Block Chain Driven Intelligent Communication System for IoT

Dr Sheetalrani R Kawale[1], Dr.B.Srilatha[2], Dr.N.S.Gowri Ganesh[3], Mr. Girish M[4], Dillip Narayan Sahu[5], A. Seshaiah Sade[6]

[1]Assistant Professor, Department of Computer Science, Karnataka State Akkamahadevi Women's University, Vijayapura, Karnataka, India.

[2]Associate Professor, Department of Electronics and Communication Engineering, The Oxford College of Engineering, Bangalore, Karnataka, India.

[3]Associate Professor, Department of Artificial Intelligence & Data Science, Saveetha Engineering College, Chennai, Tamil Nadu, India.

[4]Assistant Professor, Department of Computer Science and Engineering, Gopalan College of Engineering and Management, Bangalore, Karnataka, India.

[5]Lecturer, Department of MCA, School of Computer Science, Gangadhar Meher University (GMU), Sambalpur, Odisha, India.

[6]Assistant. Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.

Abstract

The Internet of Things (IoT) is made up of a network of connections for a large number of physically heterogeneous devices, and it also has a lot of security vulnerabilities. IoT is a sophisticated method of connecting various computer and communication equipment using their own unique identities. IoT combines numerous technologies, including mobile devices, industrial machines, animals (or) humans, or other physical-digital entity to work together to accomplish the application's goal. This creates a collaborative environment. However, there are a number of security concerns, a few of which being Denial-of-service (DoS) attacks, Data Theft (or) Data Breaches, and Botnet attacks, in which several systems attempt to take control of the victim's system and steal the victim's private data. Various 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 has benefits and drawbacks, choosing a cryptographic-based method is more generally adopted. According to the report, blockchain technology has a crucial role to play in providing security for IoT.

Keywords: *IoT, Block chain, Security, Algorithm and Attacks.*

Number: 10.14704/nq.2022.20.9.NQ44323 **Neuro Quantology 2022; 20(9):2770-2780**

1. Introduction

IoT is a sophisticated method of connecting various computer and communication equipment using their own unique identities. IoT combines numerous technologies, including mobile devices, industrial machines, animals (or) humans, or other physical-digital entity to work together to accomplish the application's goal. This creates a collaborative environment. However, there are a number of security concerns, a few of which being Denial-of-service (DoS) attacks, Data Theft (or) Data Breaches, and Botnet attacks, in which several systems attempt to take control of the victim's system and steal the victim's private data. As they are utilised to expand network coverage, unsecure devices are the key security problem in edge computing and IoT frameworks. Additionally, certain IoT devices have the ability to switch across networks, posing a severe security risk.

The standard IoT network now takes into account the idea of zero trusts, which is a strategy for protecting the IT system and internet infrastructure. Additionally, it means that it presumes that all devices are permitted before allowing them to join the network or use its resources. Therefore, after getting past the firewall mechanism in an IoT, it is not difficult for the adversaries to operate side by side with the normal node. Given the variety of IoT devices and how sensitive and insecure the majority of them are, this might be a difficult scenario. Due to this phenomena, it is simpler for an adversary to use the gateway system in an IoT context. Currently, there are a number of taxonomies for layer-based IoT operations, including Three-layered, four-layered, and five-layered structures are all examples of architectural designs. The application layer, network layer, and perception layer make up the three-layered architecture, whereas the application layer, support layer, network layer, and perception layer make up the four-layered architecture. The business layer, application layer, processing layer, transport layer, and perception layer make up a five-layered architecture. Three layers are the most often used layer in the majority of IoT applications, according to a detailed examination of all the taxonomies. Because of this, the suggested system thinks of using a three-layered design.

