

INTERNET OF THINGS (IOT): Privacy & Security Issues and their Solutions

Mitanshi Rustagi

Vivekananda Institute of Professional Studies, Delhi, India

Neha Goel

Vivekananda Institute of Professional Studies, Delhi, India

Megha Bansal

Vivekananda Institute of Professional Studies, Delhi, India

Tanvi Dalal

Vivekananda Institute of Professional Studies, Delhi, India

ABSTRACT – IoT is a term which is used commonly to show the connection of billions of devices across the globe through internet. The devices used in IoT are majorly used for data collection and sharing. IoT is anticipated to permeate almost every element of life, from smart cities to the medical field, precision farming, supply chain management, and retail, as well as smart living and smart ecosystems. IoT applications are increasing every day. With the rapid increasing applications privacy and security issues can be seen. In fact, if security is not proper in IoT, it may outweigh the benefits. This paper presents an introduction to IoT, architectures along with the privacy, and security threats. Based on the research findings, the possible existing solutions to this problem have been discussed.

Key words – IoT, Blockchain, Information Security.

I. Introduction

IoT is becoming more popular since it can be used in many different fields including everything from mining and logistics, healthcare, smart homes, and cities people's lives are being transformed by IoT. Through the use of sensors, it allows for object-to-object communication. Because of the current situation's reliance on the internet for everything, this dependence is growing and giving rise to thoughts like these.

IoT makes life easy and now is being used in numerous applications. IoT can be seen to be growing continuously. IoT applications are being widely used due to the rapid development of technologies that support IoT. It can be seen that IoT is being used across several fields in our daily lives. Its applications are not restricted to one domain. IoT applications can be seen almost everywhere like healthcare, smart cities, logistics, smart farming, and transportation as shown in fig. 1.

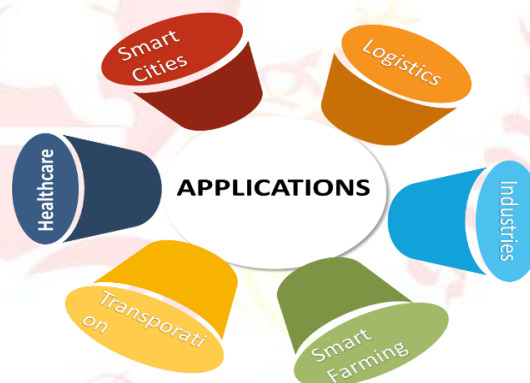


Fig. 1: Applications of IoT

A. Building Blocks of IoT

The significant elements necessary for IoT are explained below and shown in Fig. 2.

1. Identification

The fact that it guarantees that the right person receives the data makes it the most crucial component of IoT.

2. Sensing

This aspect uses sensors to gather data, sends it to data centers, and perform data analysis using various characteristics.

3. Communication

This is accomplished via Bluetooth, the internet, and other technologies.

4. Semantics

In essence, it discusses making wise decisions based on the knowledge that has been extracted or acquired data.

5. Services

IoT provides a lot of services which are referred to as collaborative aware, identity-related, information aggregation related, and ubiquitous services.

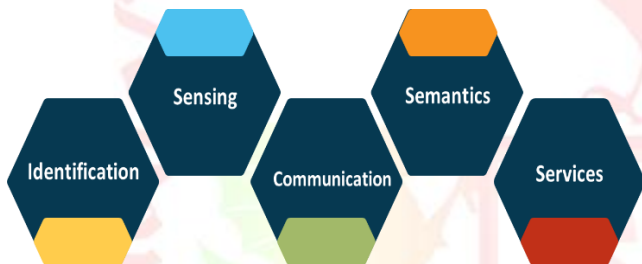


Fig. 2: Elements of IoT

B. Architecture

No unified IoT architecture agreement has been authorized so far for IoT devices. During the study, we discovered that three different forms of architecture are typically under discussion. The three-layer architecture is the first and most widely utilized. Four-layer and five-layer structures are the other two that have been suggested.

