Stochastic Modelling and Computational Sciences

ENHANCING IOT SECURITY: A COMPARATIVE ANALYSIS OF BLOCKCHAIN AND NON-BLOCKCHAIN APPROACHES

Ravinder Singh Madhan[1] and Randeep Singh[2]
[1, 2]Department of Computer Science & Engineering, IEC University, Baddi, 174103 (Himachal Pradesh)
[1]ravimadhan@gmail.com and [2]randeeppoonia@gmail.com

ABSTRACT

Nowadays, there is a significant and fast expansion in the development of the Internet of Things (IoT). The aforementioned circumstance gives rise to security concerns due to many breaches of security regulations. Furthermore, the proliferation of blockchain technology has seen significant growth since its first introduction via the widespread use of Bitcoin. The use of blockchain technology may effectively address security concerns associated with this Internet of Things (IoT) system. One such approach is establishing secure communication protocols among Internet of Things (IoT) devices. The goal of this project is to create a system for the Internet of Things (IoT), and it will do it either with or without the use of blockchain technology. After that, a comparison study will be carried out in order to assess the efficiency of both of the systems and determine which one performs better overall. In places where blockchain technology is unavailable, the MQTT communication protocol is often used in Internet of Things (IoT) devices. Ethereum, a blockchain platform, is being used in this particular scenario, and it is being accompanied with a smart contract. Both of these Internet of Things (IoT) systems will undergo analysis to assess their security levels via the simulation of assaults and observation of their security elements. The test findings indicate that the Internet of Things (IoT) system using blockchain technology exhibits a superior degree of security compared to the IoT system without blockchain technology.

Keywords: Internet of Thing, Security, Blockchain

1. INTRODUCTION

Researchers as well as practitioners are compelled to explore novel intelligent services capable of extracting crucial insights from the vast array of IoT datadue the expeditious advancement of IoT technology [1][2]. The IoT is a phenomenon that occurs when physical items, such as mobile devices, household appliances, automobiles, and buildings, are enhanced with electronics, software, sensors, and network connection. The IoT facilitates the acquisition and transmission of data among interconnected items. The IoT enables the remote detection, identification, and control of objects by using the pre-existing network infrastructure. The integration of sensors and actuators with the IoT results in the manifestation of cyber-physical systems (CPS). CPS include several ideas such intelligent grids, intelligent homes, intelligent cities, and intelligent transportation systems. The IoT has emerged as a technologically advanced field in the present context [3].The integration of IoT devices has been seen across several domains, including intelligent automotive systems, healthcare services, sustainability initiatives, and personal wearable technology. The integration of these systems has led to an increase in the quantity, diversity, velocity, and reliability of data that are handled by interconnected systems[4][5].The IoT is a network that connects many objects to the Internet, enabling communication and information exchange via information sensing devices using standardized protocols. The IoT is often seen as an expansion of the current connection between individuals and apps, introducing a new dimension of communication via interconnected physical objects. The expansion process of the IoT is a complex and extensive technical innovation process. The IoT concept facilitates many applications across several areas via its connections and communication capabilities. The inception of the Internet may be traced back to the first connection of two computers, which then led to the establishment of the World Wide Web via the interconnection of a vast multitude of computers. The emergence of mobile internet coincided with the integration of mobile devices with the internet. The IoT has emerged as a network of interconnected ordinary things that have been integrated into the Internet. IoT devices are susceptible to a wide range of malicious attacks because to their accessibility from untrusted networks such as the internet[6]. Consequently, it is imperative to address the security concerns associated with IoT networks. The assaults may manifest as either internal or external in nature. External attacks occur when the attacker is not affiliated with the network, whilst internal attacks are initiated by hostile nodes that are integrated inside the network.

The IoT is anticipated to establish a vast network consisting of billions or perhaps trillions of interconnected devices, which would encounter several practical and application-related obstacles. A vast multitude of gadgets are anticipated to connect to the internet in the forthcoming years. According to CISCO's prediction, it is expected that there would be a total of 50 billion by the year 2020.

