A Review on Internet of Things (IoT): Security Challenges, Issuesand the Countermeasures approaches

Dr.B. Sundaravadivazhagan[1], Dr.B.Subashini[2], Mr.Mohemed Ashik M[3],
[1]Department of IT, University College of Technology and Applied Science-Al Mussanah, Oman
[2]Department of Computer Science, Thiagarajar College(Autonomous),Kamarajar Salai,Madurai-9.,India
[3]Department of IT, University College of Technology and Applied Science-Salalah, Oman

Abstract

In the present scenario, Internet of Things is playing vital role in the next era of communication. The IOT applications like smart cities, smart houses, smart livestock, smart health care, smart climate etc.It can be lead to many security challenges and issues. The aim of this survey focus on the main objective of the security challenges and issues in the data privacy, security, confidentiality, integrity, availability, access control, encryption, default password, malware and ransom, botnet, phishing, cloud, routing and trust management and discussed recovery from mention security defies. This study has detailed review of IoT layered design, each of these layers having lot of security challenges such as threats, vulnerabilities and attacks. Understanding these challenges and associated countermeasures mechanism with the help of the secure routing.

I.Introduction

The different physical systems are connecting to access by way of internet is called IOT. The Internet of Things will be expecting to grown up to 1.0 trillion in the year of 2025.In this section deal with the History of IoT, Evolution of IoT, IoT Applications, Technologies used in IoT, Characteristics of IOT, Challenges of IoT, IoT layer and architecture.

1.1 History of IoT

Now daysIoT fields are enormous grown up in human life every day. The IoT are connected to many applications. The IoT concept was not involved until 1999, so now it is very fastest growing technologies. Kevin Ashton**,**ED, Auto–ID" centre was the person behind the name "Internet of Things" during the year 1999. The Following Table 1 and Figure 1 shows the evolution of model IoT.

Year	Inventor	Model
1990	John Romkey	Smart toaster-using TCP/IP Protocol
1999	Kevin Ashton	RFID, Supply chain Management -IOT
2000	Gurdsan, Forbes and Boston	RFID, Short range communication, Wifi and Sensor Network
2010	All Companies like Apple, Google, Cisco..etc	IOT devices and Applications

Table 1- Evolution of IOT

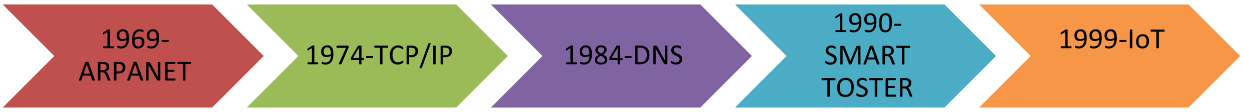


Fig 1 - Evolution Model of IOT

According to the Cisco data source, it is significant that IoT proves that future evolution of internet has beenshiftingthe whole IoT. The Table 2 shows the future evolution of IoT connected devices

.

Future Evolution of IOT Connected Devices			
Year	**Device Per Person**	**Connected devices**	**World Population**
2003	0.08	500 Millions	6.3 Billions
2010	1.84	12.5 Billions	6.8 Billions
2015	3.47	25 Billions	7.2 Billions
2020	6.58	50 Billions	7.6 Billions
2025	14.16	1.0 Trillions	8 Billions
More Connected devices then population			

Table 2- Future Evolution of IOT connected devices

According to the Table 2 the Figure 2illustrate the expected IOT connected device per person from the year 2003 to 2025.

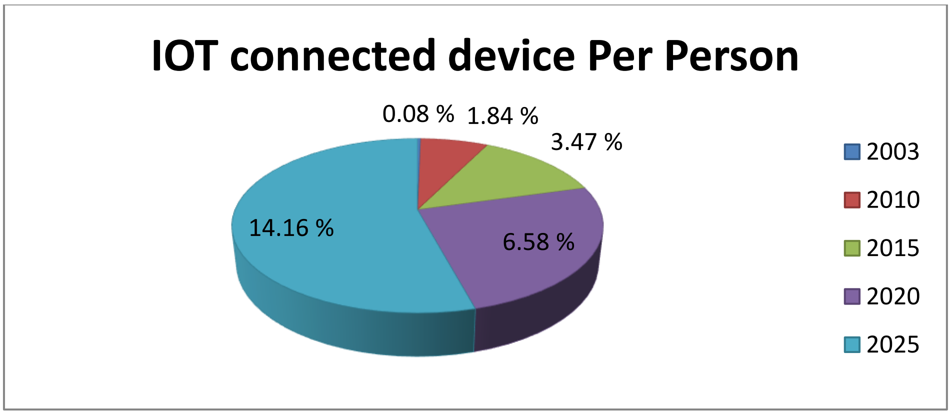


Fig 2-IOT Connected device per person from 2003 to 2025

1.2 Applications of IOT

The survey paper [2] hassummarized the various IOT applications are discussed in this paper.

Smart Cities: It contains smart hospices, insolentlightning, smart path, traffic organizationetc.,

Smart Environments: It comprisesseveralIoT applications likeforest fire uncovering,disaster management, air pollution, snow level monitoring, early earthquake and river flood detection etc.,

Smart Homes: It embracescountlessapplications of IoT. For example, lightning controller, garden maintains, intruder's detection system, water supply consumption etc.,

Smart Agriculture: It includes various IOT applications smart farming, diseases monitoring, monitoring, crop health monitoring etc.,

1.3 Characteristics of IoT

IoT is a assemblage of devices which is attached with internet. Itcollects and transfer the information using nodes and controllers. The following characteristics are discussed in this section [19].

i) **Connectivity:** Internet connectivity is attached with in the devices and sensors.

ii) **Communication:** Everythingis unified with comprehensiveevidence and communication structure.

iii) **Things related services**: IoT is capable of traditional and non-traditional computer things related services.

iv) **Security:**IoT may be transmitting sensitive data, it is very significant to givedata privacy and security.

v) **Energy Efficient:** The IOT devices should be having power backup.

vi) **Sensor:** It is an important supporting device in IOT.

vii) **Heterogeneity:** The IOT devices based on hardware and Network platforms.

viii) **Dynamic Environment:** The IoT devices support dynamic environment.

ix) **Enormous scale:**The IoT technologies support to control more number of devices and which interact.

