Blockchain-based IoT architecture for energy-efficient smart networks

Manikandan Asaithambi

Data Engineer, Software Development, Bhava Data Corp Sp.Z o.o, Gdańsk, Poland

ABSTRACT

With the rapid development of the IoT (Internet-of-Things), additional smart gadgets may be associated with the Internet, significantly enhancing data transfer and communication. For the past few years, IoT technology continues to not only gain popularity and importance but also witnesses the true realization of everything being smart. Software-Defined Networking (SDN) is known as a new model that separates the control plane and the data plane and is anticipated as a favorable solution for implementing Blockchain, to offer the scalability and adaptability required for IoT. Blockchain and SDN are two top innovations utilized to create secure network architectures and provide trustworthy data transmission. This work provides an optimized Blockchain-based SD IoT architecture for smart networks that is safe and energy-efficient. This work, is concentrated on blockchain-based SDN and creates an SDN-Blockchain Classifier. This IDS-based security tool provides a trust-based classifier by handling and reducing harmful traffic through traffic fusion and aggregation. Finally, it is concluded by evaluating the proposed framework SDN-Blockchain Classifier performance against MAC flooding attack in a simulation setting and demonstrating that it can attain optimized average throughput, response time, packet loss of crossing domain path, energy efficiency, end-to-end delay, file transfer operation, energy consumption, and CPU utilization compared to the baselines taken into consideration, thereby achieving efficacy and also security in the proposed smart network.

Keywords: *Machine Learning, Artificial Intelligence, Internet-of-Things, Blockchain, Intrusion Detection, Intrusion Prevention.*

1. INTRODUCTION

1.1 Internet of Things (IoT)

The Internet of Things (IoT) is a network of intelligent physical objects that connects to the outside world to exchange information by Salim et al. (2020). There have been efficient methods suggested for managing the analysis of complicated data, improving security and privacy, and reducing power consumption as a result of the IoT networks' rapid expansion over the past several years shown by Tahsien et al. (2020). It is an emerging new network technology with the objective and opportunity to transform human life by enhancing the technology of the Internet. Therefore, its applications in diverse paces of life are seen to be increasing significantly described by Ahanger & Aljumah (2020). IoT is a new paradigm that enables a large number of smart things to be linked with the Internet. The objects like actuators and sensors devise are capable to manage and forward the data to a system without human contribution.

IoT is anticipated to be the greatest impact after the advent of the Internet. The world of digital gadgets is expanding rapidly, and by 2010, there will be more devices on the planet than people. Similarly, projections indicate that by 2020, there will be around 50 billion gadgets online. The number of devices linked to the Internet has beyond all predictions because of advancements in technologies like low power and resource-constrained devices, which have extended the Internet's scope to the farthest reaches of the globe. Figure 1 shows the IoT platform. Moreover, the IoT ecosystem core may focus on three key technical domains: connected devices or perception, connectivity or network (also called transport), and applications or services.

Fig-1 Internet of Things platform

1.2 IoT- security

The increasing number of connected devices in the era of the Internet of Things (IoT) has also increased the number of intrusions. Intrusion Detection System (IDS) is a secondary intelligent system to monitor, detect, and alerts about malicious activities; an Intrusion Prevention System (IPS) is an extension of a detection system that triggers relevant action when an attack is suspected in a futuristic aspect. Both IDS and IPS systems are significant and useful for developing a security model. Several studies exist to review the detection and prevention models; however, the coherence in the opportunistic advancements in the models is missing. Besides, the existing models also have some limitations, which need to be surveyed to develop new security models. Jayalaxmi et al. (2022) describe the survey as the first one to present a study of risk factor analysis using a mapping technique, and provide a proposal for a hybrid framework for an efficient security model for intrusion detection and/or prevention. More specifically, emphasize Machine Learning (ML) and Deep Learning (DL) techniques for intrusion detection-prevention systems and provide a comparative analysis focusing on the feasibility, compatibility, challenges, and real-time issues.
With the increasing number of devices and sophistication of attack tools: hacking and security breaches have grown unlimited. IoT establishes a heterogeneous pervasive network of smart devices. Some of the complex IoT devices relate to a hostile interface, developed on uncontrolled platforms, and encounter vulnerabilities to individual systems available in the integrated network Gomathi et al. (2018). Lack of interoperability and accessibility in the vast heterogeneous landscape results in poor monitoring of the security mechanism in IoT networks.

The remaining paper can be organized as follows:
Section 2, discussed some of the recently published related states of arts.
Section 3 describes the methodology and the model constructions.
Section 4 discusses the experimental performances of the proposed work and some other related works.
Section 5 presents the conclusion along with the future scope of work.

2. LITERATURE REVIEW

2.1 HIOT

The Internet of Things (IoT) is playing a vital role in the rapid automation of the healthcare sector. The branch of IoT dedicated to medical science is at times termed as Healthcare Internet of Things (H-IoT). The key elements of all H-IoT applications are data gathering and processing. Due to the large amount of data involved in healthcare, and the enormous value that accurate predictions hold, the integration of machine learning (ML) algorithms into H-IoT is imperative. Bharadwaj et al. (2021) aim to serve both as a compilation as well as a review of the various state-of-the-art applications of ML algorithms currently being integrated with H-IoT.

2.2 Architecture of H-IOT

An H-IoT system comprises an end-to-end network typically consisting of three major layers of operation. The data collection layer is responsible for the collection of medical data from various sensor devices attached to the patient/test subject that needs to be monitored/ examined. The data storage layer is responsible for the storage of big data collected from various sensors and transmitted through the Internet. The data processing layer analyzes the data

stored in servers to generate the required response through the application of computing algorithms. The implementation of these layers is enabled using the following technologies as shown in Figure 2.