1. 3-Layer Architecture

This is the most widely used architecture. This architecture is often referred to as fundamental architecture. It comprises of three layers and has been shown in fig. 3 below:

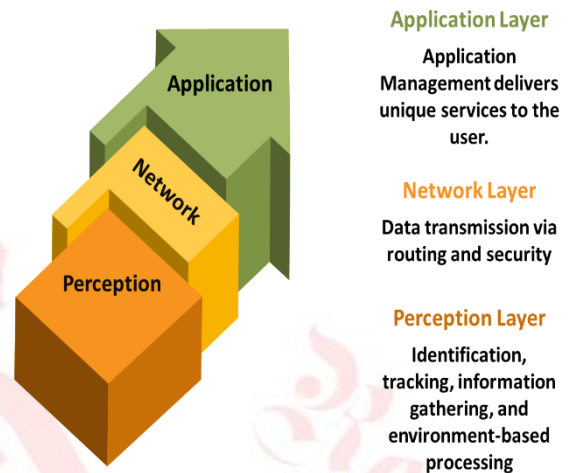


Fig 3: 3-Layer Architecture

2. 5-Layer Architecture

Also suggested is a five-layer architecture. Five different levels make up this architecture. Perception, Transport, Processing, Business, and Application layers make up the five layers. Information transmission and data confidentiality are handled by the transport layer. The Processing layer is concerned with managing services and storing data. The IoT system is finally managed by the business layer, which also keeps an eye on the other 4 layers. Perception and Application continue to function in the same ways as the other two layers.

II. Literature Review

M.A. Iqbal et al. [2] states the importance of IOT along with the crucial security and privacy issues. The author also discussed about various possible solutions related to security.

O. Alfandi et al. [3] briefed about the tremendous growth in IoT applications over the years. 4-layer architecture helps in determining potential privacy and security risks and minimizing those weaknesses by implementing blockchain technology.

M. Dabbah and A. Rayes [4] discussed about IoT and its applications. Security and privacy are the serious concerns rises due to IoT when gadgets are interconnected with each other, followed by what defensive measures may be implemented to stop, detect or lessen those attacks.

S.N. Mohanty et al. [5] briefed about security & privacy and solutions offered with the help of blockchain in IoT. The author proposed an ELIB model which can be installed in a smart home environment.

AKM. B. Haque and S. Tasmin [6] demonstrated IoT, its architecture, elements of IoT. Also, the security and privacy issues were highlighted with their recommended solutions.

Q.I. Sarhan [7] demonstrated the importance of IoT in our daily lives. Features of IoT were also been stated. The functioning of protocols on different layers of IoT architecture along with security challenges on each layer were also been stated.

A.H. Hussein [8] briefed about IoT and its numerous applications like smart cities, precision farming, medical science, smart home & environment, smart living, and supply chain management. The author threw light on a few challenges related to privacy and security that needs to be addressed along with potential solutions to the issues.

P.I.R. Grammatikis et al [9] shared a glimpse on IoT, devices used in IoT, its architecture, security requirement, challenges, and challenges. The threats were categorised to low, medium, and high. Few protocols were being identified to minimize the threats.

M. Abomhara and G.M. Koien [10] drew attention on IoT perception by enabling connections between people and objects via any path, network, and service at anytime, anywhere. Few privacy and security concerns were also being raised.

H. Jain and N. Jain [11] briefed about IoT, building blocks of IoT, applications, and different types of architectures. The author also focussed on Green IoT, the newer concept of IoT, and the challenges related to green IoT.

The literature review has helped in understanding the applications of IoT, architecture, and various types of IoT challenges.

III. Security & Privacy Issues

The key security requirements for IoT system are confidentiality, integrity, availability, and authentication. Protecting private information so that only permitted persons can view and access it along with preserving information privacy is known as confidentiality. Integrity is ensuring that no unauthorized parties have altered or damaged the data. Availability refers to accessibility of information. Authentication, confirming the legitimacy of the parties making the information access request.

As we know that IoT is a structured multi-layered model. IoT 4-layer architecture includes perception layer, network layer, processing layer, and application layer. Few risks associated with each layer is shown in fig. 4.