1.4 IoT Challenges

Security is one of the key threats in IoT applications that involve the following problems and issues in recent IoT applications [1-5]. All these challenges, attacks and countermeasures are discussed in the section 3.

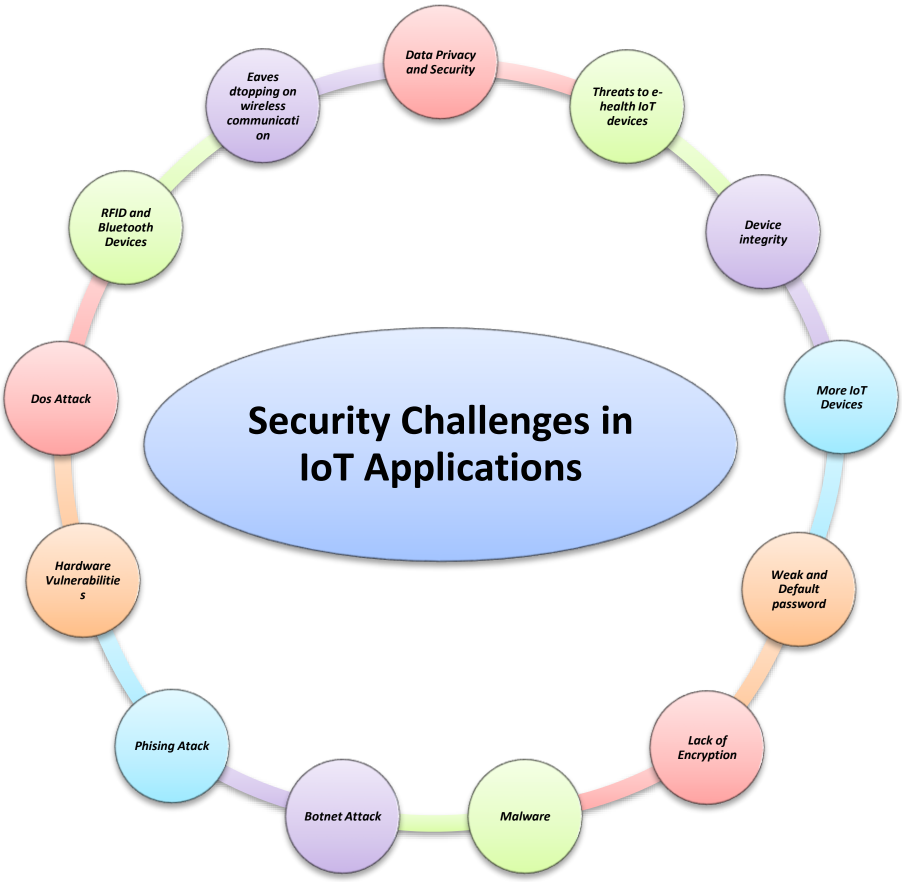

Data Privacy and Security
Threats to e-health IoT devices
Device integrity
More IoT Devices
Weak and Default password
Lack of Encryption
Malware
Botnet Attack
Phising Atack
Hardware Vulnerabilitie s
Dos Attack
RFID and Bluetooth Devices
Eaves dtopping on wireless communicati on
Security Challenges in IoT Applications

Fig 3–Security Challenges in IoT Applications

1.5 IoT Layered architecture

Application of IoT consists of four layers:i) Layer of Perception ii) Layer of Network iii) Layer of Middleware iv)Layer of Application[2, 8, 20, and 21]. The Figure 4 shows the IoT layered architecture. In this architecture discussed the various devices and technologies are available in each layers. The Section 3 will be discussing in the various security challenges, threats, vulnerabilities, attacks and counter measures details in each layer.

1.5.1 Perception layer

In other words it is called as physical or sensor layer. There are many kinds of sensors such as actuators, sensors, etc., attached to the things to gathering data.

1.5.2 Network Layer

The network layer is named as transport layer. It carries and communicating the information from the middleware to the processing layer.

1.5.3 Middleware Layer

It is also known as the processing layer. It acts as a conduit between thetransport and application layer. This layer provides Application Programming Interface (API)and cloud storage. This can also offer powerful competencies in computing and storage.

1.5.4 Application Layer

The customer has been provided service in the application layer. It has the duty to give the application the services.

The forthcoming part of the study covers Literature Review, Security challenges, threats, vulnerabilities and attacks in IoT applications. Counter measures of security challenges, Discussion, Conclusion and References.

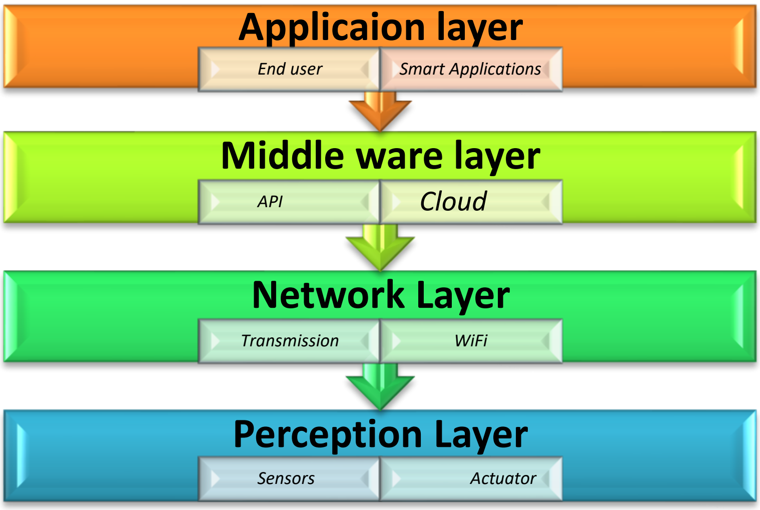


Fig 4 – IOT Layered Architecture

II. Background

A literature review of relevant articles was published in recent years, to identified security challenges, issues, threats, vulnerabilities attack and counter measures in IOT applications.

citation	Year	Topics of the survey	Enhancement's in our paper
[1]	2018	Current research on Internet of Things (IOT) Security: A survey	This survey paper analysis of the recent trends in IoT security research and open issues and challenges.