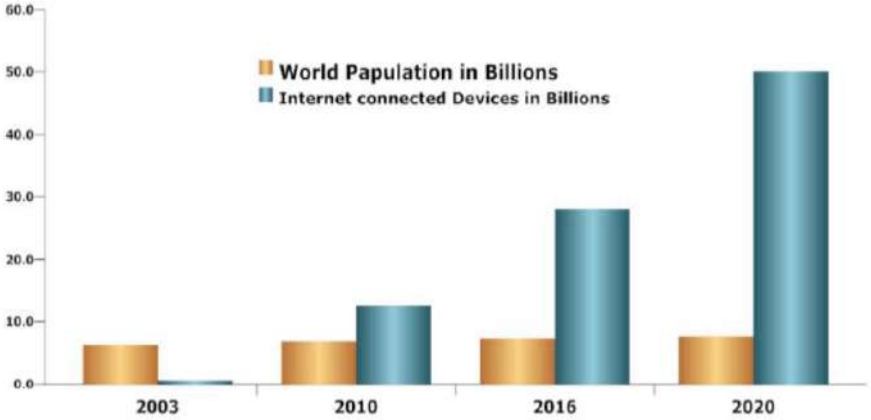


Figure 1. The development in Internet connected objects by 2020[7].

The Internet is often linked to a broad range of devices on a global scale, including computers, smartphones, and tablets. As seen in Figure 1, the quantity of entities connected to the Internet has exceeded the global human population. Based on CISCO's projections, it is anticipated that by the year 2020, every person worldwide will be connected to the Internet via more than six gadgets. Hence, it may be argued that the IoT is poised to emerge as a very significant technical advancement during the current decade. The IoT is a component of a broader, dynamic phenomena that encompasses the integration of newly affiliated objects with the preexisting connections of people, processes, and data. The expansion of the IoT demands the implementation of strong security measures to safeguard connected devices and their associated systems. This necessitates the exploration of innovative security techniques for the IoT.

1.1 Security Issues of the Device

The market for IoT devices has seen remarkable development, as shown by the findings in many business surveys[8]. According to estimations, the number of IoT endpoints is expected to reach 5.8 billion by the conclusion of the current year. Additionally, it is anticipated that global expenditure on smart devices would amount to USD 1.2 trillion by the year 2022. The emergence of contemporary technologies such as machine learning, artificial intelligence, and real-time data streaming, along with the rapid access to the cloud, has enabled companies to see these gadgets as viable solutions to their unique challenges[9]. An increasing number of firms are increasingly dependent on them to undertake the process of remodeling and optimizing their businessneeds[10][11].

- **Resource Limitation:**All research studies have consistently identified limited resources inside the device as a significant obstacle in the implementation of cryptographic algorithms. There exists a potential scenario whereby an adversary might deplete the memory resources of a device by inundating the open port with a substantial volume of requests.
- **Lack of User Authentication:**The limited memory capacity of the device poses a constraint on the feasibility of deploying intricate authentication methods. Therefore, in order to adhere to regulatory regulations, manufacturers often resort to utilizing default credentials and widely shared keys.

- **Inadequate Encryption:**Encryption is a powerful method for making data unintelligible to a prying eye. Cryptographic systems rely on the randomness of the algorithm and the size of the keyto successfully transform data. The device's small storage capacity makes it difficult to save large keys. An opponent may take advantage of this by attempting to crack a lower key size via a brute force assault.
- **Efficient Access Control:**The absence of a well-implemented access control mechanism on the device is often seen. Numerous manufacturers permit the use of default credentials on their devices, whereby the same user is bestowed with administrative powers. The potential for greater harm exists when an attacker has elevated privileges, since they may inflict damage not just on the targeted device but also on the network within which it is situated.