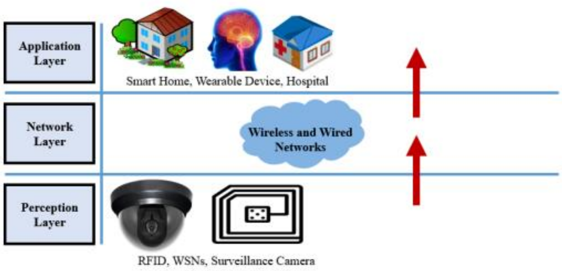

Figure.1. Three Layered Architecture of IoT

Figure.1. demonstrates the three-layer design, where the application layer is used to describe all IoT applications deployed and is often harmed by different intrusions, such as malicious programmes and cross-scripting assaults. But it depends on how sensitive the application is. All of the data acquired from the IoT device is sent via the network layer for transmission reasons. This layer contains the bulk of the communication protocol. Such strata include several intrusions, including man-in-the-middle attack, storage assault, exploit attack, and denial of service attack. The perception layer, which is essentially the bottom layer, is in charge of retrieving the unprocessed sensory input and sending it to the network layer. Typically, node capture attacks and replay eavesdropping attacks may exploit this layer. The suggested research employs the network layer as the host to dwell in the algorithmic operation since it focuses on creating a secure communication scheme in which blockchain plays a vital role. If the network layer operating as an intermediary bridge is highly protected, other levels (such as application and perception) may be automatically secured. The next security concern in an IoT setting is the network's lack of visibility. It is now rather challenging to provide generic Security for all of the devices due to the exponential growth in IoT device use. Accounting for every component linked to the network is required under traditional security procedures in information technology, but since there are so many IoT devices and mobility issues, this is not practical. It is still unclear how mobility and security are related. Figure.2. identifies the many types of IoT security problems.

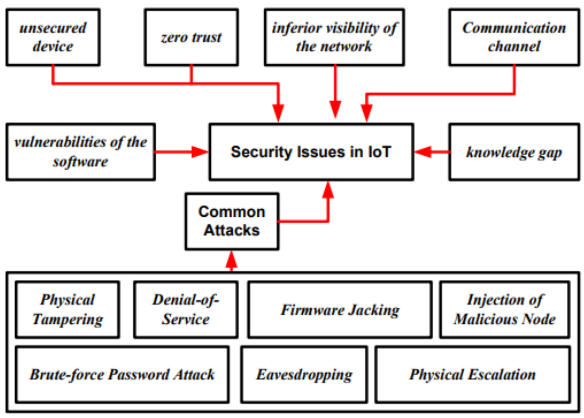

Figure.2. Taxonomy of Security issues in an IoT

The IoT's software vulnerabilities are connected to the following security issue. For instance, bargained IoT sensors connected to their user networks may easily launch cyberattacks on telecommunication service providers (TSP). Such cyber-attacks will have a significant impact on the telecommunication service providers (TSPs) and the powerful impacts they have on the target systems. Additionally, various overlapping software must be used due to the use of many protocols and IoT devices. Each piece of software has a distinct function as well as flaws that an enemy may exploit. Additionally, it will cause downtime because errors will be generated when the components interact or because more susceptible data will be produced. Even while upgrading the software may substantially help repel the attacker, doing it simultaneously is not practicable with such a large amount of software. Not only will it cause downtime, but it will also make the whole network susceptible. Another common practise in many businesses is the use of open-source software to access vital resources; unfortunately, such open-source software is extremely simple to infiltrate by an attacker. A knowledge gap among users is a crucial security risk in the IoT context. Users cannot be expected to be aware of all the many attack methods and environments that are susceptible. The consumers are less troubled by the security problems related to the use of IoT devices and are more concerned with the simplicity of utilising them. Another factor contributing to IoT security problems is the communication route. Attacks that originate from the communication channel used by an IoT component linked in a variety of ways to other IoT components are more likely to occur. Several protocols are now being utilised in an IoT communication system that has previously been identified as having a security flaw and is known to have an adverse effect on the whole networking infrastructure.