[2]	**2019**	A Survey on IoT Security: Application Areas, Safety risks, and architectural solutions	The key goal of security related issues and sources of danger in this survey is to achieve a high degree of confidence in IoT applications. Discussed are the various technologies for rising the level of protection in IoT such as block chain, fog computing, edge computing and machine learning.
[3]	**2017**	A roadmap for threats to security in the Internet of Things	Detailed analysis of the systematic and cognitive approach to IoT security, and discussed in IoT privacy , trust, identification, and access control.
[4]	**2017**	Internet of Things: A survey on the security of IoT frameworks	In this paper, we survey the security of the main IoT frameworks, for each framework, we clarify the proposed architecture, the fundamentals of emerging third-party smart apps, the well-matched hardware, and the security structures.
[5]	**2019**	Modeling Botnet Malware Spread in IoT Wireless Sensor Networks	In this paper, the invention of a new model of IoT – SIS, an creative propagation model considers the characteristics of the restricted processing capacity , energy constraints, and node density on the creation of a botnet and explores the concepts of epidemic modeling for IoT networks consisting of wireless sensor nodes.
[6]	**2019**	A Practical Way to Secure IoT Systems from Attacks and Datasets for Security Incidents	The companies produced devices to enforce functionalities but overlooked some serious problems affecting the security of the system. The revolutionary technique of IOT security systems using Berkeley Packet Filters (BPFs) is tackled in this report.
[7]	**2018**	On security problems in the Internet of Things and transparent issues	The goal of this paper is to address security issues in IoT systems and IoT applications. Moreover, it also describes proposed architectural security projects, evaluated and available problems.
[9]	**2019**	IoT Compliance Issues and Drawbacks	The aim of this paper is to provide an detailed overview of security issues in IoT environments. In addition, the survey was conducted to take the views of researchers and IT experts on the main challenges and constraints of the internet of things technology.
[10]	**2019**	IoT Challenges and Countermeasures	Throughout this article, IoT solutionsare discussed security problems and security concerns in the IOT world.
[11]	**2018**	IoT and Mobile networking using current communication technologies	The biggest obstacles to align WSN nodes with the MANET nodes in this proposed IoT architecture as the nodes have different amounts of resources, heterogeneous protocols and chances of snooping. The suggested countermeasures that include network protocols, distribution of range and node, MANET routing and versatility pattern and finally implementation of IoT applications.
[12]	**2018**	A systematic survey of IoT attacks focused on a Build-blocked Reference Model	Within this paper an advanced four-layered IoT was proposed, IoT asset-based surface attack reference model, Second, IoT protection targets set. Fourth, define taxonomy of IoT attacks for every asset. Finally, demonstrate the

			relationship between each attack and its violated security goals, and also define a collection of countermeasures to protect each asset.
[13]	**2017**	Security attacks in IoT: A survey	In this survey discussed various level of IOT attacksand discussedcountermeasures and finding the most noticeable attacks in IoT.
[14]	**2014**	Security challenges in Internet of Things: survey	In this survey article analyzed the security challenges face in Internet of things, such as privacy, confidentiality, integrity, authentication and access control.
[15]	**2015**	Internet of Things: Effects on security and privacy	The Internet of Things (IoT) has a new security privacy risk that IoT system manufacturers are not able to anticipate. The IoT systems aid in processing, analyzing, tracking, and exchanging large amounts of data with other networked devices and users. The article aims at reviewing the privacy of a user is insecure and evaluating the approaches to address privacy problems of the user.
[16]	**2015**	IoT: Issues and Technology Flaws	This article discusses the security risks, weaknesses, and forms of attacks discussed in addition the IoT protection and privacy countermeasures.
[17]	**2017**	An Internet-of-things report on security and privacy issues	This survey explored four parts. The first section comprised of limitations on IoT products and solutions, while the second section addressed IoT assault classification. The next section focused on authentication and access control mechanisms and architectures, and final section analyzed the security issues and problems in IoT layers.
[18]	**2017**	An Internet of Things Survey: Infrastructure, Software Enabling, Protection and Privacy, and Applications	This survey paper discusses the relationship of cyber-physical systems (CPS) and IoT, fog / edge computing and IoT, IoT architectures, IoT technologies, and IoT protection and privacy problems, and finally addressed the various smart applications and how to apply fog / edge computing-based IoT in real-world applications.
[19]	**2016**	Cloud of Things-IoT: Description, Architecture, Enabling Technology, Implementation & Potential Challenges	This study discussed IoT 's explanation of how IoT supports various technologies and architecture, functionality & applications, and further discussed IoT's potential challenges.
[20]	**2018**	IoT Features, Layered Architectures and Privacy Issues	This study covered description of the various layered architectures and IoT attacks on IoT is discussed. In addition, a process analysis which helps to provide security solutions along with a novel stable layered IoT architecture was proposed to help to solve the security issues.
[21]	**2019**	IoT Applications and Security	In this paper, IoT smart applications were addressed and the concepts of security criteria including data confidentiality, data integrity, availability, authentication and non-repudiation are also applied.
[22]	**2019**	An IoT Security Survey: Domain Areas, Security Threats & Architectures	This survey examined the security related issues in IoT applications and, in addition, addressed high security , safety, authentication and recovery from threats ,