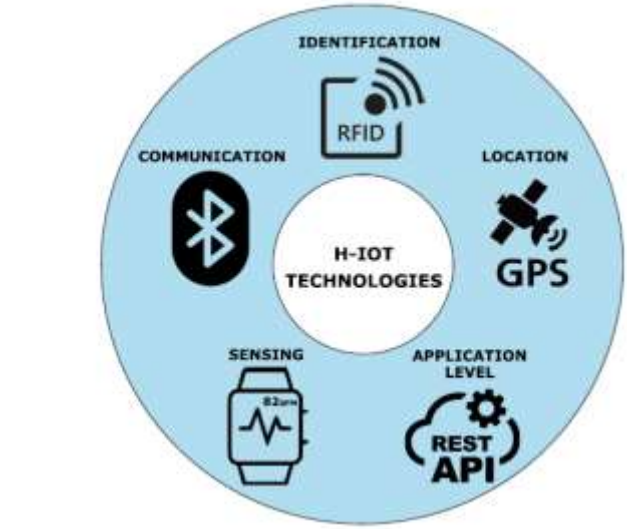

Fig-2 H-IoT Technologies

The nodes in the network of an H-IoT framework to access information and communicate with each other securely, each node must be identified uniquely through technologies such as a unique identifier (UID). Both short and long-distance communications between the nodes in the H-IoT network require pathways. Global positioning system (GPS) enables the various nodes to accurately track each other's geographical locations which is extremely important for certain use cases of H-IoT. Various other location tracking systems may also be required to compensate for instances of poor GPS connectivity.

The data analyzed to draw inferences in an H-IoT system is generated by sensors. A large variety of sensors are available for the acquisition of such data, for instance, gyroscopes for measuring angular velocity, and electrocardiogram (ECG) sensors to measure electrical activity in the heart shown by Almotiri et al. (2016). Application-level architectures such as service-oriented architecture (SOA) or representational state transfer (REST) allow the various devices in the system to perform independently of each other

2.3 IoMT

Internet of medical things (IoMT) is getting researcher's attention due to its wide applicability in healthcare. Smart healthcare sensors and IoT-enabled medical devices to exchange data and collaborate with other smart devices without human interaction to securely transmit collected sensitive healthcare data to the server nodes. Alongside data communications, security, and privacy is also quite challenging to securely aggregate and transmit healthcare data to Fog and cloud servers.

In IoMT, data aggregation is a requisite technique to abolish redundant health parameters of patient data and diminish transmission costs. In data aggregation, numerous medical sensing devices collect patient data. Edge devices aggregate data from the medical sensor nodes and then send the aggregated data to the cloud server described in Engineer et al. (2019). The collection of data can be categorized into two types of devices Homogeneous and Hybrid devices. Both types of devices separately transmit data to the Fog node. Moreover, mobile devices are introduced as a collector node for efficient data aggregation by Tang et al. (2019). It is a challenging task in remote health monitoring systems because nodes are mostly located in hostile surroundings with insecure transmission medium. There is a need for secure data aggregation while preserving the data integrity and privacy of the patient Guo et al. (2021). In IoT, security and privacy for the sensitive data of patients is essential and quite challenging in IoMT. In this context, cyber-physical systems (CPS) are also used in social services, especially in healthcare-based applications. It enhances the quality of medical care and extensively reduces healthcare cost.

Fog-based system escorts the cloud computing model to the edge of the network thus enabling low latency, interoperability, and local analysis as a few basic attributes of Fog computing. The term ``FoG server'' was invented by Cisco Okay & Ozdemir (2018). Smart healthcare architecture allows monitoring devices to interact with the patient and remotely share data with the server. It reduces the overhead at the cloud server and also balances the load

among multiple local fog nodes. It also provides local processing and storage to attain better quality and response as compared with the cloud. Integration of fog and IoT provide more reliable, secure, and efficient services for users. The fog node locally processes data and predict intelligent decisions in an emergency to efficiently handle the critical situation of patient health.

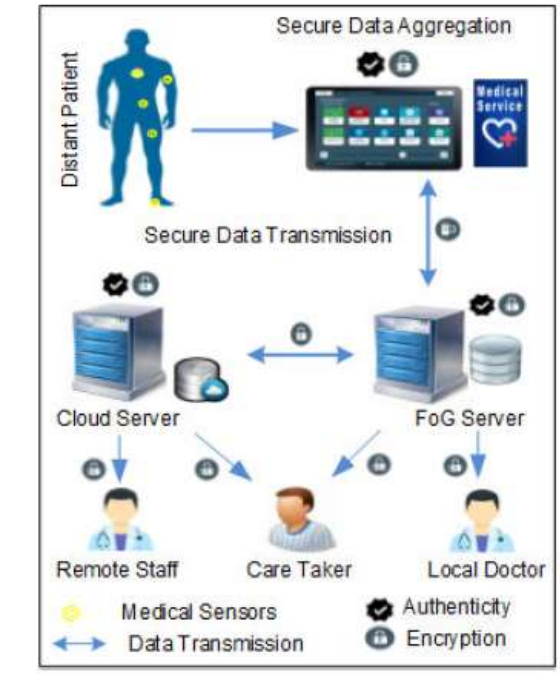

Fig-3 Secure data transmission and storage at FoG and cloud

In smart healthcare systems, fog nodes with smart collector nodes at the edge of the network can be applicable because healthcare systems have attributes of low power, energy, and bandwidth. Fog computing and cloud computing can be an appropriate combination to overcome challenges in IoT and healthcare systems Puliafito et al.(2019). Fog computing in healthcare focuses on secure data collection and data aggregation for local and remote patients. Security and privacy are essential to ensure the confidentiality and integrity of data while transmitting sensitive medical data to the cloud server as shown in Figure 3.