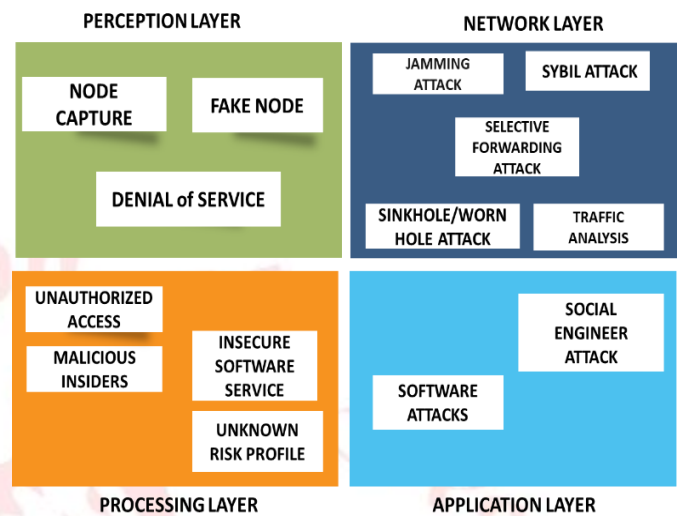


Fig 4: Security risks associated with each layer

Furthermore, the security risks can be categorized into:

A. Low-level risks

Some of the low-level risks are Sybil attacks, jamming attacks, attacks of sleep privation, insecure start-up, and physical interface unreliable. Based on the literature review, the suggested remedies for low-level risks are as follows: anti-jamming mechanism, safe physical layer communication, detect Sybil attack and spoofing threats, inappropriate physical protection, and sleep deprivation attacks.

B. Intermediate level risks

A few examples of this category are the assault of RPL, fragmentation report, sinkhole or wormhole attack, and end-to-end transportation safety. As per the study, a few solutions are recommended: Elliptical curve encryption (ECC), VeRA authentication system, and a cloud-based IoT through an authentication technique for safe packet forwarding.

C. High-level risks

They are concerned with IoT applications. Some examples are listed: unsafe interfaces, security of middleware, CoAP security issues, and uncertain software. According to the literature review, some solutions are suggested to minimize high-level risks.

IV. Remedial Solutions for Privacy and Security Issues

IoT has three main issues: privacy, confidentiality of business processes along with third-party dependability. Protection of user data and privacy can be seen as one of the key challenges which IoT is facing. Thus, advanced technology is required to make IoT more secure.

To address the security and privacy issues in IoT, extensive research has been carried out. Some of the common solutions can be by making use of cryptographic algorithms like Triple DES, RSA etc., changing the passwords frequently, not relying on cloud technology, updating the IoT devices on regular basis, collect only relevant data for the operation. Authors in [16] have proposed a software model, layered approach in [17], blockchain [5], access control models [4].

Blockchain can prove to be an optimal solution for the issue addressed above, this has been concluded on the basis of research carried out by various authors. Table 1 clearly shows that this technology has been used by several authors across the globe to deal with the problem.

Table 1: Review of work done by Authors using Blockchain

Name of Author	Year	Technology used
Rahman	2020	Blockchain
Mohanty	2020	Blockchain
Mohanta	2020	Blockchain
Islam	2020	Blockchain
Sachi	2020	Blockchain
Omar	2020	Blockchain
Miraz	2018	Blockchain
Roy	2018	Blockchain
Dorri	2017	Blockchain
Fremantle	2017	Blockchain
Ouaddah	2017	Blockchain

Blockchain is the foundation of Bitcoin. It allows the execution of the transactions in a decentralized manner. This technology is gaining huge popularity and is being used in a vast variety of areas including digital currencies, record keeping, securities, smart contracts, etc. Blockchain exists in three types as shown in fig. 5: public, private, and consortium. All users of a network can read and write on a public or permissionless blockchain without anyone having to acknowledge their identity. In contrast, read/write access to a private or restricted blockchain is only granted after the user's identity has been approved. In a consortium or federated

blockchain, anybody can access the data, but only those with the proper permissions can make changes. Blockchain being used as a booster for security and privacy of IoT devices is shown in [5]. Decentralization, Security, and Immutability and finally Identity are some of the major improvements which can be seen after integrating blockchain with IoT. Since the blockchain has a nature of decentralization it can help in overcoming the centralized security issue. The distributed ledger and decentralization offer redundancy of data wherein every node is required to have a copy of data thereby making the data immutable and reliable. Smart Contracts is a special feature that blockchain provides which helps in ensuring security of data. An ELIB model has also been proposed in [7] which uses the concept of blockchain. Its application in smart homes has also been shown. A similar approach is shown in [15] that ensures security and privacy in IoT devices.