2. REVIEW OF LITERATURE

Awajan, (2023)[12]examined that cybercriminals are more interested in assaulting the IoT now than ever before due to its rapid expansion. The increasing frequency of cyberattacks on IoT devices and intermediate communication mediums lends credence to this assertion. If an attack on the Internet of Things goes unnoticed for a long time, it might disrupt services severely, costing a lot of money. In addition, it carries the risk of having one's identity stolen. To ensure the dependability, security, and profitability of IoT-enabled services, real-time intrusion detection on IoT devices is required. In this research, we provide a new intrusion detection method for IoT devices that relies on Deep Learning (DL). This intelligent system utilizes a four-layer deep Fully Connected (FC) network architecture to detect malicious traffic that might lead to attacks on IoT devices. The proposed system was built to be compatible with any existing communication standard to facilitate rapid rollout. The proposed system performs well in experimental performance analyses against both simulated and real invasions. Among the types of attacks, it can see are Blackhole, Distributed Denial of Service, Opportunistic Service, Sinkhole, and Workhole, with a detection rate of 93.74 percent on average. The proposed intrusion detection system achieves average values of accuracy (93.71%), recall (93.82%), and F1-score (93.47%). The average detection rate of this cutting-edge deep learning-based IDS is 93.21%, making it an excellent candidate for improving the security of IoT networks.

Yazdinejad et al., (2023)[13]intended that a recent innovation in secure computational communication systems is the incorporation of blockchain into the IoT. Even as blockchain-based IoT solutions are becoming more popular, security risks are adapting and creating new dangers. Furthermore, when blockchain is integrated with IoT networks, vulnerabilities, privacy concerns, and security risks are amplified due to fraudulent transactions and active assaults. Both the IoT and the blockchain communities are interested in the idea of blockchain-based IoT attacks. The whole breadth of security and privacy concerns posed by the intertwining of IoT and blockchain may be reduced to network assaults. Since ambiguity and vagueness concerns are inevitable in IoT data, blockchain alone is inadequate to cope with risks and attacks in IoT networks, despite the fact that it may offer security advantages. Uncertainty is a major problem in IoT networks due to the diverse nature of IoT inputs. For effective nonlinear aggregation in detection, the suggested fuzzy DL makes use of the fuzzy Choquet integral. To minimize the inaccuracy introduced by attack detection in ANFIS, we use metaheuristic techniques. To combat fraud and improve performance on the blockchain layer, we use FM to verify transactions. This framework is the first secure, intelligent, fuzzy blockchain framework that also takes consideration of uncertainty problems in Internet of Things (IoT) networks and provides more leeway in terms of making decisions and allowing payments at the blockchain layerwhen it comes to detecting and identifying security concerns. Based on the results of the study, it can be concluded that the blockchain layer is efficient in terms of throughput and latency, while the intelligent fuzzy layer is efficient in terms of performance metrics for spotting risks on the blockchain and IoT network sides.

Natarajan et al., (2023)[14]studied that the Internet of Medical Things (IoMT) is a novel approach that establishes a connection between medical devices and their corresponding software and computer networks used in the healthcare 5.0 domain. The rapid advancement of intelligent medical devices on IoMT platforms has resulted in the integration of noteworthy technologies in the modernization of healthcare systems, the management of diseases, and enhancements in patient treatment protocols. The aforementioned developments have resulted in the integration of significant technological advancements in the modernization of healthcare operations, the management of illnesses, and the enhancement of patient treatment protocols. The IoMT enables users to use a diverse array of cloud-based services, including but not limited to data screening, data exchange, tracking patients, information collection and investigation, and sanitary hospital care. The effectiveness of the approach that was recommended was analyzed and compared to that of a number of other ways that were already in use. The findings shown that the suggested method offers both improved safety and increased efficiency in the use of energy.