Patient-centric healthcare system helps in reducing clinic-centric treatment by remote monitoring by local/remote medical staff. Generally, the patient-centric healthcare system consists of a multi-layer structure by Farahani et al. (2018). In this context, fog computing faces different challenges like reducing latency, privacy, energy efficiency, bandwidth, scalability, and dependability. It is a challenging task to efficiently aggregate data from healthcare devices and locally process data in the fog then transmitted it towards the cloud server. Rahul *et al.(2020)* introduce privacy preserved healthcare framework for electronic medical records (EMRs) using Fog. EMR considers privacy as a main challenging issue and focuses on preserving privacy with fast response time in the Fog-assisted healthcare scenario. Fog-assisted smart cities, smart vehicles and smart grids are also considered that achieve secure, efficient, and reliable data collection with low computational cost and compression ratio.

2.4 Machine Learning

Machine learning techniques are majorly categorized as supervised learning, unsupervised learning, and reinforcement learning. Training with fully class-labeled data, and establishing the relation between the input and target units are the properties of supervised algorithms. Classification and regression are the two major categories of supervised learning. Unsupervised learning techniques find the hidden structure in the unlabelled data without training. Dimensionality reduction described by Su et al. (2018), density estimation, and clustering are the three major techniques used to make relevant groups for comparison and compression with unique identification. Arulkumaran et al. (2017) explain two major reinforcement methods policy search and value function approximation.

The most popular machine learning algorithms which achieve good results in detecting the specious activities of IDS are decision trees, random forests, SVM, and neural networks. The accuracy of the models and the efficiency of the

algorithms depends on the application and the type of attack detected. A recent work experiments with interception, injection, and denial of service attacks; IPS is found to be immune to these attacks in Alves et al. (2018). It uses K-Means techniques after removing the outliers and integrates Local Outlier Factor (LOF) algorithm to evaluate a score reflecting the abnormality of the observations. Tree Automata based on Automatic Approximations for the Analysis of Security Protocols, abbreviated by Werth and Morris (2019) propose a layer-based prevention technique that stimulates a physical system based on the payloads of the packets. It uses three layers: layer zero for physical devices, layer one for the ladder logic program, and layer two to activate the internal states of the ladder logic program.

Li and lui (2019) introduce an ML technique using SVM in snort IDS to minimize the error rate and improve the performance. The combination of this model with a firewall gains high defensive ability. Nikhil et al. (2020) propose an integrated technique for prediction and prevention in the agriculture sector with smart connected devices. The experiment was conducted on real-time agriculture data using sensor devices and processed using machine learning and deep learning techniques.

2.5 Wireless Sensor Networks

IoT is a network of physical objects or things that can communicate and share information. In IoT-enabled Wireless Medical Sensor Networks (WMSN), the smart sensing devices share remote patient monitoring data with central repositories. During medical data aggregation and transmission, security is mandatory to guard against intruders. The main problem in existing base schemes is that complex multiplication operations are used for batch key creation. These schemes are computationally expensive and require huge memory space at the aggregator node (AN). Ghawar Said et al. (2022) present a lightweight Secure Aggregation and Transmission Scheme (SATS) for secure and lightweight data computation and transmission. SATS provides a lightweight XOR operation for obtaining batch keys instead of the expensive multiplication operation.

In Wireless Sensor Networks (WSN) sensors cover a large area and can have several sensors in the same region. It may lead to the collection of repeating data patterns, resulting in high computing and communication costs described by Ullah et al. (2020). Therefore, aggregation is a critical activity for removing repeating patterns from data before transmitting it over a communication channel to reduce communication costs and storage capacity. Many key challenges disturb the narration of the WSNs due to their appearances. Efficient energy utilization is the main issue for the survivability of the network in the IoT-enabled WSN in Singh et al. (2020). IoT-enabled wireless sensor networks are used in several survivability applications like remote health monitoring, smart homes, and intelligent transportation systems.

Wang et al. (2019) presented a time-scheduling algorithm that provides effective data gathering by employing mobile sink nodes. Although, each mobile sink node moves on its trajectory, and a minimum spanning tree is employed to reduce the transmission cost. Naghibi et al. (2021) in this article authors suggest a secure data aggregation structure based on a grouping of the star and tree structure. Physically, the network is separated into four equal halves. Each portion recognizes a regular and consistent star structure to convey data. Hasheminejad & Barati (2021) describe a viable data aggregation approach based on tree topology. The scheme intends to lower energy usage, improve network dependability, and extend the life of the network. SATS protects against several security threats such as denial of service attacks, the man-in-the-middle attack, and reply attacks The proposed SATS are compared with relevant schemes and the results show that it provides better storage capacity, computations cost, communications cost, and energy consumption.

