Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

Data Security in IOT

Vongaiishe Ruth Moyo
Department of Computer Science and Applications
Sharda University
Greater Noida,India

Kudzaishe Mazonde
Department of Computer Science and Applications
Sharda University
Greater Noida,India

Neha Kashyap
Department of Computer Science and Applications
Sharda University
Greater Noida,India

***Abstract*— Internet of Things (IoT) has been a growing field from past few years, it comes with a lot of advantages to the users for example the famous creation of Smart-Cities, Smart-homes, Smart-Agriculture and more. However it comes with its own challenges especially on its applications, platforms and security of data. In that aspect, the purpose of this review paper is to outline the challenges which are faced by each layer of IoT and weigh the different solutions by reviewing which algorithms and cryptographic concepts will be the best to solve the security issues. Based on the findings of this study, the concluded algorithms are supposed to work efficiently when deployed to solve the data security issues..**

***Keywords*— Internet of Things(IoT), DataSecurity, Algorithm, Cryptography**

I. INTRODUCTION

Internet of Things (IoT), a continuously evolving arm of technology today has become a major contributor to the advancement of industries and the world at large. IoT can be described in simple terms as a concept of connected objects and devices of all types over the internet [15]. IoT can be branched into 4 types which are consumer, commercial, industrial and infrastructural. It comprises of layers in which the real world is brought into the computer based system. This is done through the sensors that generate and collect data and shared through the network layer[3].Due to the enormous IoT data, extensive storage space and high maintenance are a demand[5] thus leading to the cloud based IoT which in turn raises the concerns of data security.

The role of IoT is to make day to day life easier. With the forming of wireless networks, advanced sensors, Artificial intelligence, Machine learning and more popular and trending emerging technologies IoT is rapidly becoming one of the biggest fields. Today's technology based companies are also discovering and introducing devices which do predictions. IoT applications can be recognized under many other sectors, like factory production, home automation, supply chain, smart cities etc.

Cloud computing is the system which completes the IoT, this is because it collects all the big data from IoT and humans at a low cost service in the cloud. This whole process happens in the cloud [5] the sensors gather data and store in the cloud, other devices which exchange the information with the sensors that get it from the cloud. In the cloud there is cloud discovery which keeps data inside a data warehouse, the Cloud data Migration that determines which data to load in the cloud depending on how useful efficient it is and the last are cloud data maturity which basically makes the cloud data management strategy [10,5,11].It is shocking to know that almost 30 billion devices connected will mark through the Internet meaning this rate is very high and it keeps on increasing every year [5]This makes the field of IoT the most vulnerable if data is not handled properly, systems can be attacked jeopardizing the users trust and need to enjoy the luxury they bring[17].Data security sure that the data is safe even when stored in cloud encryption advanced techniques are used to ensure that attacks are reduced.

II. OBJECTIVE OF THE PAPER

The objective of this review paper is to figure out and analyze the different mechanisms and techniques that are used in securing data in the field of IoT. A lot of other related works have been gathered from different sources to bring the conclusion on the concept of securing data in IoT. It takes a lot of months, time, and resources from the authors to do research and bring out discoveries and conclusions, they also try to keep up with the new and emerging technology. The goal of this paper then is to indicate where there are gaps, what should be done, and the improvements needed to protect data as new fields like Artificial Intelligence(AI) and Machine Learning(ML) are becoming popular and are being used in our daily lives. It clearly describes the algorithms and the cryptographic methods that are being used and analyses which one is the best; therefore, it compares the different techniques which are there and which is the best. This paper address the best way to secure data in IoT devices so that hackers and other unauthorized personnel cannot access the data due to the concept recommended.

The problem that we have now is the users trusted the IoT devices and they adapted to use them in their day to day life however fraudulent, hackers and other unauthorized personnel are using the data like critical credentials, medical records, bank details and other critical information of users, to use the information against their will also some companies even gather the data of the users without their consent and sell it to other companies too to train their AI models and do other activities without the user concern. This brings them to a point where they are concerned about their overall well-being and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

assessing if this technology is worth it; therefore, their trust in this technology is broken.
In this paper the Architecture of IoT is discussed. data storage is also explained along with the security issues in IoT devices and the different Algorithms and Cryptographic techniques which are used to secure the data. The main focus on the paper is to get the best mechanisms of securing the data.

