© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

Intelligent IoT Communication System Based on Block Chain

Ishita Gupta
ishita0935@gmail.com

1 Introduction

The Internet of Things (IoT) is a sophisticated form of networking that uses unique identifiers for each device. IoT integrates various technologies such as hand-held digital devices, industrial machinery, animals (or) people, or any physical-digital entities to work together to achieve the application's purpose. However, there are several security concerns. Among them are denial-of-service (DoS) attacks, data theft (or) data breaches, and botnet attacks, in which several systems take control of the victim's system to extract the victim's confidential data. Unsecured devices are the primary security concern in edge computing and IoT frameworks because they are used to increase network coverage. There are also devices within an IoT that can migrate from one network to another, posing a serious security risk. The conventional IoT network now considers the concept of zero trust, which is a mechanism for safeguarding the internet infrastructure and the IT system. It also implies that it allows any device to join a network or access resources within a network, assuming they are also authorized. As a result, once a firewall system in an IoT has been bypassed, it is easy for attackers to function concurrently with the normal node and could be difficult because there are numerous IoT devices, most of which are highly vulnerable and unsecured. This phenomenon facilitates an adversary's use of the gateway system in an IoT environment.

There are currently three layer-based IoT operations: i) three-layered architecture, ii) four-layered architecture, and iii) five-layered architecture. The application layer, network layer, and perception layer comprise the three-layered architecture, while the four-layered architecture includes the application layer, support layer, network layer, and perception layer. The business layer, application layer, processing layer, transport layer, and perception layer are the five layers of architecture. A closer examination of all taxonomies reveals that three layers are the most commonly used in most IoT applications. As a result, the proposed system considers a three-layered architecture.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed
DOI : 10.5281/zenodo.7016184

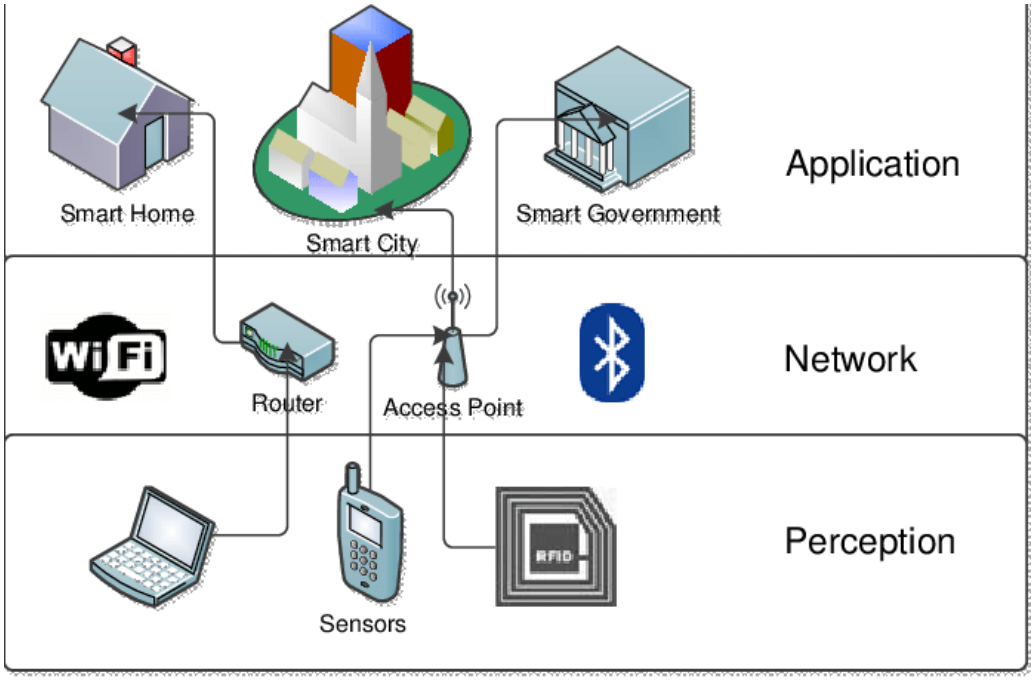

Figure: Three-layer architecture of IoT (Source: DOI: 10.20533/ijisr.2042.4639.2015.0070)

The application layer is used to define all IoT applications and is frequently infected with various intrusions, such as malicious code and cross-scripting attacks. However, it is dependent on the application's sensitivity. The network layer is used for transmission and forwarding all data received from the IoT device. This layer contains the majority of the communication protocol. There are numerous types of intrusions in such layers, including denial of service attacks, man-in-the-middle attacks, storage attacks, and exploit attacks. The perception layer is the bottom layer, responsible for extracting raw sensory data and forwarding it to the network layer. This layer is generally vulnerable to eavesdropping replay attacks and node capture attacks. Because the proposed study focuses on developing a secure communication scheme in which Blockchain plays a significant role, the network layer is used as the host in the algorithmic operation. Other layers (application and perception) can be automatically secured if the network layer serving as an intermediate bridge is highly secure.