			vulnerabilities and attacks to incorporate the following security steps. Additionally, discussion was made on various potential and current technologies such as blockchain, fog computing, edge computing, and machine learning to seek to increase the level of protection in IoT applications.
[23]	**2019**	Internet of Things (IoT): Research Challenges and Future Applications	This article focused on the identify the certain research challenges and issues in IoT applications. Furthermore, discussion in recent development of IoT technologies and discusses future applications and research challenges.
[24]	**2019**	Blockchain for Internet of Things: A Survey	In this paper, investigate the overview of blockchain technology with IoT and discussed the convergence of blockchainand IoT and proposed BCoT architecture further discuss the issues about using blockchain for 5G beyondin IoT.
[25]	**2011**	Middleware Function for Internet of Things: A Study	This article describes the consequences of the middleware framework for (IoT) and addresses the work gaps and potential directions of middleware technology, proposes basic functional foundations for middleware, and analyzes open issues and the scope of work in this field is discussed.
[26]	**2019**	Survey on BlockChain Technology to IoT- Study Patterns for BlockChain Technology to IoT	In this survey based on the robust security blockchain technology is helping to address the IoT issues and problems. As a result, various research is underway to increase the IoT network's stability, lightness and efficiency by applying blockchain to IoT. This paper describes work trend for applying blockchain to IoT.
[27]	**2019**	IoT Protection Network Intrusion Detection Based on learning techniques	This survey addressed the IoT security threats and problems categorizations in IoT networks and focused on the design of the network intrusion detection systems, detection strategies, algorithms and implementation. In addition, the paper addressed machine learning with the techniques for network intrusion detection systems. Focused on IoT network intrusion detection systems implemented with Machine learning algorithms in this investigation, they have a good safety and privacy success rate. The survey also offers a review, discusses IoT threats and problems, and introduces potential intrusion detection solutions for the network.
[28]	**2019**	A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems	Proposed software defined networking (SDN) and network function virtualization (NFV) security framework in this survey which is helping to provide stable IoT systems. The proposed security framework assists in the identification, recovery and defense of threats to IoT infrastructure.
[29]	**2019**	The Impact on Protection and Privacy of IoT Emerging Features: Emerging Threats, Current Solutions, and Problems Yet to be solved	This survey focused on the latest IoT protection and privacy features and included the threat issues and potential solutions. Finally, this survey clarifies the work on IoT protection and points out how IoT features impact existing security work.

[30]	**2017**	Robustness, protection and privacy in location-based IoT systems: a sample, a special section on security and privacy in applications and potential Internet of Things systems,	This paper addresses strategies for enhancing the threats to robustness, security and privacy and cryptographic solutions related to location-based services in IoT systems, and finally examines policies and procedures for security and privacy issues of IoT-location-based services.
[31]	**2017**	Heterogeneous IoT preparation with time assurances, "the 8th International Ambient Systems , Networks and Applications Conference (ANT 2017)	In this paper the algorithm proposed to help create a heterogeneous IoT network to work with timing constraints. Single entry, token-ring and single access control protocols based on Carrier Sense will coexist in the same network
[32]	**2019**	IoT: Disrupting the Internet? A Review of Vulnerabilities in Traditional IoT Systems	The aim of this survey article is to summarize the risks , vulnerabilities in IoT devices and address some of the counter-measures that help to which the safety danger. Additionally, the emphasis was on the different security mechanisms that IoT communication tools implement. Next, look at some of the attacks on actual IoT apps. Finally, this article covered emerging IoT technologies with security characteristics including confidentiality, transparency, availability, anonymity, access control, authentication, authorisation, durability, self-organization.
[33]	**2019**	Anatomy of Internet of Things Risks	This paper discusses the vulnerabilities in IoT architecture in various layers, with a emphasis on the anatomy of IoT malware attacks. Eventually, IoT protection architecture has been established and some research problems opened up.
[34]	**2020**	In IoT Defense machine learning: current approaches and future problems	In this paper, the basic concepts of protection, threats, and emerging machine learning and deep learning security approaches are examined to support the various security challenges in IoT networks. Finally, the forthcoming study for IoT security based on computer and deep learning was debated.
[35]	**2014**	A holistic and systematic IoT Security strategy	The interactions of these four IoT elements, human, intelligent entity, technical environment, and mechanism, illustrate a systemic and cognitive dimension within the protection of the IoT in this paper proposed the systemic and cognitive approach for IoT safety.
[36]	**2019**	Internet of Things security: vulnerabilities, threats and steps to combat them	This article focused on the active and passive security attacks with IoT technology in wireless sensor networks, and addressed the safety framework that also helps to ensure safe communication.
[37]	**2019**	IoT: Disrupting the Internet? A Practical Survey Vulnerability in Actual IoT Apps	This article examined summary of IoT System security vulnerabilities and proposed some potential countermeasures. Several of the attacks on IoT devices were also explored.
[38]	**2017**	IoT Middleware: A Survey on Problems And Providing Technology	This paper explored supporting IoT middleware technologies for an IoT application, as well as further evaluating the difficulties and enabling technologies in creating an IoT middleware.

Table 3: Existing surveys on Security challenges and issues, threats, vulnerabilities, attacks in IoT Environments

III Threatsagainst Safety, Vulnerabilities, Attacks in IoT Environments

Safety is a primary aspect of applications of IoT and devices. In this section various security terminologies such as threats, vulnerabilities and attacks are discussed in details.

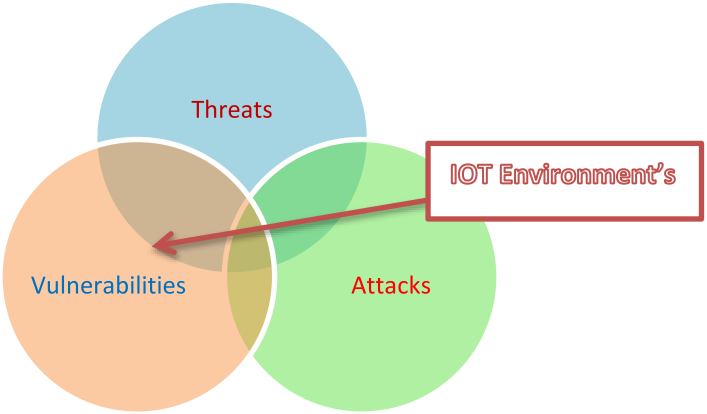


Fig 5: Threats, vulnerabilities and attacks in IoT Environments.

3.1 Standard IoT Security Principles

The security has become one of the most important areas in IoT applications. The following figure illustrates the standard IoT security principles in IoT Environment.