2. Literature Survey

On top of the named data networking stack, the conventional architecture of the content-centric Internet of Things (IC-IoT) provides intriguing solutions to a distinct manner of communication. The authors [11] examine the IC-possible IoT's design flaws and opine that the security issue is less often investigated. The authors discover that the differential privacy (DP) approach improves the extent of data privacy. The DP strategy, which is used by the randomised concept of Security in the research that is being given, provides a better level of data security and integrity without sacrificing the usefulness of consumer features. According to the research, the idea is suitable for IoT applications like smart grid. However, a thorough examination of the complexity of execution and energy consumption within a dynamic networking architecture is omitted, which raises serious questions about its robustness in key IoT applications where mobile payment protocol-based user privacy protection is really crucial [12]. The research of [13] envisions building an effective security schema for user/device authentication to secure mobile payment since IoT links a lot of smart devices that run different types of online payment schemes. The paper that is being presented provides a condensed design of security protocol for maintaining user privacy in IoT mobile payment systems. For the authentication utilising the mobile payment systems protocol, the solution method uses a re-signature-based mechanism independent of certificates. With user/device privacy preservation and anonymity maintenance procedures, the lightweight design optimises execution speed and achieves better Security. The performance validation includes a scenario for testing mobile payment systems in a controlled environment, demonstrating that the system can be applied to IoT devices with limited resources due to its potential for handling the overhead of millions of connected users. However, the scenario does not specify a thorough security analysis under various types of design flaws, leaving the payment gateway systems links vulnerable to an uncertain and unknown for. An IoT research issue was also addressed by the authors [15]. In order to describe a situation of communication with dynamicity where each IoT node may travel in any direction with a variety of speed characteristics regardless of growing time, the system representation uses random mobility modelling. However, this research also offers a security architecture that can defend the confidentiality of node data from both internal and external attackers. The technology also addresses issues with sensing coverage overlap. Additionally, it guarantees improved privacy protection by using an ID-based authentication schema to spot incursion from various hostile node actions throughout the communication scenario. It can be shown that the system does not guarantee that harmful node actions can be stopped using this technique and its assessment, although offering a mechanism to detect the malicious activities of nodes. The estimation of delay and latency factors and accuracy have not been highlighted by the system in its performance metric [16]. The authors [17] investigated how IoT may be used to enhance e-healthcare applications for smart and intelligent real-time diagnosis, which can be performed more quickly and accurately thanks to an intelligent and smart computing paradigm. A security framework aimed at the e-healthcare application area is introduced in the study. It makes an effort to protect electronic medical records so that user privacy and patient data anonymity are maintained. The experimental investigation using standard network characteristics provides reduced delays with a maximal reaction time inside a controlled simulated environment. However, the security architecture is solely appropriate for the healthcare industry. When it comes to location-aware privacy and mobile crowdsourcing, it isn't strong enough [18]. The most recent study does not address the mobile crowd sensing (MCS) for IoT privacy preservation technique. [19] have created the job selection process while taking into account the privacy concerns in MCS. The findings imply that MCS may effectively use resources while protecting privacy across wide regions [20]. The edge node threats where user data might be compromised have not been addressed by the author. As a result, [21] differential privacy strategy is proposed to limit data loss and minimise data uncertainty. IoT privacy, heterogeneity, and real-time implementation difficulties were the subject of a recent paper by [23]. Real-time and privacy-preserving architecture are provided for the smart city concept to address these problems. Under heterogeneity, the architecture may provide privacy in a real-time environment [24]. The main issue is the protection of data privacy for IoT statistical data. A partitioned histogram data protection technique based on wavelet transforms has been described in [25]. The technique delivers increased histogram accuracy and a significant increase in data accessibility [5]. The protection of IoT medical privacy and security is a crucial job. [26] makes a proposal for a biometric-based authentication method to ensure the privacy of medical IoT data. The data results indicate that the new protocol has better packet delivery ratio, throughput, latency, and routing overhead [8]. IoT heterogeneity and data security are significant issues that need to be addressed. A Snap4City architecture for universal data security has been given by [27], and the results provide a superior option for an IoT-based smart city [9]. To address the many security and privacy risks posed by human to machine and machine to human communication, trust management in IoT and cloud computing is required. As a result, [28] introduces a context-aware trust management approach that assesses user credibility in a Fog-based IoT. (FIoT). User trust management is made effective and trustworthy by the model [4]. IoT's fast and widespread implementation creates problems with message delivery security and authentication. In order to improve privacy against attack, [29] have developed a reliable message authentication technique based on signature-based identification. According to the results, the authentication system provides a high degree of privacy [3].