Kumar et al., (2022)[15]examined that the implementation of the industrial healthcare system has facilitated the potential for achieving sophisticated real-time patient monitoring and enhancing the standard of medical services by means of data exchange among intelligent wearable devices and sensors. However, public network communication and surveillance are inherently risky, which opens up new security and privacy vulnerabilities due to the interconnectedness of gadgets. Taking cues from the presentations that came before, we propose a novel data sharing system we call PBDL, which combines DL techniques with permissioned blockchain and smart contracts. The primary focus of PBDL is the implementation of a blockchain framework that facilitates the registration, verification, and validation of the participating entities. This is achieved via the use of a consensus mechanism based on smart contracts. The SA-BiLSTM model is employed for identifying assaults and improve the process of detecting them, while the SSVAE technique is responsible for encoding or changing healthcare data into a unique format. Experimental findings and security analyses performed on the IoT-Botnet and ToN-IoT datasets verify the PBDL framework's supremacy over the state-of-the-art methods currently in use.

Rathore et al., (2022)[16]stated that high-speed wireless network technologies are of great importance in the context of autonomous vehicle communication systems (AVS), especially in the realm of the Internet of Vehicles (IoV), as they significantly improve the efficiency and dependability of the communication network. The increasing scale of IoV connectivity has become an integral component of our daily activities. The IoV enables the seamless remote interconnection of vehicles with one another, as well as with other platforms and organizations that use a shared communication system. The establishment of a robust connection between cars and the need for information sharing among them provides a susceptibility and potential risks that may be used by those engaging in cybercriminal activities. The primary focus of this study is to enhance the level of data security in real-time communication inside the IoV context. This paper proposes a privacy strategy for the IoV that relies on trust, encryption, and steganography techniques. The present approach employs an EAST which incorporates encryption and steganography methods. The proposed EAST algorithm is subsequently compared to several existing encryption methods, namely AES, DES, G-DES (Generalized DES), and Standard LSB. The experimental findings demonstrate the potential of the suggested EAST approach, exhibiting superior time efficiency (0.86 ms), avalanche effect (58.81%), and PSNR (78.58%) in comparison to existing state-of-the-art techniques.

Bhaskar et al., (2022)[17]suggested that Electric vehicles (EVs) already have a prominent position within contemporary transportation automation systems, serving as a viable alternative to traditional fossil fuel-powered cars. Electric vehicles (EVs) primarily rely on electric charges, with the optimal use, charging, and energy management serving as crucial factors in the operation of EVs. It is essential to implement effective energy management strategies within the context of contemporary electric vehicle (EV) managementin order to address these challenges. This research presents a revolutionary approach to energy management in transportation automation via the use of a blockchain-based secure system. The electric vehicles (EVs) are mostly equipped with Internet of Things (IoT) sensors to gather data pertaining to variables such as charging status, anticipated journey distance, and EV position. The provided data has been analyzed by an information center and afterwards used in a random forest classifier for the purpose of determining the billing fee. Subsequently, the data may be used by the power scheduling algorithm to determine the closest charging facility (minimizing distance) and optimal charging time for a certain electric vehicle. Ultimately, the aforementioned data is saved in discrete units known as blocks, with the purpose of minimizing the potential for misrepresentation in electric vehicles (EVs) and facilitating secure financial transactions between users and charging stations. The findings demonstrate that the suggested approach offers enhanced electric vehicle (EV) management, achieving an accuracy rate of 94.5%. Additionally, it reduces communication overhead by 10% in comparison to current state-of-the-art methods.

Cui et al., (2021)[18]examined that the identification of anomalies in the IoT is of great standing, as it plays a crucial role in ensuring the security of contemporary vital infrastructures. This includes the detection of faked data injection and the diagnosis of transmission line problems in smart grids. A range of detection approaches, facilitated by ML techniques, have been developed by researchers. In recent times, the use of federated learning (FL) as a distributed machine learning paradigm has gained traction in efforts to enhance detection performance. This approach is particularly appealing owing to its inherent benefits of protecting privacy and reducing latency. Nevertheless, the current solutions based on FL continue to encounter hurdles in terms of efficiency, robustness, and security. In this paper, we provide a blockchain-based decentralized and asynchronous FL framework for detecting anomalies in IoT systems. This framework aims to solve the aforementioned issues by enhancing data integrity, mitigating single-point failure risks, and boosting overall efficiency. Additionally, we propose an enhanced differentially secure FL approach that utilizes GANs to maximize data utility during the training phase. To the best of our current understanding, this system represents a novel implementation of a decentralized FL strategy that incorporates privacy-preserving techniques for the purpose of detecting anomalies in the IoT domain. The simulation results obtained from the real-world dataset exhibit notable advantages in terms of resilience, accuracy, and rapid convergence, all while maintaining a high degree of privacy and security protection.