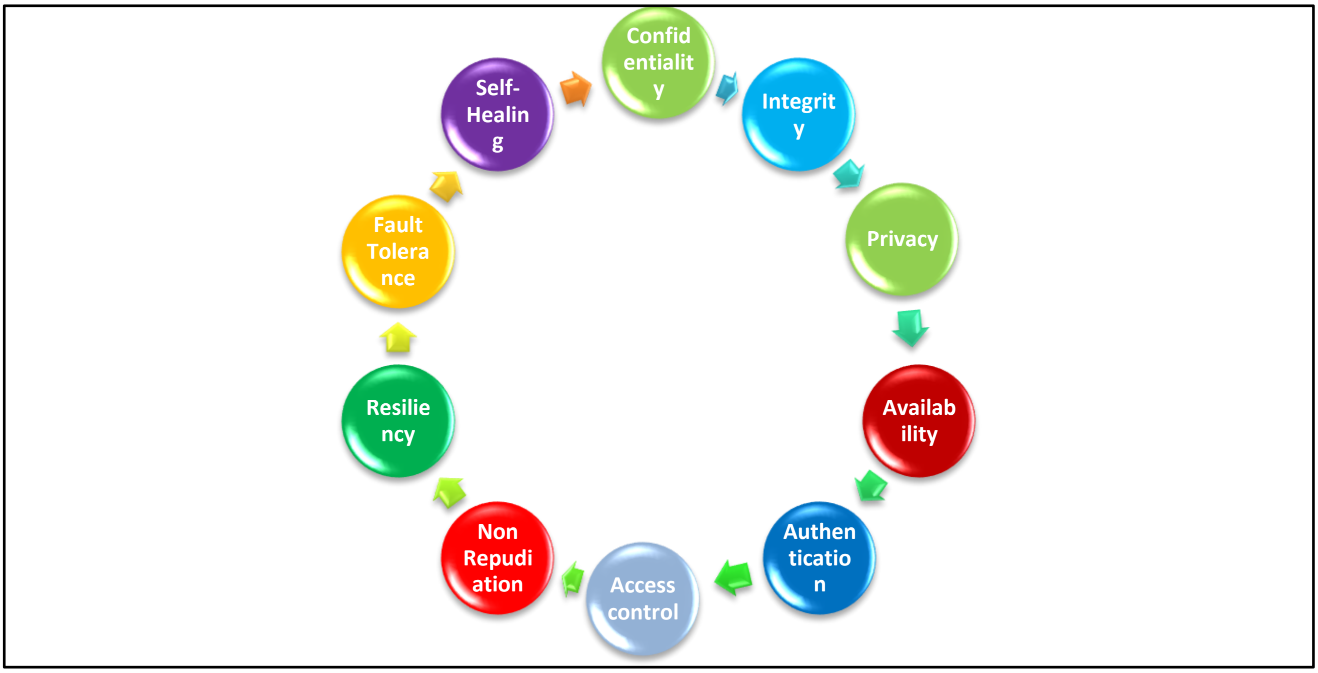


Fig 6:Standard Security Principles in IoT Environments

Confidentiality

The information should be preventing from the unauthorized person and to make data confidential. The organization make a security policy and procedure helps to access information only authorized person.

Integrity

The integrity should not able to modify the data during transmission.

Privacy

The user personal information should not be disclosed to any one during the exchange of information.

Availability

The information must be available every authorized request at all times.

Authentication

The system is confirmed by authorized person's identity, once the identity is confirmed; authorized person has rights to access the particular system.

Authorization or Access control

The authentication process over and then go to authorization, given permission to access system and other login restrictions.

Non Repudiation

The non-repudiationmeans is the guarantee that someone cannot repudiate the legitimacy of something.

Resiliency

This security principle protects the system and data from any attack.

Fault Tolerance

It refers to the IoT interconnected devices continue to give security services without any interruption supposed to be if any one or more system fault.

Self-Healing

If any one of the devices may fail .The remaining interconnected devices support to operate the system with minimum level of security**.**

3.2 Threats and Vulnerabilities in IoT Layers:

Threats	**Vulnerabilities Exploited**
Physical layer	
Eaves dropping	Vulnerable communication conduit, no encryption
Attacks at disposal of batteries	Un volume of legal request, no encryption
Malicious informationinstillation	Fragileentree control
Unauthorized access	Use of weak password
Transformation of alignment	Weak execution of cryptographic processes
Timing attack and Hardware exploitation	Open debugging ports
Network Layer	
Dos attack	Error in Standardentree control and communiqué protocols
MITM, Eavesdropping	Lack of authentication mechanism
Message fabrication and reply attack	Weak data authentication
Network interference and device conciliation	Feeble IDS, access control,

Storage attack	No protection about malware such as crypt locker and ransom ware
Application Layer	
Malevolent code	Cloud protection fail, authentication mechanism, authorisation mechanism
Modification of Software	Lost Internet Protection
SQL injection	Flaws in SQL
Login and identity fraud	Faulty authentication implementation

Table 2: surveys on Security threats and vulnerabilities in IoTLayer.

3.5 Security Challenges in IoT Devices

More IoT Devices:

Further IoT devices mean to increased vulnerabilities in terms of security and this is a growing concern for security professionals.

Weak and Default password:

Most IoT devices come with poor, original default passwords.

User unawareness:

The user has a lack of security training and knowledge of the IoT technologies is possible to attack their IoT environment.

Lack of Encryption and authentication:

The user has a lack of Encryption and authentication mechanism is one of the biggest challenges in IoT technologies..

Malware attacks:

It is a malicious program deliberately designed to gain access to or harm an infrastructure without the knowledge of the owner.

Botnet attacks:

A botnet occurs when hackers remotely monitor and use internet-connected computers for illegal use.

Phishing attack:

Hackers are enabled to send a signal to an IoT system that causes several complications.

Data privacy and Security:

As per the security audit results, approximately 90 percent of IoT devices collect user personal information in some way. This unauthorized collection of information is vulnerable to attacks against data protection, privacy and dignity.

Threats to eHealth IoT Devices:

They use Biomedical Sensor Network (BSN) to monitor the health of patients. Due to mobile nodes, power limitations and low bandwidth IoT communication protocols BSN has dynamic network topology. Therefore, BSN is vulnerable to various attacks including DoS, eavesdropping, and release of personal health information without authorisation.