The prevalence of privacy attacks on mobile IoT services is a result of the systems' rapid development. As a result, the attacker may hack into the user's computer and steal their data. To improve accuracy and efficiency in security management for Mobile IoT systems [6], a query-based intelligent security system is provided in [30]. A deep convolution neural network (DCNN) is presented for a privacy-based yoga gesture detection method for elderly individuals in [4], which addresses the privacy concerns in the current IoT applications for yoga instruction. The method results in enhanced gesture recognition accuracy [7]. Applications that are linked to the Internet of Things (IoT), such as smart homes, medical devices, and industrial machinery, are vulnerable to cyberattacks. As a result, [Liu et al., 2018] have presented a privacy-preserving approach to satisfy the privacy requirements for IoT-connected devices. The plan's results provide higher privacy protection while using less network power [8]. The current privacy-preserving query methods increase communication costs. As a result, the author [20] has provided a homomorphic encryption technique that aids in maintaining data privacy and security. This encryption approach results in minimal computing cost and little transmission overhead while protecting data privacy [9]. In a paper by [12], the author suggested a ciphertext policy (CP) attribute-based encryption (CPAE) technique to address the overhead and user privacy concerns of the Internet of Things. The mechanism's security analysis performs better in terms of offering a safe and effective solution to security problems, as well as less overhead [8]. The privacy problem relating to sensing data is highlighted [19] and a game theory-based, customised privacy preservation solution is suggested. The results of this protection approach aid in greater privacy preservation for sensing IoT data [1]. [17] has developed a hierarchical location tree architecture to solve the IoT location privacy problem. The results of this methodology improve locational information for IoT devices in terms of security, applicability, and privacy [18]. Due to privacy concerns with physical data sharing in the industrial IoT, [5] has suggested a privacy-preserving physical data sharing method [3]. In order to safeguard communications, the traditional Advanced Encryption Standard (AES) algorithm was improved in the work of [1]. The encryption technique lowers the encryption power while simultaneously resisting various security assaults [2]. The problems with information-centric IoT have not been solved by the system. Utilizing the attribute-based encryption (ABE) approach made up of the Cipher text policy first described in [3], sufficient data security may be attained. Performance is increased, and calculation overhead is reduced, thanks to the encryption technique [4]. The IoT devices with limited resources suffer from a variety of problems, including poor processing power, excessive latency, low bandwidth, etc. In [5], a lightweight encryption method for the Internet of Things that is based on cellular automata addresses these problems. The method may decrease runtime and stop data theft [6]. In earlier studies, the complexity parameter has not been addressed. A less complicated and quicker block encryption technique for the IoT has been described in the work of [7]. Block encryption mechanisms need fewer calculations and provide more security, supporting low-power Internet of Things (IoT) devices [8]. A multiparty authentication-based encryption technique for narrowband Internet of Things terminals has been presented through [9]'s work. The data privacy and effective support for the 5G network are provided by the encryption method, which is based on certificates policy [8]. In [9], the chaotic encryption method is presented for key-controlled neural networks in the Internet of Things (IoT) for intelligent data transfer. When compared to the current approach, cryptanalysis provides better information entropy [9]. Existing studies do not cover the benchmarking of IoT apps using an encryption technique. IoT applications' cloud storage is benchmarking of symmetric encryption technique is provided in [4]. The results of the dynamic symmetric encryption technique point to a trade-off between security and cloud performance in the current system [10]. For IoT applications, the throughput and error performance are not examined. [20] proposed a simple encryption method for IoT, and performance in the Additive White Gaussian Noise (AWGN) channel is evaluated for error and throughput with and without coding. The system produces lower mistakes, improved performance, and higher security without impacting processing time [11]. Combining probabilistic and lightweight encryption techniques is not covered by the encryption mechanism. The safe surveillance model for the smart healthcare IoT application is provided in [14], which makes use of both probabilistic and lightweight encryption techniques. The plan promises greater patient data security in IoT devices together with decreased storage, increased bandwidth, and lower transmission costs [15]. Prior studies for safeguarding the IoT environment did not include the hybrid lightweight proxy encryption. A hybrid re-encryption approach is provided in [16], and it reduces encryption and decryption [3] while being effective. However, the IoT-based healthcare system does not support hierarchical attribute-based encryption (HAE). [17] provided details of a Cipher text policy using the HEA algorithm to prevent key leakage from healthcare data [4]. The research did not include the IoT smart grid's encryption system. For an IoT-based smart grid, a compact and safe sign encryption system is proposed in [18]. The findings imply that the security system provides greater security than current security plans while using less money and communication resources [9].

3. Security Approaches in an IoT

The IoT security solutions available today are very tailored to the various IoT protocol levels (Figure.3). Constrained Application Protocol

(CoAP) and secured Message Queue Telemetry Transport (MQTT), which utilise an encryption technique over the traffic data, are provided by the application layer of an IoT. To provide security across the transport layer, the transport layer primarily uses TCP, UDP, DTLS, and SSL. The network layer is primarily used for transmission and secures all data using the IPv6, 6LoWPAN protocol. The IEEE 802.15.4e standard, which is used for the link-layer, features a built-in traffic management system.

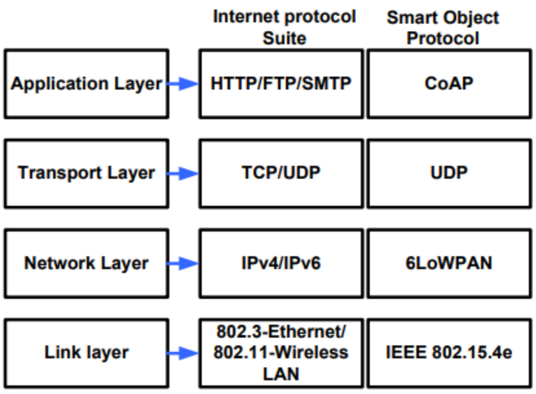

Figure.3. Protocol suite for Smart Objects in IoT

There are several studies that examine security measures for IoT, including [1-8]. Existing methods for protecting the Internet of Things mostly rely on authentication-based methods [5], key management methods [1], privacy protection methods [2], fault tolerance methods [3], and explicit mechanisms for thwarting certain attacks [4-6]. In addition, it is impractical to carry out complex security activities using equipment with inferior processing power. The lack of attention on security standards is another significant security risk in IoT. A deeper examination of the current security solutions reveals that they are more focused 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 using 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.