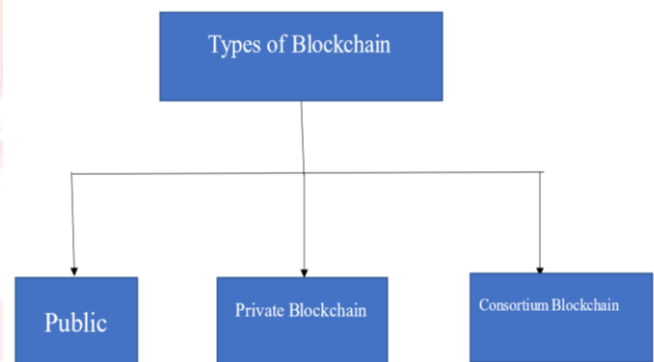


Fig. 5 Types of Blockchain

To deal with security and privacy issues, Access Control methods is yet another way. The access control mechanisms are bifurcated into 4 distinguished segments: DAC (Discretionary Access Control), RBAC (Role-based Access Control), ABAC (Attribute-Based Access Control), and MAC (Mandatory Access Control). RBAC is the most popular amongst these. It gives the data requestors particular roles and accompanying access rights. This paradigm is inadequate to determine the access privileges of IoT devices as continuously the roles are being changed depending on the functions of each. The ABAC model, is more adaptable, processing the ability to determine the access control rules according to each device's characteristics. The integration of ABAC model with blockchain technology can be a potential strategy in this field.

V. Conclusion

IoT is the collection of all the devices possessing the ability of connecting to the internet and collecting and sharing of data. It is a billion-dollar business now a days and provides smart solutions to a vast variety of applications. This smart technology faces a lot of privacy and security threats. The current paper presents the various privacy and security threats that IoT faces. Based on work done by various authors the possible solution which exist to deal with this problem are presented It has been concluded that block chain technology can prove to be an ideal solution to deal with this problem, despite of some of the problems like high resources are required, computationally expensive, involve high bandwidth, and may cause overhead delays.