The network's low visibility is the next security issue in an IoT environment. Currently, the use of devices in an IoT is increasing exponentially, making it difficult to provide generalized security for all devices. Traditional information technology security practices require accounting for all network components; however, this is not feasible in IoT due to many IoT devices and mobility factors. The connection between security and mobility has yet to be resolved. The next security issue in an IoT is related to software vulnerabilities. For example, telecommunications service providers (TSP) are vulnerable to cyber-attacks by bargained IoT sensors linked to their user networks. Such cyber-attacks will significantly impact the target systems' intense effects and the

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

telecommunication service providers (TSP). The use of multiple protocols and IoT devices necessitates the use of numerous overlapping software. Each piece of software has a distinct feature and vulnerabilities that an adversary can exploit. It will also cause downtime due to the generation of errors when interacting with one another, as well as more vulnerable data.

Adopting open-source software is another commonly used step in many organizations to protect critical resources; however, such open-source software is easily compromised by attackers. Although updating the software could help significantly thwart the attacker, updating such large amounts of software is impossible. It not only causes downtime but also makes the entire network vulnerable. Another critical security issue in the IoT environment is a user knowledge gap. Users cannot be expected to know all the various attack strategies and vulnerable environments. Users are less worried about the security problems related to IoT device use and more interested in the ease of these devices. Another source of security concerns in IoT is the communication channel. Attacks are more likely to originate from the communication channel used by an IoT component connected in various ways. Currently, multiple protocols are used in an IoT communication system with a reported security issue known to harm the entire networking system.

Existing security solutions do not place the same emphasis on maximum security standards in IoT. More effort is being directed toward achieving privacy, primarily at the expense of other criteria. As a result, the proposed study identifies this issue while incorporating different security standards, such as anonymity, confidentiality, availability, integrity, and privacy. It is not practical to use existing encryption practices for secure communication. There is no evidence that they are more sustainable than devices with limited resources when balancing communication demands and security. The proposed study employs analytical and experimental models to provide proof of concept for data security using Blockchain and the McEliece algorithm. Existing approaches cannot construct precise decisions for providing reliable resistance against unknown threats in IoT due to a lack of appropriate intelligence-based security services. The proposed system also includes an SDN capable of providing more information and making better decisions regarding data routing from the sensor to the IoT cloud. There is no doubt that blockchain technologies offer exceptional security. There is no doubting, however, that it has several shortcomings that have not yet been addressed in any previous studies. This problem is addressed by revising the traditional blockchain design, which eliminates legacy issues.

2. Objectives

The study's main goal is to build an intelligent framework that can more securely streamline an IoT's communication demands to resist lethal adversaries. By utilizing the potential features of Blockchain, security in the communication process is developed.

3. Types of attacks in IoT

- **Physical Tampering:** When physical devices are used in environments that humans cannot access, there is a risk of unauthorized tampering with such equipment.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

- **Denial-of-Service:** This assault, one of the most frequently reported in both cloud and IoT contexts, paralyzes the whole network and servers, making it simpler for attackers to access the network or carry out other nefarious purposes.
- **Firmware jacking:** The updates may also be compromised if the network is penetrated. When such compromised firmware updates reach hardware, they infect it because the source of the firmware update origination point's source authentication was unsuccessful.
- **Malicious Node Injection:** The adversary physically places the malicious nodes among the typical IoT devices. The malicious nodes are capable of illicit data sniffing and different sorts of unauthorized network management.
- **Brute-force password assaults** are further used to access devices in exposed IoT setups.
- **Eavesdropping:** The attacker node can compromise and intercept the open communication channel. There is a weak place in the communication route where the attacker may take all the vital information.
- **Escalation in force**: An attacker may exploit several operating systems, hardware, and software weaknesses to gain unauthorized access to IoT resources.

4. Current security methods and use of blockchain technology to improve security in IoT

Today's IoT security solutions are tailored to the various IoT protocol levels. Constrained Application Protocol (CoAP) and secured Message Queue Telemetry Transport (MQTT), which utilize an encryption technique over the traffic data, are provided by the application layer of an IoT. The transport layer primarily uses TCP, UDP, DTLS, and SSL to provide security across the transport layer. The network layer is primarily used for transmission and secures all data using the IPv6, 6LoWPAN protocol. The IEEE 802.15.4e standard for the link layer features a built-in traffic management mechanism. There are several research studies where security measures for IoT have been examined, including. Most current methods for securing IoT rely on authentication-based techniques, key management methods, privacy protection methods, fault tolerance methods, and explicit mechanisms for thwarting certain attacks. In addition, it is impractical to carry out complex security activities using equipment with low processing power. The lack of attention to security standards is another significant security risk in IoT. A deeper examination of the current security solutions reveals that they focus more on enhancing privacy and less on maintaining data integrity, service availability, and other factors. The use of the encryption strategy presents an additional, more difficult difficulty. While encryption is necessary for greater security, it is not always done so effectively, and when dynamic attackers are present in the Internet of Things, its effectiveness is limited.