Device Integrity:

Data is forwarded between computers. IoT end devices, however, still run in a less secure environment, without any physical protection, hardware attacks, side channel attacks, etc.**Software/Code Integrity:**

In IoT, the lack of anti-virus / malware detection system contributes to attacks on the credibility of an end device's code / software. Example : Mirai malware – attack default usernames and passwords

Hardware Vulnerabilities:

Commercially designed hardware devices are developed with more emphasis on the functionality of the system rather than protection. Commercial IoT systems therefore have certain hardware bugs that can be exploited remotely.

Dos Attack:

Both of these attacks would most likely impact the operational functionality of IoT systems and their services will not be accessible to the respective users.

Security Issues of RFID and Bluetooth Devices:

Despite of lack of physical security RFID tag data is vulnerable to attacks on confidentiality and honesty. Likewise, using unpatched versions of Bluetooth devices will lead to unauthorized / malicious devices being attached.

Eavesdropping on Wireless Communication:

Attackers will mount endnode-like devices on an IoT network to sniff valuable user information

IV IoT Security counters measures

The main objective of the security mechanisms helps to reduce the risk extenuation is to reserve security and confidentiality, discretion, Integrity and availability, confirming the safekeeping of the users, environment, information and sensor devices of IoT. In this section focused various security counter measures in IoT.

4.1 Authentication Mechanismto against attack on IoT devices:

The authentication mechanisms is one of the greatest method in the current scenarios it is given permission to access IoT devices in the network and which is help to reduce the attacks to the IoT environment such as spoofing attacks are MIM, Reply outbreak, Buffer overflow outbreak, etc.

The authentication is the primary onset in terms of standard safekeeping principles in systemsecurity. This process helps to provide identity the user is established with proof and confirmed by a system, The IoTauthentication process implements the two or more authentication approaches in IoT devices. The user name and password are common authentication process and some additional authentication factors are implementing to password identity it is help to improve secure data.

Some of the IoT apps implement the authentication process by using the most familiar form of two factor authentication process method, The first step enter password into the IoT devices, the system or devices sent a OTP (one time password) to registered authentication phone number.In this paper focused Multi Factor Authentication Mechanisms (MFAM)method to implement the IoT device. It is one of the most active control mechanisms which are help to protect from unauthorized access to device or network system.Finally the multifactor authentication processsupports to the restriction of user and reduce the risk of the attack in IoT Environment.

4.2 Multi Factor Authentication Mechanism (MFAM) :

Themultifactor authentication mechanism is implemented properly, to support remote access and reduce security vulnerabilities.

There aresome of thelisted authentications mechanisms methods are used to Multi Factor Authentication Mechanism.

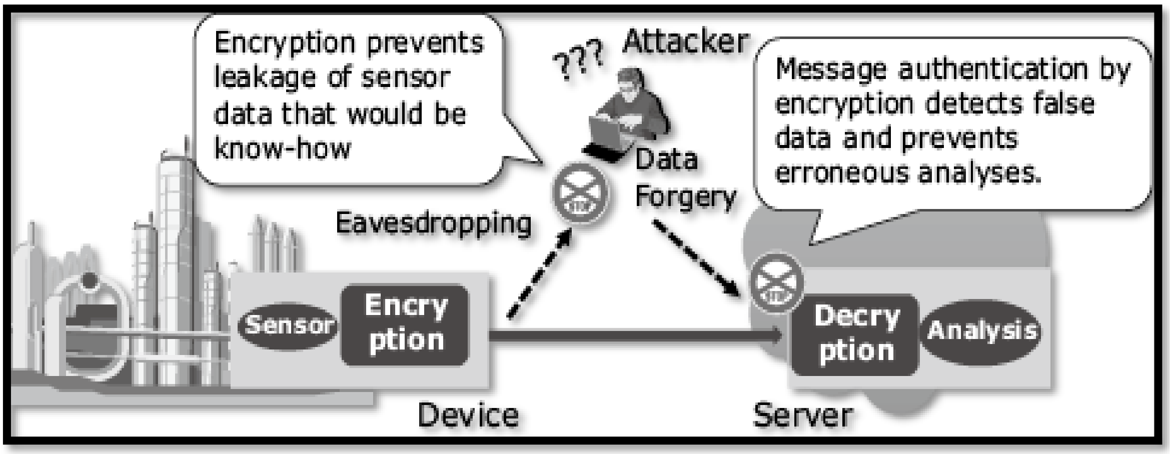
- User registered password
- The IoT devices confirmed by registered user identity like Civil ID, phone number, passport no .etc.
- The IoT devices authenticated by using Biometric authentication process such as (iris, finger print ,facial)

4.2 Analysis of Standard Encryption counter measure against attack on data collection in IoT devices:

The encryption is one of the cryptography data security technologies can protect against threats, vulnerabilities and attacks. In this method using some algorithms like symmetric and asymmetric, changing original information into cipher text to make it unreadable form to anyone except authorized user who have a proper key for the information.

The encryption method, possible evesdropper could only access the cipher text, yet the meaning of the messages shouldn't be understandable.In symmetric chiffrement algorithm using secret public key for bothsender and receiver,it is possible to known any one.In asymmetric mechanism using own private key, it cannot be easily consequent from any one [32].

The main objective ofIoT encryption mechanism is to accomplishopen contact end to end [1].The main security-related threat of IoT systems using sensor devices for data collection, it is possible to attack systems.To implement encryption mechanism to sensor devices, this can be effective countermeasures such as confidentiality, integrity and availability against threats, vulnerabilities and attack [40].The following fig 7 illustrates the encryption mechanism against attack on data collection**.**


Encryption prevents leakage of sensor data that would be know-how
??? Attacker
Message authentication by encryption detects false data and prevents erroneous analyses.
Data Forgery
Eavesdropping
Sensor
Encry ption
Decry ption
Analysis
Device
Server

Source: [40]Fig: 7 Encryption-based countermeasures against attack on data collection.