3. METHODOLOGY

3.1 Blockchain Technology

Blockchain technology has received a lot of interest from both academic and industrial sectors as a result of the success of the Bitcoin application. Building a blockchain that is resistant to temperature changes is the initial objective of blockchain technology. Blockchain technology has five significant components: (i) Node, (ii) Transactions, (iii) Blocks, (iv) Miners, and (v) Consensus. Every component plays a vital role in blockchain operation. The node can be represented by a computer, server, or individual users followed by the transaction as a building block of the network. Blocks are storage devices that contain a set of previous transaction data. Miners are a set of rules verified during block accumulation. The consensus algorithm is a major part used for blockchain execution. Figure 4 illustrates the components of a blockchain.

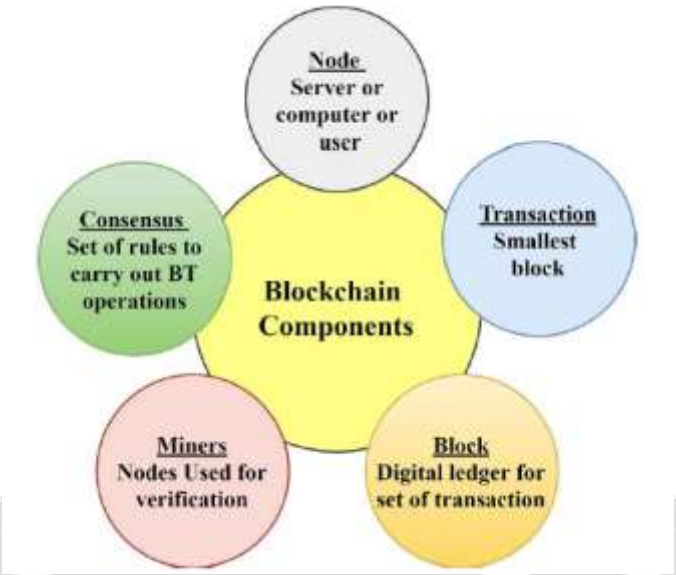

Fig-4 Major components of a blockchain.

Durga et al. (2022) explore the building mechanism of a secured private blockchain in a disinter mediating peer-to-peer network that can be employed for smart healthcare. Although many blockchain-based image encryptions have been proposed for smart healthcare by Hakak et al. (2020) improvisation is still needed in terms of the strength of the security algorithms that can defend against IoT attacks.

Khan et al. (2020) have propounded a scheme to encrypt image data by storing cryptographic pixels of an image on the blockchain. Encrypted results proved that this method could significantly secure the data from the leakage of information. The main upside of this work was that it could dispense IoT Security risks as this method could safely offload the data from different gadgets. The major limitation of this scheme is limited transaction speed and computing resources. Sultana et al. (2020) have provided a framework that gives a short outline about how to decentralize a trustless model that can handle security issues of medical images in healthcare systems. This has been finished by the fussing blockchain with zero trust standards. This method ensures role-based access that can improve the security of an image. The major disadvantage of this method is the network speed. Xiaoming et al.(2019) have proposed a shared design that relies on the blockchain to provide a hypothetical premise for non-designing practice. The principal preferred position of this plan is it can ensure the proficiency of the framework and improve the application administration capacity of distant detecting pictures. Faragallah et al. (2020) have introduced a color image crypto-logical version that utilizes RC6 for various operation vogues. A recreation model has been proposed to survey the presence of crypto logical versions with various activity vogues utilizing different encryption calibers measurements.

3.2 SDN- Blockchain Classifier

Software-Defined Networking (SDN) is known as a new model that separates the control plane and the data plane and is anticipated as a favorable solution for implementing Blockchain, to offer the scalability and adaptability required for IoT shown in Amin et al. (2021). The scalability of the network rises in direct proportion to the users' enhanced privacy on the network. Blockchain and SDN are two top innovations utilized to create secure network architectures and provide trustworthy data transmission.

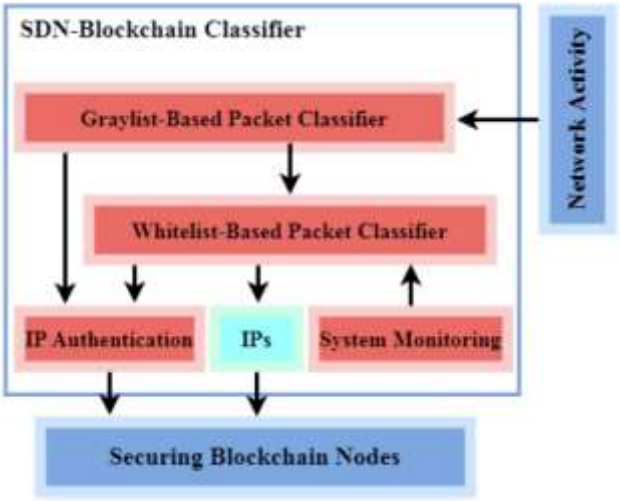

Fig-5 Proposed Architecture of SDN-Blockchain Classifier

Ghamdi (2022) proposed work, concentrated on blockchain-based SDN and creates an SDN-Blockchain Classifier shown in Figure 5. This IDS-based security tool provides a trust-based classifier by handling and reducing harmful traffic through traffic fusion and aggregation. In this work, developed SDN-Blockchain Classifier (Graylist-Based Packet, Whitelist-Based Packet), a trust-based security tool for blockchain-based SDN explained in algorithm 1. Through traffic fusion and aggregation, we reduce malicious traffic and protect blockchain nodes from attack. In a practical implementation, an incoming packet must first travel through the graylist-based packet classifier module to determine if its IP address is on the graylist.