For a number of reasons, blockchain technology is regarded as the long-term security solution in an IoT. Blockchain creates information that is cryptographically coupled and bonded in the form of a block. A chain of blocks is created, with each block including transaction data in tree form, a date, and the Secure Hash Algorithm (SHA-512) hashed value of the preliminary data (or block) [7]. Stability, traceability, process integrity, security, and quicker processing are attributes of blockchain [5]. However, there are a number of stated blockchain limitations, including increased energy consumption, unchangeable data, a reliance on self-maintenance, higher cost, and the idea is still in its infancy. This restriction may be bypassed, however, provided enough attention is paid to the encryption method used in matching blocks. For this, the suggested solution makes use of the asymmetric McEliece cryptosystem [8]. The suggested system makes advantage of the ability of the McEliece encryption strategy to connect the blockchain due to the quicker mode of encryption and decryption process with a greatly decreased number of steps.

4. Blockchain in IoT

Blockchain technology was created with the purpose of encrypting data transfers between two users or parties in the presence of a distributed ledger. Conventionally, it is understood that IoT has a centralised design for greater management, with the cloud system handling data propagation through several heterogeneous devices. Various analytics are also available to comprehend and get some important information from this data flow. Adopting such a centralised controlling system would limit operation since there are so many devices linked through the IoT network. Scalability must, therefore, obviously decrease. This puts the system in a variety of susceptible situations and causes a security breach. As a result, the clever mechanism of the blockchain network enables this IoT gadget to function in a very safe way. Additionally, it creates different agreements that are applied as needed. Applying blockchain to IoT devices provides a number of advantages that help with increased automation, cost-effectiveness, and scalability. Additionally, it helps prevent accidental overriding of certain parameters. In a fully decentralised fashion, using an encrypted communication channel, all the data that the IoT device collects is sent to the many destination nodes. IOTA is seen in this context as a common distributed ledger designed for implementing and storing transactions across various machines connected to the Internet of Things. A non-profit company called IOTA standardises the agreement that will be used when using blockchain technology in the Internet of Things. Bosch, Fujitsu, Den Norske Bank, and Volkswagen are just a few of the companies that have worked with IOTA.

Figure.4. exemplifies how the blockchain works, demonstrating how user A is motivated to give money to user B in Step 1. As shown in Step-2 operation, the second procedure involves the system creating an initial blockchain online. This block represents a transaction. As shown in Step 3 of operation, the newly produced block is subsequently broadcast to all network participants. The approval of this transaction must be performed by all the various systems involved, and then it must be validated in Step 4 operation. As seen in Step 5, this block is added to the chain to provide a visible, irreversible, and permanent record for the transaction. The operation's last step is when user-B accepts user-payment A's in operation-step-6.

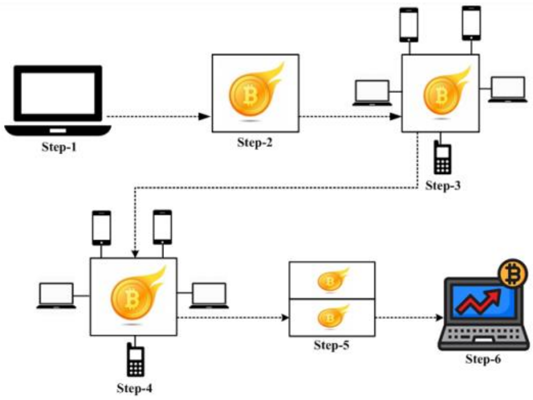

Figure.4. Operation involved in Blockchain Technology

It's crucial to utilise a simple use case to describe the function in order to comprehend how blockchain is used in the Internet of Things. Take an Android smartphone as an example, which is widely used by consumers all over the globe because to the large selection of applications it supports. It is also well known that a few years ago, the cellphone did not have these remarkable capabilities, however now, it is capable of greater levels of communication-related operation. The only reason smartphones have the potential to have more capabilities than telephones is because they can bridge communication with the internet. This is akin to the Internet of Things (IoT) idea, which states that linked objects get naturally smarter. A bigger network known as the internet connects three main categories of objects, and these objects are as follows:

Collector: These entities are in charge of gathering the specified assortment of data. Typically, they are sensors of different kinds and capacities. There is greater flexibility in the decision-making process because to the discrete information that is gathered from the environment. The information is provided to the recipient once it has been gathered.

Receiver: These are the device groups, and from the standpoint of deployment, there are often several of them. Three-dimensional printers, smart TVs, smart household appliances, wearable tech, etc. are examples of hybrid technology—groups of items that are capable of acting as both collectors and receivers. An example of one of these gadgets would be a sensor that can gather data about the outside world. The sensors may cause certain gear to operate in a specific way depending on the situation.