4.2.1 Light weight Cryptography:

Instead of standard encryption algorithm increased number of connected IoT devices, the research community has introduced new security light weight cryptography encryption algorithms.The light weight cryptography technology implement the block and stream ciphers, hash function and message authentication code. To implement the light weight cryptography technology in to IoT devices for the following reasons [32] [40].

i) Secure end to end communication
ii) Energy consumption
iii) Efficient storage capabilities and using less memory
iv) More network connections and less computingresources

4.3 RPL Secure routing optimization mechanism protect against routing attack:

In the IoT setting the IoT sensors and actuators are critical instruments. The more IoT devices connected using the IPV6 protocols. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), where each device has its unique IPv6 address.This allows the node to connect directly with the Internet using open standards, However since there is no authentication in 6LoWPAN possible for security attack.[1]

The RPL (low power and lossy network) is the compliant IPV6 compliant IoT network routing protocol. IETF for restricted networks are some constraints in this RPL protocol developed by the ROLL community which are memory, power and other network resources. RPL 's following vulnerabilities to security, such as sinkhole attack, selective forward attack and hello flood attack, warmhole and blackhole attack. Many of the security countermeasures to defend against the attacks are implemented here[41]

4.3.1 RPL Mechanism:

Steps:

i) The RPL is a vector distance and a routing protocol to source.

ii) The RPL treats the entire network as a DAG (Directed Acyclic Graph).

iii) Which is further divided into one or more destination-oriented directed acyclic graphs (DODAGs) with unique DODAGID, one DODAG root, same Objective Function (OF), and the same RPL Instance ID.

iv) In the RPL DODAG, there is one and only one DODAG root, with the remaining named nodes, each of which has a node ID(IPv6 address), a parent node, a neighbourhood list, a DODAG version number and a rank indicating its location relative to other DODAG root nodes, which decrease strictly in the Up direction to the DODAG root and increase strictly in the Down direction away from the DODAG root.

v) In other words, the distance between the node and the DODAG root is approximate [42].

4.3.2 RPL security objectives:

i) Routing information remains unchanged during transmission or in storage.

ii) Only approved nodes can use the routing data

iii) Routing information available, on demand [43].

Conclusion

The purpose of this survey was accomplished by providing a appropriate overview of IoT security problems, issues and countermeasures research trends in IoT Safety. A counter-measurement scheme was introduced in this survey paper to include a secure multiple authentication method, cryptographic encryption techniques, light weight cryptographic, and efficient routing goals between the cloud server and the IoT system. Finally, some exposed research issues were addressed about threats and vulnerabilities linked to IoT layers. Future developments of this work include the development of a safety model using cryptography techniques.

References

[1] Mardiana binti Mohamad Noor, Wan Haslina Hassan," Current research on Internet of Things (IoT) security: A survey,https://doi.org/10.1016/j.comnet.2018.11.025, Elsevier, 2018.

[2] Vikas Hassija, Vinay Chamola , Vikas Saxena, Divyansh Jain, Pranav Goyal, And Biplab Sikdar , A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE Access 2019,Digital Object Identifier 10.1109/ACCESS.2019.2924045.

[3] ArbiaRiahi Sfar, YacineChallal, ZiedChtourou, "A roadmap for security challenges in the Internet of Things", Digital Communications and Networks, Volume 4, Issue 2, April 2017, Pages 118-137, https://doi.org/10.1016/j.dcan.2017.04.003

[4] Mahmoud Ammar , Giovanni Russello ,Bruno Crispo , "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, Volume 38, February 2017, Pages 8-27.

[5] DilaraAcarali , MuttukrishnanRajarajan, NikosKomninos , and B. B.Zarpelão, "Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks", Hindawi Security and Communication Networks Volume 2019, Article ID 3745619, 13 pages https://doi.org/10.1155/2019/3745619.

[6] Bruno Cruz ,Silvana G´ omez-Meire , David Ruano-Ord´ as , Helge Janicke, Iryna Yevseyeva , and Jose R. M´ endez , "A Practical Approach to Protect IoT Devices against Attacks and Compile Security Incident Datasets",Hindawi Scientific Programming Volume 2019, Article ID 9067512, 11 pages https://doi.org/10.1155/2019/9067512.

[7]KeweiSha, WeiWei, T.AndrewYanga, ZhiweiWangb, WeisongShic, "OnsecuritychallengesandopenissuesinInternetofThings ", https://doi.org/10.1016/j.future.2018.01.059,Volume 83, June 2018, Pages 326-337

[8] Suha Ibrahim Al-Sharekh, Khalil H. A. Al-Shqeerat , “Security Challenges and Limitations in IoT Environments”, IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.2, February 2019.

[9] N Alhalafi, Prakash Veeraraghavan, “Privacy and Security Challenges and Solutions in IOT: A review”, 2019 International Conference on Smart Power & Internet Energy Systems IOP Conf. Series: Earth and Environmental Science 322 (2019) 012013,IOP Publishing doi:10.1088/1755-1315/322/1/012013.

[10] Navneet Verma, Suman Sangwan, Sukhdeep Sangwan, Devender Parsad, “IoT Security Challenges and Counters Measures”,International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019 .

[11] SankarMukherjee, G.P.Biswas, **“**Networking for IoT and applications using existing communication technology**”,**Egyptian Informatics Journal,Volume 19, Issue 2, July 2018, Pages 107-127.

[12] Hezam Akram Abdul-Ghani, Dimitri Konstantas, Mohammed Mahyoub “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018.

[13]Jyoti Deogirikar ; Amarsinh Vidhate, “Security attacks in IoT: A survey”, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),**DOI:** 10.1109/I-SMAC.2017.8058363

[14]H.Reza Ghorbani, M.Hossein Ahmadzadegan,” Security challenges in Internet of Things: survey”, 2017 IEEE Conference on Wireless Sensors.

[15] Marie-Helen Maras, ”Internet of Things: security and privacy implications”, International Data Privacy Law, 2015, Vol. 5, No.2.

[16] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges”,Conference Paper · July 2015 DOI: 10.1109/ISCC.2015.7405513.

[17] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao,A Survey on Security and Privacy Issues in Internet-of-Things, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017.

[18] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao,A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017.