Algorithm 1 SDN-Blockchain Classifier
Input: Arriving Packets
Output: Notifications in case of MAC Flooding attacks are found
START
Mode = W (Whitelist-Based Packet Classifier)
While (A=arriving packets())
{
Preprocessing (P)
if (Mode = W)
// Graylist-Based Packet Classifier IDs
B = CD(A) where B is built from a set of A
Classify B using IDs mechanism
if (MAC Flooding attack found)
{
Mode = G
Generate Notifications
}
else
{
// Whitelist-Based Packet Classifier IDs
B = SD(A)
Classify B using IDs mechanism
if (MAC Flooding attack found)
Generate Notifications
if (MAC Flooding attack not founded within the specified time)
Mode = W
}
}

END
If a match is discovered, the condition for this packet in the look-up table can be examined. If anyone criterion is not satisfied, the packets will be sent to the whitelist-based categorization module under the second condition. If the packet's IP address is not on the graylist, it must be forwarded to the whitelist-based packet classifier module.

Graylist-Based Packet Classifier consists of two sections: a look-up table for comparison and a whitelist containing all whitelisted IP addresses. To hold both general and particular conditions, the lookup table can include two sub-tables. Firstly, general conditions: This database keeps track of all extra criteria that must be checked with incoming traffic, including Flag data, network conditions, etc. Secondly, particular conditions:

Whitelist-Based Packet Classifier the arriving contents with the IDS rules that have been previously saved based on their IP addresses, this module can assist in filtering network traffic. The supervise engine may determine the IP reliability by gathering relevant network data broadcast by the installed IDS and whitelist-based packet classifier module. It maintains the whitelist by the following weighted ratio-based whitelist generation techniques as indicated in Equation 1.

$$IP\ Certainty = \frac{\sum_{e}^{m} = 1\ e}{\sum_{c}^{n} = 1\ 10 * c}\ (m,n\ \in M) \quad \textbf{(1)}$$

where 'e' denotes the number of excellent packets, 'c' is the number of poor packets and ten is the rate of weight. In prior analysis, the rate of weight varied between 1 to 30. Thus, the stability between the wrong positive and wrong negative rates could be achieved at a load of 20. It can be referred to the earlier work for further information on the creation of whitelists and the effects of the weighting factor.
Finally, it is concluded by evaluating Salman et al. (2019) proposed framework SDN-Blockchain Classifier performance against MAC flooding attack in a simulation setting and demonstrating that it can attain optimized average throughput, response time, packet loss of crossing domain path, energy efficiency, end-to-end delay.

4. EXPERIMENTS AND RESULTS

In this section, the proposed method efficiency using various parameters such as average throughput, response time, packet loss of crossing domain path, energy efficiency, end-to-end delay, a file transfer operation, energy consumption, and CPU utilization compared to some methods under flooding attacks are appraised. Blockchain Fundamental (BCF), AS Cooperative Inter-domain Reputation (ASCIR), and Blockchain-based SDN-enabled Secure Routing (BSDNSR), are methods used in their scenario. Compare the proposed solution with BCF, ASCIR, and BSDNSR. A well-known cryptocurrency called Ethereum has completed the long-awaited switch to proof of stake. Proof-of-work, a consensus method that requires a considerable amount of computational power from each decentralized node active in the network, was once the foundation of the Ethereum blockchain. The proof-of-stake has various benefits, including improved energy efficiency, fewer access restrictions, hardware requirements, and less centralization risk.

4.1 Average Throughput

The complete throughput time or complete operation time of transactions refers to the amount of transaction demands made by IoT devices in a network. Additionally, It is found that after a certain period, the efficiency of the proposed framework with respect to security and secrecy is significantly superior to BCF, ASCIR, and BSDNSR methods shown in Figure 6.

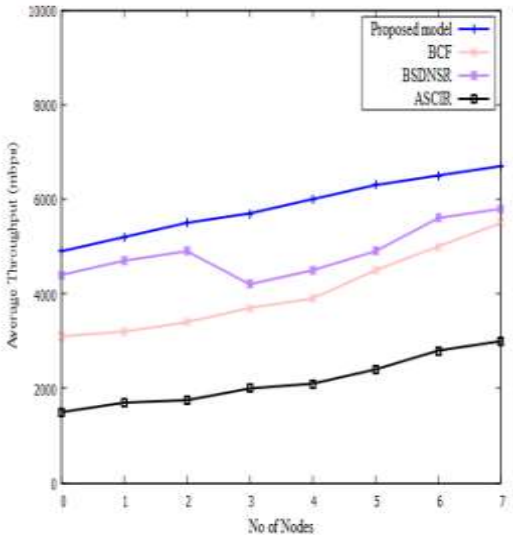

Chart-1 Average Throughput

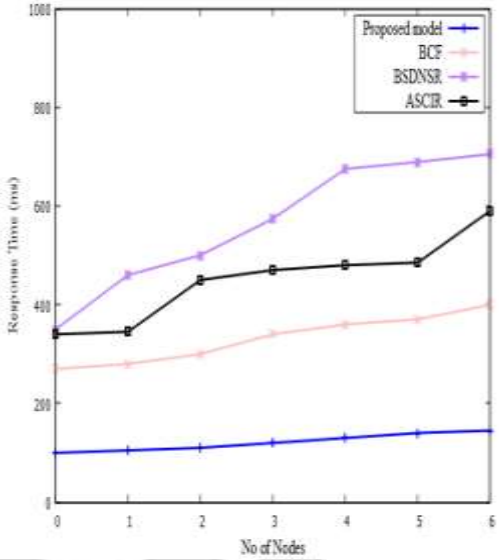

Chart-2 Response Time

4.2 Response Time

It concerns the amount of time it takes for files to be sent between two Internet of Things devices, and it can be seen that the proposed solution is faster than the conventional one since the controller uses a proprietary routing protocol. The average response time for file transfers of various bulks among IoT nodes is shown in Figure 7. Additionally, It has been stated that the proposed technique achieves better than the BCF, ASCIR, and BSDNSR methods when fewer frequent assaults are involved.