Information is an IoT's primary asset, thus it is clear that security measures must constantly be taken to prevent it from getting into the wrong hands. An IoT system that is properly maintained and managed can only benefit from this data in terms of efficiency. Further data security is required, and this is where blockchain technology comes into play.

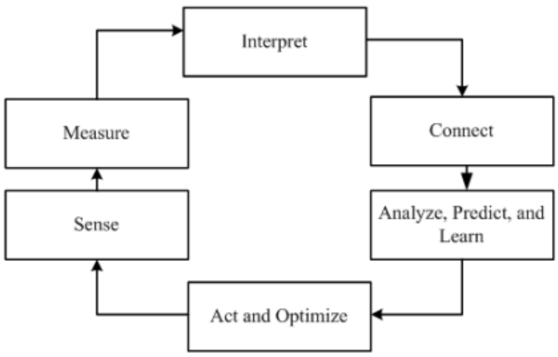

Figure.5. Applying blockchain in IoT

Figure.4 illustrates the use of blockchain in the Internet of Things, where various actions are shown cyclically. 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 makes use of a variety of analytics. The fourth step is to establish linkage with various resources to help with more complex analytical procedures. This is further facilitated by several predictive processes. The last stage is to carry out further optimization of the data that has been evaluated. Therefore, it is always advantageous to combine the potential benefits of blockchain with IoT. The first justification for the suggested system's use of Blockchain combined with an IoT is to effectively build a trust value for IoT data. As a block of data with greater room for adding security, all transactions are logged and organised. The addition of numerous security measures to the system can be trusted and dependable, which is the second justification for using blockchain in the proposed system. It is possible to organise the data more effectively and to do the analytical operation in a variety of ways with more amendment and conditional logic. Additional changes are also allowed in this area to increase security. The third justification for blockchain adoption is that it allows for more interoperability across various cloud platforms, which may lead to a more decentralised support system. Different applications may advance based on the justification stated above. The ramifications of the blockchain in the IoT ecosystem, however, 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 utilising blockchain to provide consistent performance across massive amounts of data. The need for a decentralised security system employing blockchain is the second obstacle, however blockchain is a centralised process. The suggested solution addresses the third issue, which is the dependence of early information on the attacker. A blockchain has to be developed in order to provide reduced computing complexity. The incorporation of the lightweight security operation for cost-effective operation toward the development of a potential lightweight security design over a vast network of an IoT that primarily uses resource-constrained devices is therefore crucial. The blockchain usage is specific to a particular layer when it comes to positioning it in IoT layers. Figur.6. showcases three IoT viz layers. network layer, application layer, and perception layer. The whole stream of requests is received from various nodes in the perception layer and sent to the network layer, where the decentralised blockchain operating system is located in the decentralised cloud. The decentralised cloud also interacts with the cloud in relation to a distinct application for application-layer management. The major duty of the network and application layers, where the blockchain application is located, is to coordinate communication amongst communicating nodes in Internet of Things situations. Further processing of the acquired data will be handled by the cloud's central server. 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 over the controller, which is 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. A protected IoT with SDN-based communication system secured by blockchain operation is the end result of this communication.

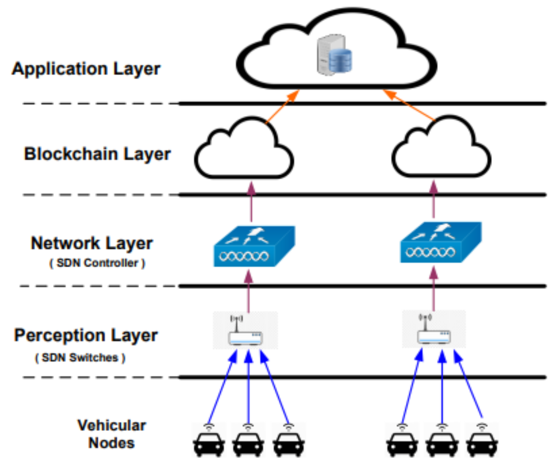

Figure.6. Position of the blockchain in IoT layers

5. Results and Discussion

The suggested approach takes into account the real-world IoT environment, as seen in Figure 7. There are three levels based on this use case. The server or software agent, which is on the uppermost layer, is where many sophisticated programmes connected to an IoT's data analysis are taken into account. The next intermediate layer, where the IoT is merged with SDN, is where the highest levels communicate. Various networking devices, such as routers, switches, and gateways, are included in the IoT block, while the controller and switch are the core components of the SDN block. The bottom layer is made up of multiple communication domains, each of which has a distinct communication protocol from the others. In order to determine how to proceed with processing the request, the SDN switches communicate with the SDN controller after receiving it from the nodes located inside this communication domain.

