IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

Survey on Security Challenges in Internet of Things Applications

M. Anitha, R. Tamilselvi, Dr. D. Arulanandham, M.P. Nachimuthu

Associate Professor, Dept. Of ECE, M.Jaganathan Engineering College, Chennimalai, Erode, India

Assistant Professor, Dept. Of ECE, M.Jaganathan Engineering College, Chennimalai, Erode, India

Associate Professor, Dept. Of Ece, Nandha Engineering College, Erode, India

ABSTRACT: Internet of Things (IoT) is one of the most rapidly used technologies in the last decade in various applications. The smart things are connected in wireless or wired for communication, processing, computing, and monitoring different real-time scenarios. The things are heterogeneous and have low memory, less processing power. The implementation of the IoT system comes with security and privacy challenges because traditional based existing security protocols do not suitable for IoT devices. In this survey, the authors initially described an overview of the IoT technology and the area of its application. The primary security issue CIA (confidentially, Integrity, Availability) and layer-wise issues are identified. Then the authors systematically study the three primary technology Machine learning(ML), Artificial intelligence (AI), and Blockchain for addressing the security issue in IoT. In the end, an analysis of this survey, security issues solved by the ML, AI, and Blockchain with research challenges are mention.

KEYWORDS: Internet of Things, Machine learning(ML), Artificial intelligence (AI), etc.

I. INTRODUCTION

Internet of Things (IoT) is a network of smart things that share information over the internet. The smart things are used to deploy in a different environment to capture the information, and some events are triggered.

The applications of IoT is a smart city, smart home,Intelligent transportation system, agriculture, hospital, supply chain system, earthquake detection, a smart grid system. As per CISCO estimated, the IoT devices connected will be 50 billion at the end of 2020. The grown of IoT devices is rapidly changing as it crosses the total world population. The data generated by the IoT devices are enormous.

In traditional IoT, architecture is three types physical, network, and application layer. In the physical layer, devices are embedded with some technology which way they sense the environment and also able to connect in wired or wireless to the other device. Like in the smart home system fridge can place an order automatically to the registered retailer whenever the fruits chamber empty it, and notification will be sent to the home users.

The similarity in smart hospital patients can monitor in an emergency through sensors and corresponding computing devices. As the sensors are low-end devices, less computation power, and have heterogeneous properties. Implementation of IoT comes with lots of challenges. The standardization, interoperability, data storage, processing, trust management, identity, confidentiality, integrity, availability, security, and privacy are some of the open challenges in various IoT applications. The IoT is one of the most emerging technologies in the last decade and its uses in numerous applications area. Security and privacy are still challenges in many applications area.

Some research work addressing security and privacy issue in IoT is already done. But as the new technology comes, which can address so of the security issue in IoT.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

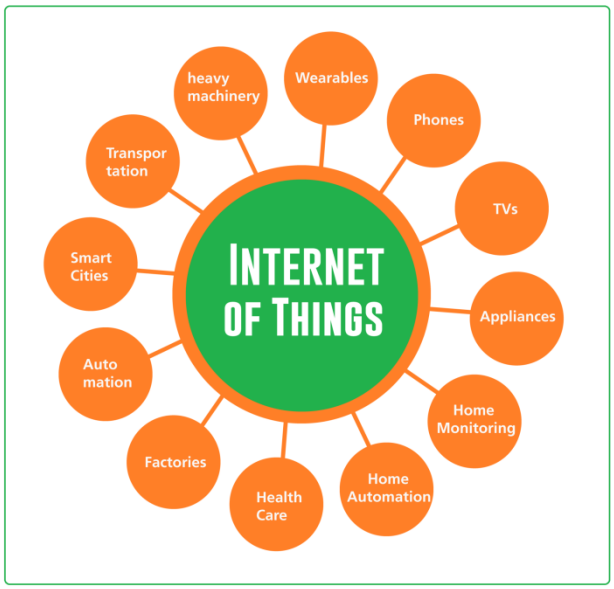

Fig 1. Internet of Things.

Applications:
The main objective of this survey is to find out the security and privacy challenges that exist in IoT applications. It is also identified that some emerging technology that can address security issues present in the system. Here the main goal is to find the research challenges and corresponding solution approach in IoT security.

