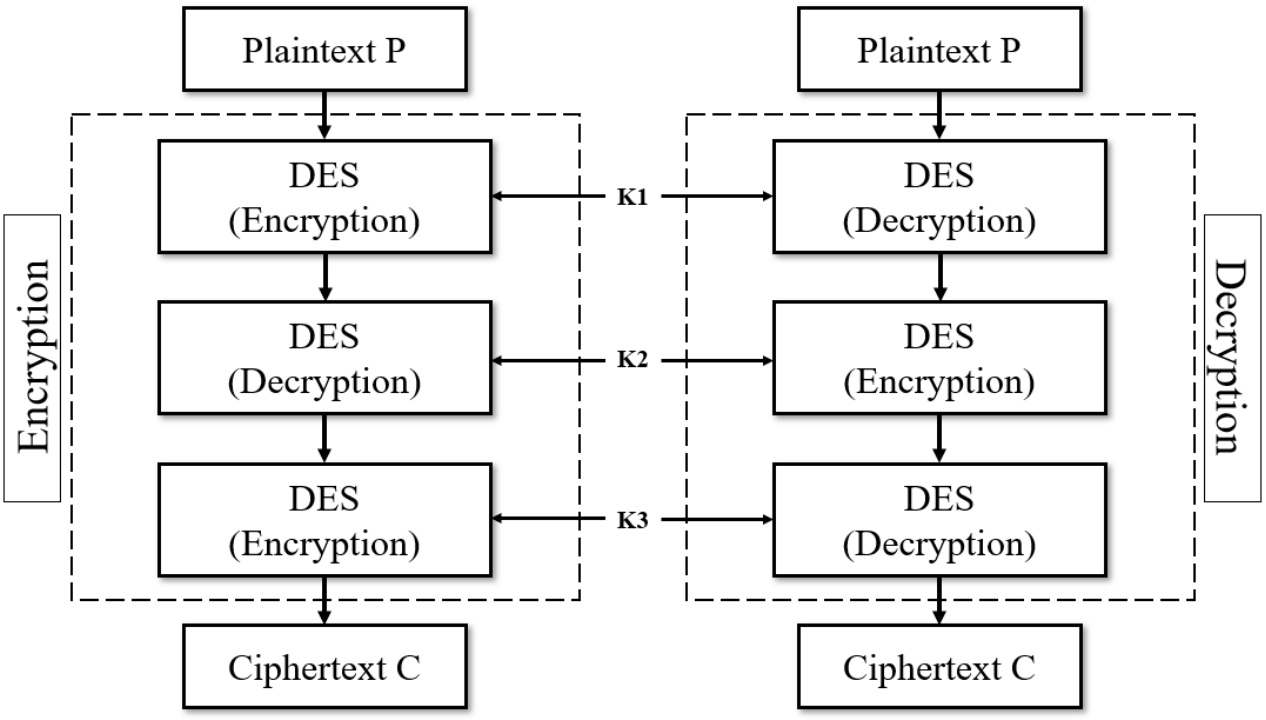

Fig 7: Process of Encryption and Decryption in Triple DES

7.5 ELLIPTIC CURVE CRYPTOGRAPHY [21]

ECC uses a public key based on the elliptical curve form over finite fields. For ECC to have equivalent security with respect to Non-EC cryptography only smaller sized keys are required. In applications, the end nodes require performance optimization of the device by increasing computing speed and reducing power consumption without any security compromising on the connected devices. The difficulty of ECC makes it tough for the attacker to comprehend the ECC and breach the security key. The security level provided by SA needs1024-bit key but in ECC it can be obtained with a 160-bit key. Therefore, it is very apt for resource limitation devices such as smart cards, mobile devices. The selection of the suitable elliptical curve is also not simple. Standardization of ECC is essential for effective and practical implementation. Specifications for ECC that are considered secure to use in the cryptographic application are presented by NIST.