Contributions:
This is the summary of the whole idea of this paper:

- The first question is "What is the best method of securing the data of the IoT devices?"
- We studied the different the previous works of data security, specifically the algorithms and cryptographic mechanisms on IoT data protection
- The paper gives the literature review of privacy concerns, algorithms, data security, attacks on IoT data

III. ARCHITECTURE OF IOT

The architecture of IoT is made up of multi-layers, which have been presented by researches uniquely [19] some researchers say the architecture is composed of 4 layers, others 5 layers [20]and the proposed CISCO Model have 7 layers, it all differs based on the researcher, their specialty and their analysis. Even though there is no standardized design of architecture, each uses a variety of technologies, raising a security concern [3,12]. This paper is going to focus on 4 important layers that will outline the functions of the IoT devices and systems. These layers are the Physical Layer, Network Layer, Middleware Layer, and Application Layer. Fig 1 shows how the IoT is structured and how data is shared from layer to layer.

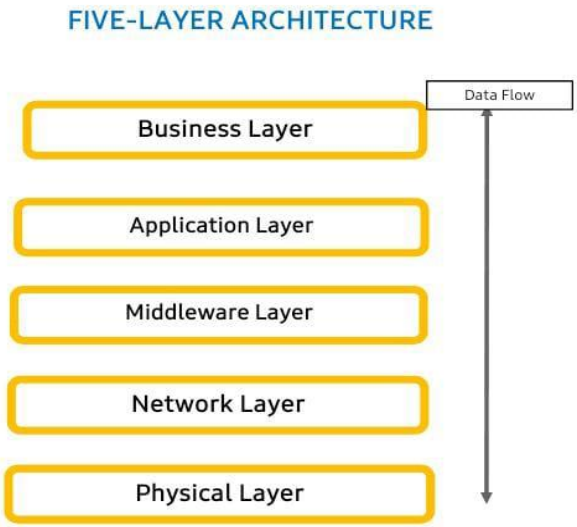

Fig. 1: IoT Five Layer Architecture

A. Physical layer

It is the base layer as it focuses on the physical devices that collect data from the outside real-time environment and then convert it into electronic signals.[21] The physical devices include the different types of sensors, actuators, RFID chips, barcodes, etc. The main role of sensors is to sense what is happening in the environment they are in, and the actuators are the ones who take action based on the sensed data.[20] So, for example, there is fire, and the sensors will sense the heat, and then the actuators will then make action so they work hand in hand. However, there are a lot of attacks for this layer, and we will focus on a few, which are False Data Injection Attacks (FDIs). This is an attack where there is a generation of incorrect data resulting in the malfunctioning of the whole system. Another one is there is a chance that, because of the different authentication mechanisms which are used between different nodes, sensitive data is accessed without authorization. [13]

B. Network Layer

For various communication protocols are used for connectivity and for delivering information from the perception layer to the computer processing system. These include Zigbee, Bluetooth, LoRa, Wi-fi, WiMax, etc, these transmission mediums deliver the information from the perception layer to the information processing system [21]. However, there are also attacks that breach these designed protocols and can cause disruption of the network flow, manipulation of data, and illusions in the network [10], causing a different range of malicious outcomes [3]. The few common attacks are Distributed Denial of Service (DDoS) attack, this is launched by a hacker having intentions of the disabling the network [10]. Another one is the Routing Attack which changes the data transmission paths so as to delay or redirect the data. In addition, Man-In-The-Middle (MITM), it is when an attacker will come between two different communicating parties so that they redirect the data or disrupt the communication. Lastly there is a Sybil attack which involve a malicious device, mimicking multiple identities in the network [3]. Fig 1.1 shows some of the gateways involved when transporting data