Due to many factors, blockchain technology is now seen as the IoT's long-term security solution. Blockchain creates information that is cryptographically coupled and bonded in the form of a block. A chain of blocks is made, with each block including transaction data in tree form, a date, and the Secure Hash Algorithm (SHA-512) hashed value of the preliminary data. Blockchain's

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

characteristics are stability, traceability, process integrity, security, and quicker processing. However, there are several stated blockchain limitations, including increased energy consumption, unchangeable data, reliance on self-maintenance, a higher cost, and the concept is still in its infancy. However, this restriction can be bypassed, provided enough attention is paid to the encryption method used in matching blocks. For this, the suggested way makes use of the asymmetric McEliece cryptosystem. The proposed system makes use of the ability of the McEliece encryption strategy to link the Blockchain due to the quicker mode of encryption and decryption process with a greatly decreased number of steps.

5. Methodology

Using Blockchain in the Internet of Things involves several cyclical procedures. The initial action is to do information sensing, and then the next is to measure the sensitive data inside the data. The final step involves conducting interpretation, which uses a range of analytics. The fourth step is establishing linkage with various resources to help with more complex analytical procedures. Several predictive processes further facilitate this. The last stage is to carry out additional optimization of the data that has been evaluated. Hence, it is always beneficial to integrate the potential feature of Blockchain with IoT. The *first* reason behind the proposed system to adopt Blockchain integrated with an IoT is to construct a trust value for IoT data successfully. All the transactions are recorded and arranged as a block of data, where there is more probation for incorporating security. The *second* reason for adopting Blockchain in the proposed system is that various security measures added to the system can be trustworthy and reliable. With more amendments and conditional logic, managing the data better and multiple possibilities of performing the analytical operation is feasible. Different customizations are further permissible in this aspect to make it more secure. The third justification for blockchain adoption is that it allows for more interoperability across various cloud platforms, leading to a more decentralized support system. Different applications can advance based on the justification stated above.

However, the ramifications of the Blockchain in the IoT ecosystem are not without problems. Scalability is the first problem that the suggested approach attempts to solve. The method that is being presented aims to develop the security measure utilizing Blockchain to provide consistent performance over massive amounts of data. The need for a decentralized security system employing Blockchain is the second obstacle. However, Blockchain is a centralized process. The suggested solution addresses the third issue, which is the dependence of early information on the attacker. A blockchain has to be developed to provide reduced computing complexity. It is crucial to incorporate the lightweight security operation for a cost-effective procedure to construct a future lightweight security design over a vast network of an IoT that primarily employs resource-constrained devices.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