8. Comparison of Encryption Algorithms

The following table gives an insight into the different encryption algorithms, out of which the Triple-DES and Two-fish algorithms are the recent ones for the concern on security.

Parameters	Public Key Infrastructure	RSA Encryption	Two-Fish Algorithm	Triple DES	Elliptical Curve Cryptography
Created by	British Intelligence Agency	Ron Rivest, Adi Shamir, Leonard Adleman	Bruce Scheiner	IBM	Neal Koblitz, Victor S Miller
Year	1970	1977	1998	1998	1985
Block Size	128 bits	2048 bits	128 bits	64 bits	192 bits
Key Size	256 bits	1024 bits	128 bits	112,168 bits	160 bits
Cipher Text Type	Hybrid	Asymmetric	Symmetric	Symmetric	Asymmetric
Security	Low	Low	Sufficient security	Sufficient security	Low
Speed	Adaptive*	Slowest	Fast	Slow	Slow

*Adaptive indicating that it can vary with respect to the choice. It can either be “key encapsulation” which is a public key infrastructure or “data encapsulation” which is symmetric in nature.

9. Latest approaches in IoT security

A well-defined structure and interface are not yet available for an end-to-end IoT application. A standard IoT application is composed of a big chain of devices, technologies, and geographies that are interconnected, and even if one of the layers, device or technology or their combination becomes vulnerable, the whole application is at a risk. Earlier, various encryption techniques utilized in IoT security were discussed. These encryption techniques are implemented on various layers of IoT which include various steps of encryption, decryption and re-encryption. This whole process of involving multiple steps make the system vulnerable to attacks. Therefore, it is important to introduce other approaches involved in IoT security.[22]

Some of the latest technologies in IoT security are block-chain technology, fog computing, machine learning and edge-computing.

9.1 Block-Chain Technology

The block-chain is basically a chain of blocks that contains information. The data, hash to that particular data and the previous hash are present in every block of the chain. The data stored in the blockchain depends on the type of the blockchain. There is a hash value for each block of the chain that can be matched with fingerprints. The hash of that particular block will also be produced when the new block is formed. With the changes made in the block, the hash of the block will be modified as well. Thus, when making changes in the block, the hash value is a very significant factor. It would not be assumed to be in the same block if the hash value of either block is changed. Other than the present block's hash, the block still contains the previous block's hash. By linking the current block to the previous block it helps to make a chain. These block features in the chain make the blockchainmore safe and secure [23].

Therefore, block-chain technology is a promising approach in IoT because of the various advantages associated with it. Due to the hash linking of the blocks and the distributed consensus system, the transactions captured on a blockchain are tamperproof.This includes a permanent record of transactions and communication and secure IoT data acquisition. In the blockchain, the time-stamped transactions recorded are transparent and easy to track. [24]

9.2 Fog Computing [25]

An extension of cloud computing as well as edge computing is given by the Fog computing framework. It offers user-level features such as computation, communication and storage. Fog computing 's architecture is based on a decentralised platform which is quite different from other conventional models. The architecture of Fog computing consists of three layers which are Cloud Layer, Fog Layer and Terminal Layer. The terminal layer is a physical environment which comprises all the IoT devices like sensors, smart cards, smartphones, gadgets, etc. This layer collects the information from the users and passes it to the next layer which is the fog layer. The fog layer consists of fog nodes such as routers, switched, access points, and gateways which are distributed throughout the network line. The IoT

devices are connected to the fog nodes and can be used for computation and storage. The last layer is the cloud layer which consists of high-performance servers along with high-speed internet connectivity and high-end storage devices. Therefore, these high-end storage devices help in storing an enormous amount of data permanently. In the case of IoT, fog nodes combined with cryptographic techniques can be used to secure the data. Many types of security threats on IoT systems need to pass through the fog layer. This layer can identify and mitigate unusual activities before it passes into the system. Fog computing also allows for malware detection. Fog also constraints the data generated by IoT to be sent to the cloud. Hence, it restricts the passing of useless data to the next layer.