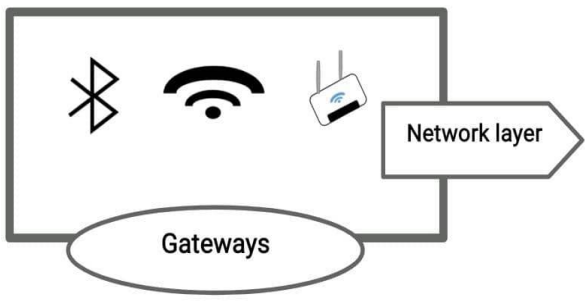

Fig. 2: Gateways Working on Transporting Data

B. Middleware Layer

The objective of this layer is to connect the network layer and the application layer [13], by processing the data received from the computing processing systems and make decisions based on the results [11]. It also gives quality computing and storage services [20]. The few common attacks involved in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

this layer are the SQL Injection Attack. It is when the attacker threatens the whole database system, obtaining user private data, they can do this by using SQL statements like delete, update, read and write operations. Another common attack is the Signature Wrapping Attack (SWA) where the attacker can break the algorithm of signatures to modify or falsifying signatures [10].Fig 1.2 shows the processes units involved in this layer.

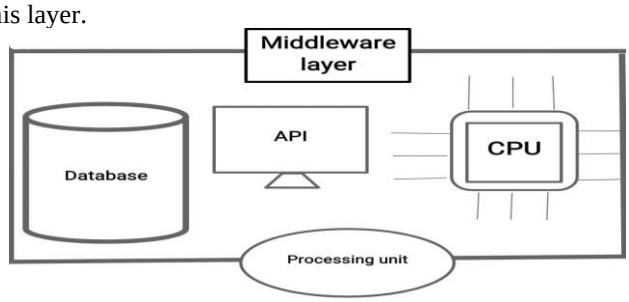

Fig. 3: Processing of Middle Layer

C. Application Layer

In this four-tier architecture, this is the top layer. It is the one that is directly connected to the end users as it the visual output of the data produced by the IoT technology. Its purpose is to deliver the customized services to the user [19,20]. All the IoT applications like SmartHomes, SmartCities, SmartAgriculture etc are all present in this layer. The devices on this layer are all dependent on the applications, and that is how they can be operated by the user [13]. The various attacks which involved in this layer are different from the three others. The type of the issue present are the data theft and privacy issue.Fig 1.3 shows various use of application layer.

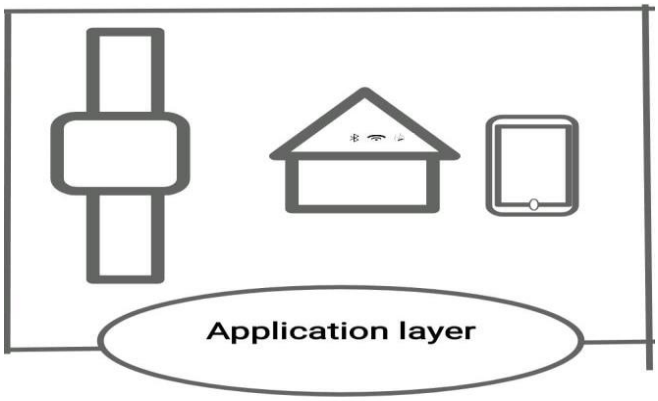

Fig. 4: Uses of Application Layer

E. Business Layer

It controls the entire IoT systems. It encourages research for good business models and profit models. Business models ,graphs, flowcharts are build using the data provided by the application layer.The success of IoT system does not only depend on technologies but by the gurantee of customer service satisfaction.

IV. TECHNIQUES

For all these layers to transmit data, different communication protocols like, Zigbee, Bluetooth are used. Owing to the prevalence of risky applications due to their natural multiplicity of data collection there is need to keep data secured to the highest level possible. Ways that can help secure data include

A. Authentication and Authorisation

Information security is one of the most vulnerable in the authentication of Iot.[15].Multifactor authentication and role based access are needs as they helps block unwanted foreign data access and provide only relevant data respectively.