[19] Keyur K Patel, Sunil M Patel, “ Internet of Things-IOT: Definition, Characteristics, Architecture, EnablingTechnologies, Application & Future Challenges”,DOI 10.4010/2016.1482 ISSN 2321 3361 © 2016 IJESC.

[20] Muhammad Burhan, Rana Asif Rehman , Bilal Khan and Byung-Seo Kim , “ IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey”, Sensors 2018, 18, 2796; doi:10.3390/s18092796.

[21] Hanaa F. M., Entesar, H.I,Azza A.A,“ Internet of Things Applications and its Security”, International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 41, February 2019.

[22] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, And Biplab Sikdar,” A Survey On IoTSecurity: Application Areas, Security Threats, And Solution Architectures”,Digital Object Identifier 10.1109/ACCESS.2019.2924045,2019,IEEE Access.

[23] Abdel Rahman H. Hussein,” Internet of Things (IOT): Research Challenges and Future Applications”,(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 6, 2019

[24] Hong-Ning Dai, Zibin Zheng, Yan Zhang, “Blockchain for Internet of Things: A Survey”, IEEE 2019.

[25] Soma Bandyopadhyay, Munmun Sengupta, Souvik Maiti and Subhajit Dutta , “ROLE OF MIDDLEWARE FOR INTERNET OF THINGS: A STUDY”,International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.3, August 2011.

[26] Sunghyun Cho, Sejong Lee, “Survey on the Application of Block Chain to IoT- Research Trend for Applying Block Chain to Io”,Published in: 2019 International Conference on Electronics, Information, and Communication (ICEIC),IEEE,2019.

[27]Chaabouni, Mohamed Mosbah , Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki ,” Network Intrusion Detection for IoT Security Based on Learning Techniques Nadia”,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 3, THIRD QUARTER 2019.

[28] Ivan Farris , Tarik Taleb , Yacine Khettab, and Jaeseung Song, “A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019.

[29] Wei Zhou , Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu , “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”,IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 2, APRIL 2019.

[30] Liang Chen, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Anette Alén-Savikko, Helena Leppäkoski, M. Zahidul H. Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara1, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen1, Päivi Korpisaari, And Heidi Kuusniemi “Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey”,Special Section On Security And Privacy In Applications And Services For Future Internet Of Things, IEEE access,VOLUME 5, 2017.

[31] José Cecílio , Pedro Martinsa , Pedro Furtad, “Planning for Heterogeneous IoT with Time Guaranties”, The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017), Procedia Computer Science 109C (2017) 249–256.

[32] Francesca Meneghello, Matteo Calore, Daniel Zucchetto ,Michele Polese , and Andrea Zanella , “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”, IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 5, OCTOBER 2019.

[33] Imran Makhdoom , Mehran Abolhasan , Justin Lipman , Ren Ping Liu , and Wei Ni, “Anatomy of Threats to the Internet of Things”,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 2, SECOND QUARTER 2019.

[34] Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain “Machine Learning in IoT Security: Current Solutions and Future Challenges”,arXiv:1904.05735v1 [cs.CR] 14 Mar 2019.

[35] Arbia Riahi ,Enrico Natalizio ,Yacine Challal ,Nathalie Mitton ,Antonio Iera, “A systemic and cognitive approach for IoT security”, 2014 International Conference on Computing, Networking and Communications (ICNC)

[36] Ismail Butun, Patrik O¨ sterberg, Houbing Song, “Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2019.

[37] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Poles, Andrea Zanella “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”, IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 5, OCTOBER 2019.

[38] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng, IoT Middleware: A Survey on Issues and Enabling Technologies, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 1, FEBRUARY 2017.

[39] Sooyeon Shin,Taekyoung Kwon,”Two-Factor Authenticated Key Agreement Supporting Unlinkability In 5G-Integrated Wireless Sensor Networks”,Special Section On Recent Advances On Radio Access And Security Methods In 5g Networks, IEEE Access,2018

[40] OKAMURA Toshihiko, “Lightweight Cryptography Applicable to Various IoT Devices”,NEC Technical Journal,Vol.12,2017.

[41] Ahmed Raoof, Ashraf Matrawy, Chung-Horng Lung "Secure Routing in IoT: Evaluation of RPL's Secure Mode under Attacks", 2019, IEEE Global Communications Conference (GLOBECOM).

[42] Wei Yang , Yuan Wang , Zhixiang Lai , Yadong Wan and Zhuo Cheng "Security Vulnerabilities and Countermeasures in the RPL-based Internet of Things", 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

[43] Smitesh Mangelkar, Sudhir N. Dhage, Anant V. Nimkar, "A Comparative Study on RPL Attacks and Security Solutions", 2017 International Conference on Intelligent Computing and Control (I2C2).

[44] Aleksandr Ometov, Vitaly Petrov, Sergey Bezzateev, Sergey Andreev, Yevgeni Koucheryavy, and Mario Gerla "Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications",Article in IEEE Network · March 2019 DOI: 10.1109/MNET.2019.1800240.

[45] https://blog.ipswitch.com/balancing-security-and-ease-of-use-with-two-factor-authentication

[46] R. Sathish, R. Manikandan, S. Silvia Priscila, B. V. Sara and R. Mahaveerakannan, "A Report on the Impact of Information Technology and Social Media on Covid–19," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 224-230, doi: 10.1109/ICISS49785.2020.9316046.

[47] Manikandan, R and Dr.R.Latha (2017). "A literature survey of existing map matching algorithm for navigation technology. International journal of engineering sciences & research technology", 6(9), 326-331.Retrieved September 15, 2017.

[48] A.M. Barani, R.Latha, R.Manikandan, "Implementation of Artificial Fish Swarm Optimization for Cardiovascular Heart Disease" International Journal of Recent Technology and Engineering (IJRTE), Vol. 08, No. 4S5, 134-136, 2019.

[49] Manikandan, R., Latha, R., & Ambethraj, C. (1). An Analysis of Map Matching Algorithm for Recent Intelligent Transport System. Asian Journal of Applied Sciences, 5(1). Retrieved from https://www.ajouronline.com/index.php/AJAS/article/view/4642