VI. References

- [1]. Yong Ho Hwang, "IoT Security & Privacy: Threats and Challenges", IOTPTS's15 April 14, 2015, Singapore.
- [2]. Muhammad A. Iqbal et. al, "A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches", Global Journal of Computer Science and Technology: E-network, Web & Security, Volume 16, Issue 7, version 1.0, 2016, Online ISSN: 0975-4172.
- [3]. Omar Alfandi et. al, "A Survey on Boosting IoT Security and Privacy through Blockchain", Cluster Computing, Springer Science+Business Media, LLC, part of Springer Nature 2020.
- [4]. Mehیار Dabbagh and Ammar Rayes, "Internet of Things Security and Privacy", Internet of Things from Hype to Reality, Springer Nature Switzerland AG 2019.
- [5]. Sachi Nandan Mohanty et. al, "An Efficient Lightweight Integrated Blockchain (ELIB) model for IoT Security and Privacy", Elsevier Future Generations Computer Systems 102(2020) 1027-1037.
- [6]. AKM Bahalul Haque and Sonia Tasmin, "Security Threats and Research Challenges of IoT: A review", Journal of Engineering and Advancements, Volume 01(04)2020, pp 170-182.
- [7]. Qusay Idrees Sarhan, "Internet of Things: A Survey of Challenges and Issues", Int. J. Internet of Things and Cyber-Assurance, Volume 1, No. 1, 2018.
- [8]. Abdelrahman H. Hussein, "Internet of Things (IoT): Research Challenges and Future Applications", International Journal of Advanced Computer Science and Applications (IJACSA), Volume 10, No 6, 2019.
- [9]. Panagiotis I. Radoglou Grammatikis et. al, "Securing the Internet of Things: Challenges, Threats and Solutions", Elsevier Internet of Things, Volume 5, pp.41-70, 2019, ISSN: 2542-6605.
- [10]. Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things: Current Status and Open Issues".
- [11]. Hamender Jain and Neha Goel, "A Newer Approach to IoT: Green IoT", International Journal for Modern Trends in Science and Technology, 7(03): 154-160, 2021, ISSN online: 2455-3778.
- [12]. Paul Fremantle et. al, "Enhancing IoT Security and Privacy with Distributed Ledgers- a Position Paper", ResearchGate, Conference Paper, 2017.
- [13]. Mirza Abdur Razzaq, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", ResearchGate, Article in International Journal of Advanced Computer Science and Applications, January 2017.
- [14]. Shavan Askar et. al, "Blockchain for Securing IoT Devices: A Review", ResearchGate, Article 2017.
- [15]. Ali Dorri et. al, "Towards an Optimized Blockchain for IoT, Proceedings of 2nd ACM/IEEE International Conference on Internet of Things Design and Implementation, Pittsburgh, PA, USA, April 2017.
- [16]. Salman, O., Elhajj, I., Chehab, A. and Kayssi, A., 2017, May. Software defined iot security framework. In 2017 Fourth International Conference on Software Defined Systems (SDS) (pp. 75-80). IEEE
- [17]. Tewari, A. and Gupta, B.B., 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems, 108, pp.909-920.

Manuscript Processing Footprints

A. Journal Volume/Issue Details

This manuscript is published in **Vol. 15 No. 02 2025** issue of IARS' International Research Journal (I'IRJ).
This is a Peer Reviewed (Refereed) International Journal published by IARS' Press Australia (International Association of Research Scholars)
The Volume/Issue is a regular issue of the journal published in **August 2025** Available at: <https://research.iars.info/index.php/curie>.

B. Copyright, License, and Publishing Rights

- IARS' Press Australia (International Association of Research Scholars) respects the rights of the authors of research content published with IARS' International Research Journal. The "First Publication Rights" (FPR) to the original work accepted for publication at IARS' International Research Journal is granted to the Publisher of the Journal but copyright for all work published in the journal is retained by the author(s). Works published in the Journal are distributed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). (This license lets others distribute, remix, adapt, and build upon your work, even commercially, as long as they credit you for the original creation. This is the most accommodating of licenses offered. Recommended for maximum dissemination and use of licensed materials.)
- After publishing the content with IARS' International Research Journal, the author holds complete right on the content for its amendments and reuse in any form. IARS' International Research Journal confirms that author(s) holds the copyright of the content.
- Author(s) grant(s) permission for their work to be indexed in part/full form in commercial and non-commercial indexes. Author(s) grant(s) permission for their work to be harvested in part/full form in commercial and non-commercial archives and distributed through them. Author(s) grant(s) permission for their work to be translated in part/full form in any language and republished and redistributed. Author(s) may enter into separate, additional contractual agreements for the non-exclusive distribution of the published version of the work, with an acknowledgement of its initial publication in this Journal.
- It is the responsibility of the author(s) to secure all necessary copyright and/or permissions for the use of third-party content in their manuscript(s). Author(s) have declared the same at the time of submission of manuscript and 'may also be required' to provide written evidence of this permission anytime in case required for any purposes.
- Publications Ethics and other Terms and Conditions as mentioned on official website of IARS' International Research Journal.

C. Last Plagiarism Report



Settings: Quotes Excluded, Bibliography Excluded

**INTERNET OF THINGS (IOT): Privacy
& Security Issues and their Solutions**
1 part - 2,452 words

9%

Mitanshi
Rustagi

Exemption / Relaxation by Editor: None

D. Processing Track

Date of Submission	28 June 2025
Date of Final Review	05 August 2025
Date of Acceptance & Schedule	20 August 2025
Date of Publishing	29 August 2025

----- O -----