B. Data Encryption

Cryptography is used to secure information and communication channel.
The most trustable method currently being used by most companies is the public key infrastructure[6].
Public encryption with keyword search scheme (perks) was introduced by Boneh .Later proposal of multidimensional range query cipher text were raised and introduced by

Table I: Comparison of Symmetric Key Algorithms

Algorithm	Key Size	Block Size	Speed	Security
AES	128-256bits	128bits	Fast	High
DES	56bits	64bits	Slow	Low
3DES	168bits	64bits	Slow	Medium
Blowfish	32-248bits	64bits	Fast	Medium
Twofish	128-256bits	128bits	Fast	High

Table II: Comparison of Asymmetric Key Algorithms

Algorithm	Key Size	Speed	Security
RSA	1024-4096	Slow	High
Elyptic curve cryptography	160-512	Fast	High
Diffie Hellman	1024-4096	Slow	High

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

Table III: Literature Review of Other Authors' Works

Paper	Focus	Key Findings	Challenges
15	IoT security challenges	Identifies spoofing,jamming and unauthorised access as major threats	Difficulty in securing Iot networks.
16	IoT security trends	Simulation tools and modelers help in Iot Security research	Failure in Iot Security can lead to serious consequences
17	IoT Security and privacy	Evaluates GDPR compliance of major IoT platforms	Ensuring compliance with GDPR and other data protection and regulations while implementing solutions
19	IoT Cybersecurity Framework	Emphasis on the need for scalable and testable cybersecurity measures	Ensuring uniform standard security across Iot Devices
20	IoT Security and privacy	Addresses security concerns such as authentication and encryption	Privacy and security remain unresolved issues
22	IoT Platform Comparisons to	Highlights technological approaches to Iot Security	Security risk from wireless sensor networks requiring robust cryptographic security solutions

CONCLUSION

IoT data security has always been a key area of concern in which more issues and solutions have been developed each day over time .Through use of some of the mentioned techniques and methods,the risk of users' data security can be reduced and put under control.As the technologies on the other hand continue advancing, the data security efforts should in turn also advance respectively in order to have a better chance of tackling possible threats

REFERENCES

[1] Xiong, J., Shen, L., Liu, Y., & Fang, X. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. Scientific Reports, 15(1), 3.
[2] El-Sofany, H., El-Seoud, S. A., Karam, O. H., & Bouallegue, B. (2024). Using machine learning algorithms to enhance IoT system security. Scientific Reports, 14(1), 12077.
[3] Adam, M., Hammoudeh, M., Alrawashdeh, R., & Alsulaimy, B. (2024). A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access.
[4] Kashyap, N., Rana, A., Kansal, V., & Walia, H. (2021, September). Enhanced Data Security and Authentication Techniques for IoT Devices on Cloud. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-6). IEEE.
[5] Laghari, A. A., Li, H., Khan, A. A., Shoulin, Y., Karim, S., & Khani, M. A. K. (2024). Internet of Things (IoT) applications security trends and challenges. Discover Internet of Things, 4(1), 36.
[6] Anedda, M., Floris, A., Girau, R., Fadda, M., Ruiu, P., Farina, M., ... & Giusto, D. D. (2023). Privacy and security best practices for IoT solutions. IEEE Access, 11, 129156-129172.
[7] Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. Scientific Reports, 13(1), 21255.
[8] Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. IEEE Access, 11, 120918-120934.
[9] Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. Scientific Reports, 13(1), 21255.
[10] Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in Internet of Things: A review. IEEE access, 10, 104649-104670.
[11] MAHMOUD ABBASI , (Member, IEEE), MARTA PLAZA-HERNÁNDEZ1,JAVIER PRIETO , (Senior Member, IEEE), AND JUAN M. CORCHADO "Security in the Internet of Things ApplicationLayer: Requirements, Threats, and Solutions"
[12] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.
[13] Tao, Y., Xu, P., & Jin, H. (2019). Secure data sharing and search for cloud-edge-collaborative storage. IEEE Access, 8, 15963-15972.
[14] Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. IEEE access, 8, 23601-23623.
[15] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEe Access, 7, 82721-82743.
[16] Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big data, 6(1), 1-21.
[17] Ganapathy, S. (2019). A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks, 151, 181-190.
[18] Chaudhary, A. (2022). Internet of things (IOT): Research challenges and future applications. International Journal of Emerging Trends in Science and Technology
[19] Meziane, H., & Ouerdi, N. (2022). A Study of Modelling IoT Security Systems with Unified Modelling Language (UML). International Journal of Advanced Computer Science and Applications, 13(11).
[20] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEe Access, 7, 82721-82743.
[21] Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big data, 6(1), 1-21.