4.3 Energy Efficiency

In the Blockchain-enabled SDN-IoT framework, energy efficiency is one of the crucial elements to be monitored and optimized. Energy indicates the proportion of energy used by all IoT devices currently connected to the network. As a result, the energy efficiency between the proposed model with that of BCF, ASCIR, and BSDNSR methods as shown in Figure 8 uses around 50% less energy. Finally, when compared to the other components, the proposed method uses the best energy efficiency.

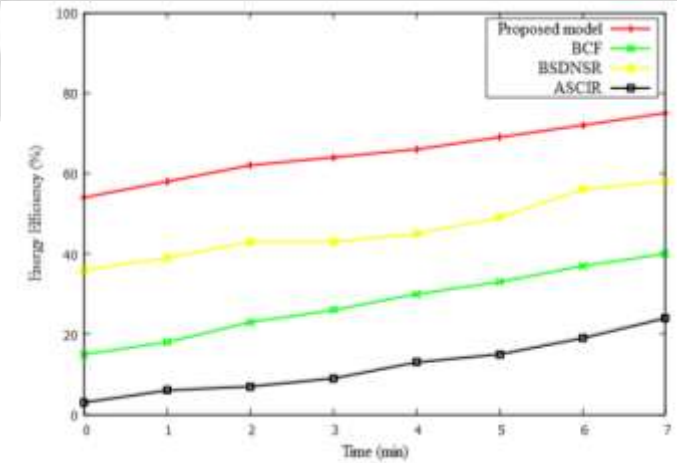

Chart-3 Energy Efficiency

4.4 End To End Delay

The real-time systems use IoT applications, so it is essential to complete all tasks as quickly as possible. The head of each cluster should therefore be chosen very carefully. The end-to-end delay as a function of simulation duration is

shown in Figure 9 curves when the proposed method, BCF, ASCIR, and BSDNSR methods are performed for seconds.

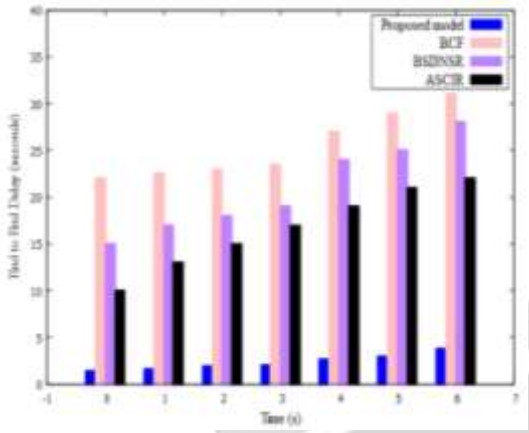

Chart-4 End-to-end delay

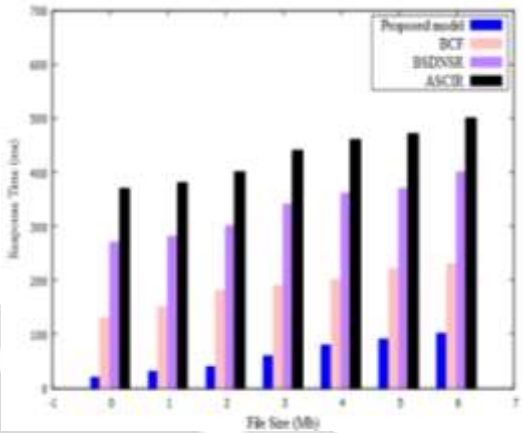

Chart-5 File transfer operation

4.5 File Transfer Operation

A TCP-based network, like the Internet, uses the File transfer Protocol (FTP) as a regular network protocol to share data from one computer to another. FTP has distinct control and data interfaces between the user and server and is based on a client-server framework. The local host in an FTP transaction is frequently referred to as the system of the final user. The second computer in an FTP connection is called the remote host, which is frequently a server. Both computers must be networked and configured properly to send data using FTP. The proposed approach can transport huge files more quickly than the current core-based method depicted in Figure 10. As a result, the suggested method enables speedy and safe file transfers.

4.6 Energy Consumption

Networking components and routing devices often use a lot of energy while transmitting data. Particularly, the device's energy use is inversely associated with the rate of data it transmits. The energy usage may be decreased by utilizing the SDN-Blockchain classifier concept and using the CHs for transmission. It is clear that the suggested method uses less energy and selects the CHs more effectively than the BCF, ASCIR, and BSDNSR methods depicted in Figure 11.