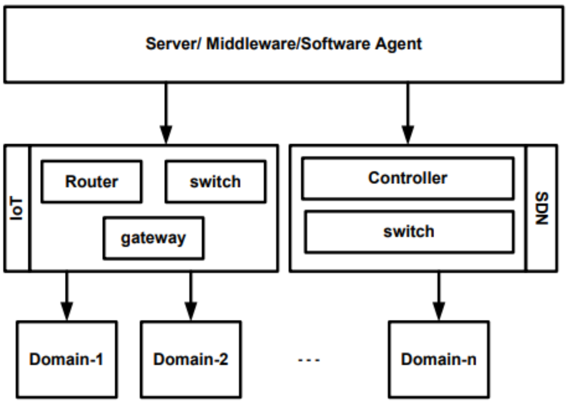

Figure.7. Use case considered in the assessment

The suggested system does two types of the preliminary evaluation to demonstrate the vulnerability of the unknown adversary through the malicious flow. The SDN controller may allocate stream entries of static origin to determine the capacity of the stream connected to the SDN switch by performing the first evaluation through the northbound protocol. In this situation, there is no other way to get rid of the stream entries in static form other than by hand. Two IoT nodes are taken into consideration for this scenario, and they speak to one another through a model Switch. This test witness is tied to a particular SDN switch as a consequence of the communication collapsing with a much greater number of stream entries. A fixed number of data packets are introduced to the SDN switch in the next phase of the first test to map with the malicious stream of the data packets. According to the research, two IoT nodes might trick an SDN controller into sending data packets to one another. All data packets are given unique IoT node identifiers and are then requested to have a specific entry in a stream allocated by the SDN communication protocol system.

MATLAB is used to simulate the proposed system in its entirety. Implementing the use case scenario comes first, and then executing communication in the adversarial data flow comes second. The investigation is conducted over a matrix that stores all the data flow information and non-current beacons for a predetermined d period of time in order to perform simulation of the proposed SDN block operation. The speed of the request for switch Si and its corresponding statistical data are emphasised in figure 8 to carry out the first stage of monitoring.

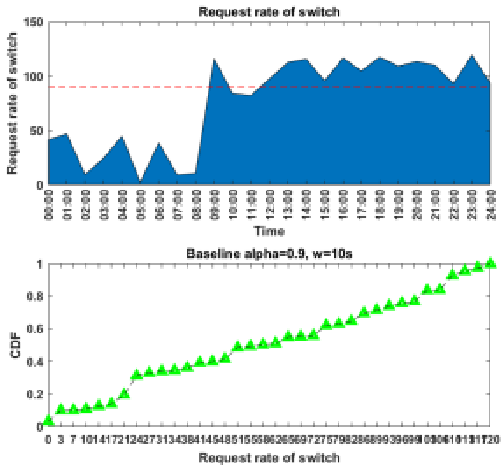

Figure.8. Speed of Request in Switch

Similar to this, the suggested research examines the SDN switch's equivalence score, as illustrated in figure 9. According to the graphical results, the greatest value of the equivalence characteristic I and its statistical score is discovered to be about 35 data packets for each data flow at a unit of duration slot. Comparatively, the lowest value for I is 8 data packets or less for a unit data flow within a unit duration slot. The numerical result of I D is discovered to be 8.1 in Figure.9. It should be noticed that both of the analyses in figure 8. and figure. has taken into account a comparable testing environment of the amount and percentage of lawful data h.

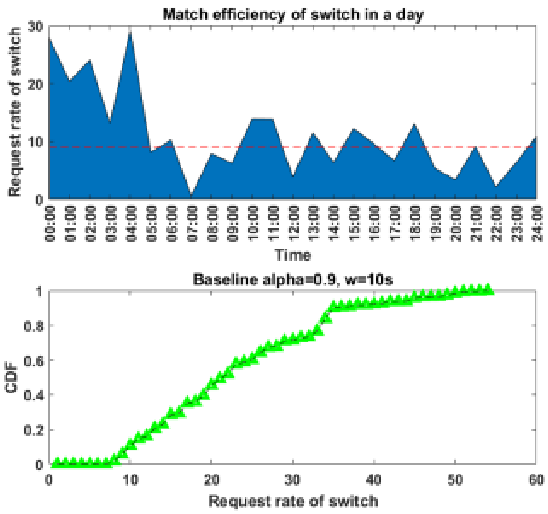

Figure.9. Equivalency Score performance of Switch

6. Conclusion

The secure communication system in the Internet of Things, which is the next advancement in networking and data processing, is covered in this study proposal. IoT provides wide communication between all of the devices due to the availability of many devices, enabling applications to fulfil certain goals. The data distribution process in an IoT, which is still being developed, is nonetheless accompanied by a number of communication-based problems. Out of all the potential issues with IoT, security is the one that practically all IoT applications are most concerned about. It is rather difficult to successfully integrate security into the bigger set of connections utilising various communication protocols across a vast network of heterogeneous devices. Various 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 has benefits and drawbacks, choosing a cryptographic-based method is more generally adopted. The research indicates that blockchain technology has made a substantial contribution in this respect to providing security for IoT.