9.3 Machine Learning [26]

Machine Learning is one of the most suitable techniques for providing security of data in IoT. Machine Learning (ML) has the ability to make future predictions based on inputted data. It also enables us to train a system without explicitly programming. Basically, ML makes use of mathematical models on huge datasets to build models of behavior. IoT networks can be characterized as heterogeneous. They have different types of device connected in a network which also use different communication protocols. This feature of IoT introduces a lot of challenges when it comes to the security of the network. The interconnectivity nature of the IoT also brings to light privacy issues. Supervised machine learning algorithms like support vector machine algorithms can be made use of for security. Machine learning algorithms can be used for authentication and access control. The data received from the devices is pre-processed and passed through a decision support system to obtain accurate information. The basic categories in access controls are role-based access control, context-aware access control, and policy-based access control. Deep learning is also made use of heterogeneous IoT networks. A recurrent neural network can be used to train a long short-term memory architecture. An experiment was performed to determine the optimal parameter to find the false alarm and detection rate. Random Neural Networks also can be used to realize an efficient, fast anomaly-based intrusion detection in low power networks.

9.4 Edge-Computing [27]

There are four key parts of the edge-centric IoT architecture: the cloud, IoT end devices, the edge, and the users. IoTusers requests access to IoT data or commands to manage IoT devices in the edge-centric IoT architecture via a web or mobile app-based interface supported by the cloud or the edge. These requests and commands will ultimately enter the edge layer. The edge layer would then handle them by either transmitting them to IoT end devices or managing them on behalf of IoT end devices on the edge layer.Also, it is possible to migrate several existing IoT end system resources from the cloud to the edge and to configure them depending on the needs of IoT end devices. The edge can operate independently of the cloud in terms of the interaction between the edge and the cloud, or the edge can operate with the cloud collaboratively. The edge layer not only bridges them with users and the cloud but can also store data gathered and uploaded from IoT end devices and unload major computing requirements, such as big data processing and robust security algorithms from IoT end devices, by communicating with IoT end devices. End-to-end security among IoT devices is always preferred. Nevertheless, it is complicated to obtain end-to-end encryption in the IoT, primarily because of the complexity of certain applications. As the edge layer acts as a bridge between heterogeneous IoT devices and the cloud, researchers have

proposed designing a secure middleware for secure end-to-end communications between IoT devices deployed at the edge layer.

10. Conclusion

IoT is a very widely used concept and is often misunderstood to have complete security of information.This paper discusses the architecture of IoT with respect to different layers. It is essential to understand the security threats possible in everyday IoT devices to find solutions to the weak links. Hence, this paper also discusses about the security threats associated with every layer of the IoT architecture. Multiple security techniques can be used to implement a certain level of security during the communication between devices.Encryption using different algorithms have been developed over the years to secure communication and make it difficult for hackers to obtain information. The encryption techniques have evolved and have become more complex to decode. The idea of encrypting the data was highly necessary due to the domains Internet of Things was used in, such as the Military sector that makes use of sensors, drones for survey, and detection purposes. If the data gathered by such devices were to be accessed by unauthorized users, it would be an issue of national threat. With the consistent efforts to improvise the existing algorithms constantly to avoid any breaches and increasing their speed of operation this paper provides an insight into the most popular encryption techniques and their functionality in detail.