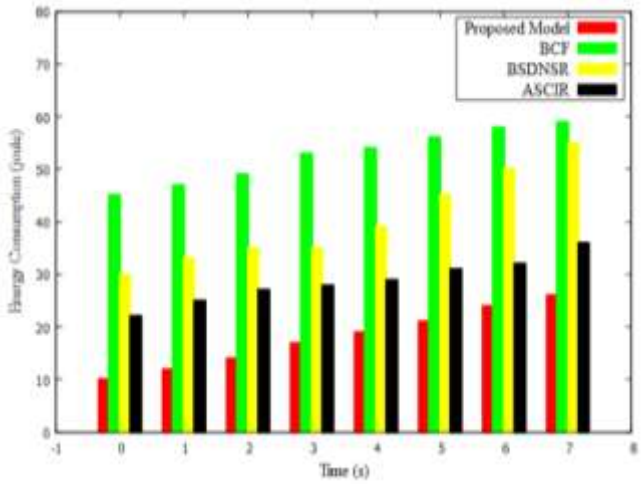

Chart-6 Energy Consumption

5. CONCLUSION AND FUTURE WORK

IoT is essentially important to improve the quality of human life through the interconnection of different technologies, smart devices, and applications. Healthcare schemes consider medical architecture and its role in the physical world. Blockchain enables SDN-IoT ecosystems to struggle with underdeveloped workflow descriptions in the early stages of development as well as a dearth of resources to effectively install and accomplish this environment.

SDN controllers may turn into a single point of failure because of the centralized control, making them a prime target for numerous attackers. The study of the convergence between Blockchain and SDN is becoming more prominent due to the growing use of blockchain technology. MAC flooding attacks might make blockchain nodes incapable of sending or receiving any block information, making blockchain-based SDN insecure. Because of this problem, SDN-Blockchain Classifier is created in this work, a trust-based security instrument for blockchain-based SDN, by reducing hostile traffic and safeguarding blockchain nodes through traffic fusion and aggregation.

The proposed approach SDN-Blockchain Classifier outperforms than assumed baseline on both energy use and end-to-end latency, according to the experimental assessment. Overall, compared to a traditional Blockchain, the SDN Blockchain-Based IoT framework achieves greater performance. The processing times displayed by the SDN controllers are also appropriate when compared to the file transfer operation in transactions made on the Ethereum Blockchain. The paper highlighted some of the key technologies, protocols, and standards with their native security challenges, concerns, and resolutions. In the future, it will be planned to develop the functionality of the architecture and implement the suggested architecture in a large-scale, real-world situation in the future.

6. ACKNOWLEDGEMENT

The author would like to appreciate the effort of the editors and reviewers. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

7. REFERENCES

[1] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (Jan. 2020) Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Network, 34(1), 8–14,https://doi.org/10.1109/MNET.001.1900178

[2] Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image-sharing system based on zero-trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, https://doi.org/10.1186/ s12911-020-01275-y

[3] Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy*, *22*(2), 175. https://doi. org/ 10.3390 /e22020175

[4] Xiaoming, Z., Caiping, L., Dejin, T., Yuchen, S., Zhen, H., & Jisheng, Z. (2019). Design of remote sensing image-sharing service system based on blockchain technology. In *Proceedings of the IEEE International Conference Signal, Inf. Data Processing(ICSIDP)*.

[5] Faragallah, O. S., El-Shafai, W., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., Samie, F. E. A. (2020) Efficiently Encrypting Color Images With Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications. *IEEE Access*, *8*, 103200–103218. https://doi.org/10.1109 /ACCESS.2020.2994583

[6] Durga, R., Poovammal, E., Ramana, K., Jhaveri, R. H., Singh, S., & Byungun, Y. (2022). CES Blocks_A novel chaotic encryption schemes-based blockchain system for an IoT environment. *IEEE Access*, *10*, 11354–11371_ 11371. https://doi.org/10.1109/ ACCESS. 2022.3144681

[7] Al Ghamdi, M. A. A. (2022). An optimized and secure energy-efficient blockchain-based framework in IoT. *IEEE Access*, *10*, 133682–133697. https://doi.org/10.1109/ ACCESS.2022.3230985

[8] Salim, M. M., Wang, D., El Atty Elsayed, H. A., Liu, Y., & Elaziz, M. A. (2020). Joint optimization of energy-harvesting-powered two-way relaying D2D communication for IoT: A rate–energy efficiency tradeoff. *IEEE Internet of Things Journal*, *7*(12), 11735–11752. https://doi.org/10.1109/ JIOT. 2020. 2999618

[9] Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, *161*(July), https://doi.org/10.1016 /j.jnca.2020.102630

[10] Bharadwaj, H. K., Agarwal, A., Chamola, V., Lakkaniga, N. R., Hassija, V., Guizani, Mohsen, & Sikdar, B. (2021). A review on the role of machine learning in enabling IoT based healthcare applications. *IEEE Access*, *9*, 38859–38890. https://doi.org/ 10.1109/ACCESS.2021.3059858

[11] Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016). Mobile health (m-health) system in the context of IoT. In *Proceedings of the IEEE 4th International Conference Future Internet Things Cloud Workshops (FiCloudW)*, *42* p. 39–42. https://doi.org /10.1109/W-FiCloud.2016.24

[12] Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T.-H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEE Access*, *10*, 121173–121192. https://doi.org/10.1109/ ACCESS.2022.3220622

[13] Gomathi, R. M., Krishna, G. H. S., Brumancia, E., & Dhas, Y. M. (2018). A survey on IoT technologies, evolution and architecture. In *Proceedings of the Int. Conf. Comput., Commun*. *Signal Processing (ICCCSP)*, *5*, 1–5. https://doi.org/10.1109/ICCCSP. 2018. 8452820

[14] Santos, L., Rabadao, C., & Gonçalves, R. (2019). Flow monitoring system for IoT networks. In *Proceedings of the World Conference Inf*. Syst. Technol. *Lecture Notes in Control and Information Sciences*, 420–430.