References

1. J. Pacheco, D. Ibarra, A. Vijay and S. Hariri, "IoT Security Framework for Smart Water System", *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1285-1292, 2017.
2. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, Feb. 2014.
3. S. Singh and N. Singh, "Blockchain: Future of financial and cyber security", *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 463-467, 2016.
4. Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar and Eui-nam Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved", pp. 414-419, 2014
5. GAURAV. H. TANDON, *Intelligent Transportation System*, Dec 2015, [online] Available: https://www.slideshare.net/gauravhtandon1/intelligent-transportation-system-56391402.
6. P. Lade, R. Ghosh and S. Srinivasan, "Manufacturing analytics and industrial Internet of Things", *IEEE Intell. Syst.*, vol. 32, no. 3, pp. 74-79, May/Jun. 2017.
7. A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home", *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, pp. 618-623, Mar. 2017.
8. Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things", *Peer Peer Netw. Appl.*, vol. 10, no. 4, pp. 983-994, Jul. 2017, [online] Available: https://doi.org/10.1007/s12083-016-0456-1.
9. M. Conoscenti, A. Vetrò and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review", *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, pp. 1-6, Nov./Dec. 2016.
10. A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and

opportunities", *Future Gener. Comput. Syst.*, vol. 88, pp. 173-190, Nov. 2018.
11. M. Banerjee, J. Lee and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper", *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149-160, 2018.
12. T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things", *IEEE Access*, vol. 6, pp. 32979-33001, 2018.
13. M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey", *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676-1717, 2nd Quart. 2019, [online] Available: https://doi.org/10.1109/COMST.2018.2886932.
14. A. Panarello, N. Tapas, G. Merlino, F. Longo and A. Puliafito, "Blockchain and IoT integration: A systematic survey", *Sensors*, vol. 18, no. 8, 2018, [online] Available: http://www.mdpi.com/1424-8220/18/8/2575.
15. K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment", *ICT Exp.*, vol. 5, no. 1, pp. 1-7, 2019.
16. O. Khutsoane, B. Isong and A. M. Abu-Mahfouz, "IoT devices and applications based on LoRa/LoRaWAN", *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, pp. 6107-6112, Oct./Nov. 2017.
17. X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao and Z. Han, "Ambient backscatter assisted wireless powered communications", *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 170-177, Apr. 2018.
18. J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges", *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26-33, Jan. 2017.
19. R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things", *Comput. Netw.*, vol. 57, no. 10, pp. 2266-2279, Jul. 2013.
20. J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou and Y. Zhang, "Multitier fog computing with large-scale IoT data analytics for smart cities", *IEEE Internet Things J.*, vol. 5, no. 2, pp. 677-686, Apr. 2018.
21. Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey", *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352-375, 2018
22. X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems", *Future Gener. Comput. Syst.*, [online] Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318332.
23. M. Conti, E. S. Kumar, C. Lal and S. Ruj, "A survey on security and privacy issues of bitcoin", *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416-3452, 4th Quart. 2018.
24. Y. Gilad, R. Hemo, S. Micali, G. Vlachos and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies", *Proc. ACM 26th Symp. Oper. Syst. Principles*, pp. 51-68, 2017.
25. A. Dorri et al., "Towards an optimized blockchain for iot", *Proc. of the Second International Conference on Internet-of-Things Design and Implementation*, pp. 173-178, 2017.
26. P. Danzi et al., "Distributed proportional-fairness control in microgrids via blockchain smart contracts", *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2017.
27. G. Eibl and D. Engel, "Influence of data granularity on smart meter privacy", *IEEE Trans. on Smart Grid*, vol. 6, no. 2, pp. 930-939, 2015.
28. T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains", *Proc. ACM Int. Conf. Manag. Data (SIGMOD)*, pp. 1085-1100, 2017, [online] Available: http://doi.acm.org/10.1145/3035918.3064033
29. F. Idelberger, G. Governatori, R. Riveret and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems", *Proc. Int. Symp. Rules Rule Markup Lang. Semantic Web (RuleML)*, pp. 167-183, 2016.
30. R. Koulu, "Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement", *SCRIPTed*, vol. 13, no. 1, pp. 40, 2016