11. References

1. Hussein, A., 2019. Internet of Things (IOT): Research Challenges and Future Applications. *IJACSA) International Journal of Advanced Computer Science and Applications*, *10*(6), pp.77-82.
2. McClelland, C., 2019. What Is IoT?–A Simple Explanation of the Internet of Things. *IoT for all*.
3. Liu, X., Lam, K.H., Zhu, K., Zheng, C., Li, X., Du, Y., Liu, C. and Pong, P.W., 2019. Overview of Spintronic Sensors With Internet of Things for Smart Living. *IEEE Transactions on Magnetics*, *55*(11), pp.1-22.
4. Kumar, N.M. and Mallick, P.K., 2018. Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, pp.1815-1823.
5. *www.wikipedia.com*
6. Reddy, M & Student, Engineering & Professor, Assoc&Krishnamohan, Revu. (2017). Applications of IoT: A Study. 10.13140/RG.2.2.27960.60169.
7. Bhat, O., Bhat, S. and Gokhale, P., 2017. Implementation of IoT in smart homes. *Int. J. Adv. Res. Comput. Commun. Eng.*, *6*(12), pp.149-154.
8. Sharma, V. and Tiwari, R., 2016. A review paper on "IOT" & It's Smart Applications. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *5*(2), pp.472-476.
9. Soumyalatha, S.G.H., 2016, May. Study of IoT: understanding IoT architecture, applications, issues and challenges. In *1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications*.

10. Sethi, P. and Sarangi, S.R., 2017. Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.
11. Jaychand, B.N., 2017. A survey on IoT security threats and solutions. *Int. J. Innov. Res. Comput. Commun. Eng.(IJIRCCE)*, *5*(3), pp.5187-5193.
12. Varga, P., Plosz, S., Soos, G. and Hegedus, C., 2017, May. Security threats and issues in automation IoT. In *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)* (pp. 1-6). IEEE.
13. Rajendran, S., Kulkarni, V., Chaudhari, S. and Gupta, P.K., 2020. An Update on Medical Data Steganography and Encryption. In *Recent Trends in Image and Signal Processing in Computer Vision* (pp. 181-199). Springer, Singapore.
14. Prosser, W., 1960. The torts of privacy. *California Law Review*, *383*(48), pp.392-98.
15. Schatz, D., Bashroush, R. and Wall, J., 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), pp.53-74.
16. McEwen, A. and Cassimally, H., 2013. *Designing the internet of things*. John Wiley & Sons.
17. Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F. and Vassilacopoulos, G., 2012, November. Enabling data protection through PKI encryption in IoT m-Health devices. In *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)* (pp. 25-29). IEEE.
18. Jie, W., Arshad, J., Sinnott, R., Townend, P. and Lei, Z., 2011. A review of grid authentication and authorization technologies and support for federated access control. *ACM Computing Surveys (CSUR)*, *43*(2), pp.1-26.
19. Schneier, B., Kelsey, J., Whiting, D., Wagner, D. and Hall, C., 1998. N. Ferguson;"Twofish: A 128-bit Block Cipher". In *Proc. of 1st AES Candidate Conference* (pp. 20-22).
20. Koskimäki, A., 2019. Attack Resistant Services Delivery over the Internet.
21. VAHDATI, Z., YASIN, S.M., GHASEMPOUR, A. and SALEHI, M., 2019. COMPARISON OF ECC AND RSA ALGORITHMS IN IOT DEVICES. *Journal of Theoretical and Applied Information Technology*, *97*(16).
22. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, pp.82721-82743.
23. Rathee P. (2020) Introduction to Blockchain and IoT. In: Kim S., Deka G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, Singapore. https://doi.org/10.1007/978-981-13-8775-3_1
24. Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R.C., Michelin, R.A., Zorzo, A.F. and Kanhere, S.S., 2020. Blockchain technologies for iot. In *Advanced Applications of Blockchain Technology* (pp. 55-89). Springer, Singapore.
25. Kaur, K. and Sachdeva, M., 2020. Fog computing in IoT: An overview of new opportunities. In *Proceedings of ICETIT 2019* (pp. 59-68). Springer, Cham.
26. Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E., 2020. Machine learning in IoT security: current solutions and future challenges. *IEEE Communications Surveys & Tutorials*.
27. Sha, K., Yang, T.A., Wei, W. and Davari, S., 2020. A survey of edge computing-based designs for iot security. *Digital Communications and Networks*, *6*(2), pp.195-202.