[15] Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). sMachine learning for security and the Internet of things: The good, the bad, and the ugly. *IEEE Access*, *7*, 158126–158147. https://doi.org/10.1109/ACCESS. 2019.2948912

[16] Alves, T., Das, R., & Morris, T. (2018). Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *IEEE Embedded Systems Letters*, *10*(3), 99–102, https://doi.org/10.1109/LES. 2018. 2823906

[17] Werth, & Morris, T. H. (June 2019). A speci_cation-based intrusion prevention system for malicious payloads. In *Springer* National Cyber Summit. Cham, Switzerland, p. 153-*168*.

[18] Li, H., & Liu, D. (August 2010). Research on intelligent intrusion prevention system based on snort. In *Proceedings of the Int. Conf. Comput., Mechatronics, Control Electron*. Eng., p. 251-*253*.

[19] Nikhil, R., Anisha, B. S., & Kumar, R. (July 2020). P,"Real-time monitoring of agricultural land with crop prediction and animal intrusion prevention using Internet of Things and machine learning at edge,". In *Proceedings of the IEEE CONECCT*, *6*, 1.

[20] Su, B., Ding, X., Wang, H., & Wu, Y. (January 2018). Discriminative dimensionality reduction for multi-dimensional sequences. *IEEE Transactions on Pattern Analysis and Machine Intelligence* IEEE (Trans.), *40*(1), 77–91. https://doi.org/10.1109/TPAMI. 2017.2665545

[21] Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (November 2017). Deep reinforcement learning: A brief survey. *IEEE Signal Processing Magazine*, *34*(6), 26–38. https://doi.org/10.1109/MSP.2017 .2743240

[22] Ghamdi, M. A. A. Mohammed A. Al Ghamdi "an optimized and secure energy-efficient blockchain – based framework in IoT",. (2022). *IEEE Access*, *10*, 133682–133697. https://doi.org/10.1109/ACCESS.2022.3230985

[23] Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). IoT survey: An SDN and fog computing perspective. *Computer Networks*, *143*, 221–246, Oct.. https://doi.org/10. 1016/j. comnet.2018.07.020

[24] Amin, R., Rojas, E., Aqdus, A., Ramzan, S., Casillas-Perez, D., & Arco, J. M. (2021). A survey on machine learning techniques for routing optimization in SDN. *IEEE Access*, *9*, 104582–104611. https://doi.org/10.1109/ACCESS. 2021. 3099092

[25] Ahanger, T. A., & Aljumah, A. (2018). Internet of Things: A comprehensive study of security issues and defense mechanisms. *IEEE Access*, *7*, 11020–11028.https:// doi.org /10.1109/ACCESS. 2018.28 76939

[26] Ullah, A., Said, G., Sher, M., & Ning, H. (2020). 'Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN,' Peer_Peer Netw. *Appl.*, *13*(1), 163_174, Jan.

[27] Singh, J., Kaur, R., & Singh, D. (2020). A survey and taxonomy on energy management schemes in wireless sensor networks. *Journal of Systems Architecture*, Art. no. 101782. https://doi.org/10.1016/j.sysarc.2020.101782

[28] Wang, T., Li, Y., Wang, G., Cao, J., Bhuiyan, M. Z. A., & Jia, W. (2019). Sustainable and ef_cient data collection from WSNs to cloud. *IEEE Transactions on Sustainable Computing*, *4*(2), 252–262, https://doi.org/ 10.1109/TSUSC.2017.2690301

[29] Naghibi, M., & Barati, H. (2021). SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, *12*(12), 10769–10788, https:// doi.org/10.1007/s12652-020-02751-z

[30] Hasheminejad, E., & Barati, H. (2021). 'A reliable tree-based data aggregation method in wireless sensor networks,' Peer_Peer Netw. *Appl.*, *14*(2), 873_887.

[31] Said, G., Ghani, A., Ullah, A., Kwak, K. S., Bilal, M., Kwak, K. S., Kwak, K. S. (2022). Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks. *IEEE Access*, *10*, 33571–33585. https://doi.org/10.1109/ ACCESS.2022.3160231.

[32] Engineer, M., Tusha, R., Shah, A., & Adhvaryu, D. K. (March 2019). Insight into the importance of fog computing in Internet of medical Things (IoMT). In *Proceedings of the Int. Conf. Recent Adv. Energy-Efficient Comput. Commun*, p. 1–7. https://doi.org/10.1109/ ICRAECC43874. 2019.8994985

[33] Tang, W., Ren, J., Zhang, K., Zhang, D., Zhang, Y., & Shen, X. (2019). Efficient and privacy-preserving fog-assisted health data sharing scheme. *ACM Transactions on Intelligent Systems and Technology*, *10*(6), 1–23, Dec. 2019. https://doi.org/10.1145/3341104

[34] Guo, C., Tian, P., & Choo, K.-K. R. (2021). Enabling privacy-assured fog-based data aggregation in E-healthcare systems. *IEEE Transactions on Industrial Informatics*,1948–1957. https://doi.org/10.1109/TII.2020.2995228

[35] Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT ehealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*, 659–676, https://doi.org/10.1016/j.future.2017. 04.036

[36] Puliafito, C., Mingozzi, E., Longo, F., & Pulia, A. (2019). to, and O. Rana, Fog computing for the Internet of Things: A Survey. *ACM Transactions on Internet Technology*, 1-41.

[37] Okay, F. Y., & Ozdemir, S. (April 2018). 'A secure data aggregation protocol for fog computing based smart grids,' in *Proc. IEEE. Power Electronics Power Eng. (CPE-POWERENG)* 12th Int. Conf.,p. 1- 6.