The following are the contribution of the paper:

- The paper explained the IoT architecture and its enabling technology with challenges.
- The security issues in the IoT system are identified as in-depth layer-wise.
- An extensive survey on similar technologies like machine learning, artificial intelligence, and Blockchain technology integration with IoT security are performed.
- The research challenges and corresponding solution approach with emerging technology (ML, AI, Blockchain) are also explained.

The rest of the paper organized as in related work of security and privacy issues of IoT are identified, and comparison was also made. The IoT architecture details and associated technology are described. The security issues are explained. The different security issues address in IoT applications using Machine Learning, Artificial intelligence, and Blockchain technology are explained in detail in sequentially. An analysis of the entire survey and future challenges are summarized. The paper concludes with a summary of the work done.

II. RELATED WORK

The authors explain the underlying system architecture and security issues in paper.

Previously some works related to a security issue in IoT applications, infrastructure are already done. Although several works already exist in this regard from different perspectives, for implementation purposes, there is no such study done. So in this survey, it is identified the recent emerging technology (ML, AI, Blockchain).

1. Internet of things (IoT) infrastructure, protocol, application:

Smart Homes: This section provides the background of the reviewed smart home technologies. It starts with definitions of smart home and intelligence in the smart home context, followed by a description of a cloud-based smart home architecture. It also identifies important properties of smart homes that make them valuable, active participants in

the modern smart grids.

Software: This section reviews the most important software components of modern smart homes. After outlining important features of operating systems for smart homes and devices, it proceeds with describing two major software subsystems: occupant behavior tracking and data processing.

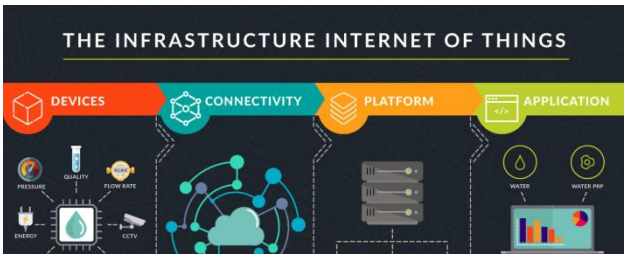

Fig 2. Internet of Things Infrastructure.

2. Connectivity and Communication Protocols:

In a smart home environment, devices need to be interconnected to exchange information. Intelligence, as we previously defined it, is when the environment is ableto understand the state of the current system. For this to happen, a single sensor is not enough to extract muchuseful information, and therefore multiple sensors are needed which can communicate with each other and extend the usefulness of the acquired information. Theways in which these devices and sensors can communicate.

3. Privacy and Security:

The concept of smart home would have not been possible without pervasive computing and multitude of sensors scattered around a house. Unfortunately, the use of these devices, which are usually connected to the Internet (directly or indirectly) and/or use wireless communication,opens up new opportunities for attacks to the security and privacy of the people living in the smart home.

4. Challenges and Future Trends:

Its identified a number of challenges for IoT-based smart homes and propose several solutions. In the area of edge (fog) computing, the point out the need to optimize communication among the SH devices and suggest development of lightweight algorithms for local data processing and reducing the number of transmissions among the devices. The big amounts of data generated by the devices then require new, big data approaches for integration, storage and communication.

Internet of Things (IoT) has lots of potentials to apply in different real-time applications. It integrates sensors, smart devices, radiofrequency identification (RFID), and the Internet to build an intelligent system. As per Goldman Sachs estimated 28 billion smart things would be connected to a different network by 2020. The growth of IoT in the last decade in such a way that it incorporates everything from sensors to cloud computing intermediate with fog/edge computing.

5. IoT has different Security attacks in internet of things:

In some common Internet of Things attacks in the different layer is shown along with the current research work done on the corresponding attacks types.
Jamming Attack: Jamming attack is a subset of DoS attacks where the attacker tries to affect the communication channel in paper also explained the details about the jamming attacks.
Dos Attack: Dos attack is one of the common attack used in IoT applications. Most of the IoT devices area low-end device which is vulnerable to the attacker.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

6. Security Issue:

The attacker Security issue using machine learning:The machine learning is a technique to perform computational intelligently. The model needs to designand test using different learning methods.