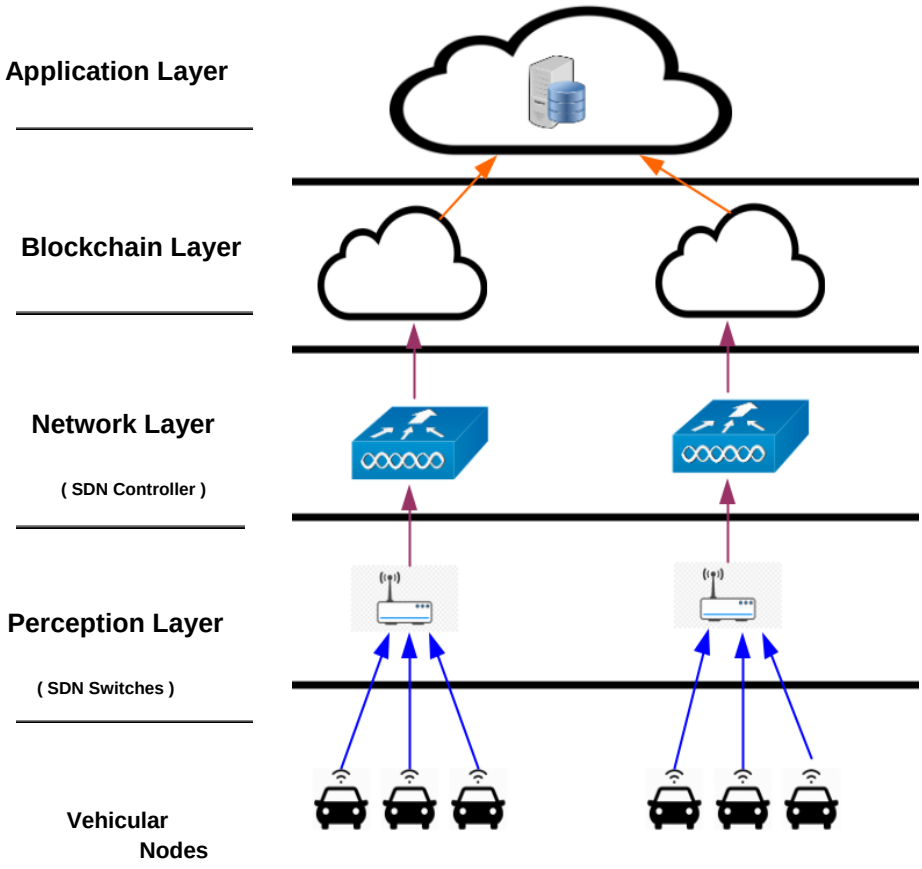

Figure Blockchain's position inside the IoT layers

The major duty of the network and application layers, where the blockchain application is located, is coordinating communication amongst communicating nodes in the Internet of Things situations. The cloud's central server will handle further processing of the acquired data. Additionally, the SDN switches are located at the perception layer, where the stream and request flows are evaluated. Based on this process, the information flow is passed to the controller, located at the network layer, and the controller then communicates with the cloud server to run an algorithm that determines whether the communication link is legitimate or malicious.

The system simulates the research in the manner described below:

- Factors that Are Included: The study creates a simulated Internet of Things ecosystem with a random distribution of nodes. The acquisition of incoming requests from the vehicular nodes is of greater importance. An experimental prototype is built to gather data, which are hypothetically assumed to be received via the perception layer, followed by the flow.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 04 | July - September 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Double Blind Peer Reviewed

DOI : 10.5281/zenodo.7016184

- Factors of exclusion: The suggested solution does not verify any reading or writing to the Blockchain. The full blockchain procedure is implemented in a distinctive manner that differs from previous experiments. In contrast to the current system, the input to the Blockchain is encoded data rather than raw data, which is further secured by the McEliese encryption method. The system does not consider any real-time SDN switch or controller settings to make the research more application-specific. In contrast, the study aims to create an all-encompassing model that can be applied in a real-world setting while modifying the hardware configuration factors.

When executing the ciphering process utilizing the asymmetric encryption approach, the McEliece cryptosystem is used to improve the randomization process. In post-quantum cryptography, employing this ciphering technique has a solid reputation. The fundamental building blocks of this method are linear codes, and the decoding operation is linked to its difficulties. The McEliece encryption system is used in the study because of its key characteristics, which set it apart from other encryption strategies. Since the suggested approach would be installed via an IoT network with several nodes, encryption must be minimal. An encryption method should run faster and use less memory to be lightweight. Compared to the theoretically robust RSA technique, the McEliece algorithm enables quicker ciphering and decoding. Although the legacy version of the McEliece algorithm does not provide a method to construct a signature, altering the traditional technique might successfully produce a signature.

6. Conclusion

The secure communication system in the Internet of Things, which is the upcoming advancement in networking and data processing, is covered in this suggested research. IoT provides wide communication between all devices due to numerous devices' availability, enabling applications to fulfill certain goals. The data distribution process in an IoT, which is still being developed, is nonetheless accompanied by many communication-based problems. Out of all the potential issues with IoT, security is the one that practically all IoT applications. Integrating security into the bigger connections by utilizing various communication protocols over a vast network of heterogeneous devices is difficult. Different security-based techniques have developed in the present to provide a beneficial security feature; these approaches may be broadly divided into cryptographic-based and non-cryptographic-based approaches. Although both have benefits and drawbacks, choosing a cryptographic-based method is more generally adopted. The study indicates that blockchain technology has made a substantial contribution in this respect to providing security for IoT.

7. Bibliography

1. Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI: https://doi.org/10.3991/ijim.v12i6.6776

DOI : 10.5281/zenodo.7016184

2. Alam T, Benaida M. The Role of Cloud-MANET Framework in the Internet of Things (IoT). International Journal of Online Engineering (iJOE). 2018;14(12):97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338
3. Alam, Tanweer, Arun Pratap Srivastava, Sandeep Gupta, and Raj Gaurang Tiwari. "Scanning the Node Using Modified Column Mobility Model." Computer Vision and Information Technology: Advances and Applications 455 (2010).
4. Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378- 3387
5. Alphand, Olivier, et al. "IoTChain: A blockchain security architecture for the Internet of Things." Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018.
6. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660. DOI: https://doi.org/10.1016/j.future.2013.01.010
7. Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990.
8. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
9. Reyna, Ana, et al. "On Blockchain and its integration with IoT. Challenges and opportunities." Future Generation Computer Systems (2018). DOI: https://doi.org/10.1016/j.future.2018.05.046
10. Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375. DOI: https://doi.org/10.1504/IJWGS.2018.095647