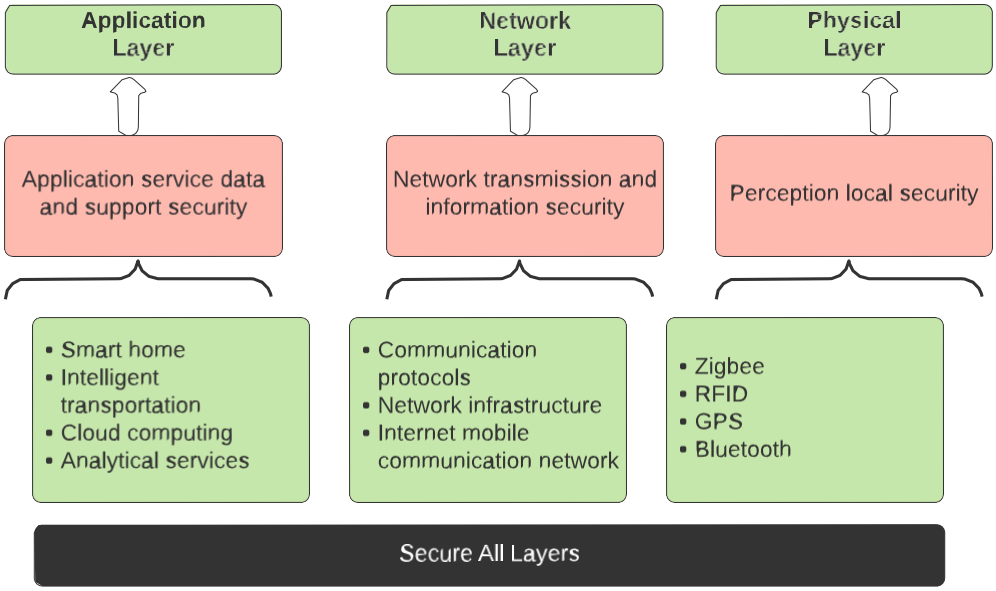

FIG.3. IOT CHALLENGES IN EACH LAYEY

Security Issue Using Artificial Intelligence:

The innovation of smart devices having sensing and actingcapability makes the IoT system usability in widely. As the numbers of devices are connected to the network are huge, which generate a large volume of data. To process and perform computation is a challenging task in an IoT environment. So Artificial intelligence comes as a rescue along with some other emerging technology to address the security issue in IoT. As shown in Fig., IoT and AI can combine to improve the analysis of the Security issue using blockchain technology

Security Issue Using Blockchain Technology:

Blockchain technology is a decentralized/ distributednetwork where each is connected to others in some way.The message is broadcast in the Blockchain network. As shown in Fig distributed architecture based on blockchain echniques in IoT application. A block consists of lots ofvalid transaction and its associated attributes. The smart contract [88] are self executable program used to implement the business logic in the network. The Blockchain network uses different consensus algorithm.

III. CONCLUSION

The authors firstly study in-depth the various security challenges exist in IoT application. Secondly, the authors have surveyed to address existing security challenges.From the survey, it was found that some research has already been done in various technology like Machine learning, Artificial intelligence, and Blockchain technology, which are capable of addressing the existing security issue.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 2, April 2024 ||

International Conference on Recent Development in Engineering and Technology – ICRDET 24

Organized by

Dhaanish Ahmed Institute of Technology, KG Chavadi, Coimbatore, Tamilnadu, India

REFERENCES

[1] K.M. Sadique et al. Towards security on internet of things: applications and challenges in technology.
[2] Procedia Comput. Sci. (2018) N.M. Kumar et al. Blockchain technology for security issues and challenges in IoT.
[3] Future Gener. Comput. Syst. (2018) M.A. Khan et al. IoT security: review, blockchain solutions, and open challenges.
[4] Internet Things (2018) M. Banerjee et al. A blockchain future for internet of things security: aposition paper.
[5] Digital Commun. Netw. (2018) B.K. Mohanta et al. Blockchain technology: a survey on applications and security privacy challenges.
[6] [6] B. Miloud, T. Tarik, B. B. Jorge, and S. Antonio, "A machinelearning security framework for IoT systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details