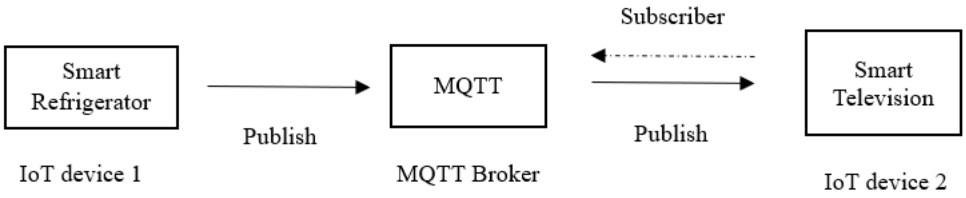
Garre et al., (2021)[19]analyzed that information theft, online service abuse, distributed denial of service assaults, etc. are just some of the ways in which botnets are wreaking havoc on individuals, businesses, and governments. New zero-day attacks, behavioral variety, and obfuscation tactics contribute to their exponential growth, despite extensive efforts to identify and counteract them. Only High Interaction Honeypots (HIH) are able to record every piece of data produced by attackers while they are establishing a botnet. ML approaches are being utilized to the produced data for detection because of their ability to unearth previously concealed patterns. However, previous studies have largely overlooked the importance of the botnet's infected early phase in favor of its later stages of activity. This is the first known method of stopping SSH-based botnets during the infection phase. Consequently, we have devised an SSH-based HIH method to provide a dataset of commands run and network details. We have used ML methods to create a model for real-time detection in this work. This method achieved perfect accuracy in its predictions with no false alarms. All known and undiscovered attempts to infect our honeypots through SSH were uncovered by our system. Our findings show that ML methods are effective for identifying new SSH infections.

Casola et al., (2020)[20]studied that DevOps and Agile are two examples of modern software development approaches that have seen widespread adoption and usage, particularly in the context of building cloud-based services and apps. Although they greatly facilitate software development cycle times, they are not easily incorporated with security design and risk management practices. Due to the absence of readily available automatic tools for assessing risk and evaluating security throughout the design and operation stages, they cannot be easily automated and need substantial financial outlays to accomplish. In this work, our organization offers a unique methodology for implementing Security-by-Design, which is founded on Security Service Level Agreements (SLAs). These SLAs may be seamlessly integrated into modern development practices, offering comprehensive automated assistance throughout the risk management life-cycle. It makes use of a guided risk analysis process and a fully automated security assessment stepto evaluate the security qualities provided by a cloud application and report them in a Security SLA. We empirically tested the suggested technique on a real-world case study and found that it successfully increased designer and development teams' understanding of security concerns while also shortening the safe design process.

Medhane et al., (2020)[21]evaluated that the IoT has a substantial impact on several aspects of society, as it facilitates independent assistance for communication and operations. This, in turn, facilitates the development and adoption of innovative services that are routinely used in everyday life. Conducting thorough research on security frameworks for next-generation IoT is vital, as it enables the development of cutting-edge confidentiality protection systems that effectively address a wide range of assaults against IoT networks. The blockchain technology emerges as a viable alternative for providing notable qualities such as ongoing secrecy, authentication, and resilience. The paper presents a paradigm for distributed security that utilizes blockchain technology, edge cloud infrastructure, and software-defined networking (SDN). The identification of security assaults is accomplished at the cloud layer, resulting in a subsequent reduction of security threats at the edge layer of the IoT network. The gateway that is equipped with SDN provides a mechanism for managing network traffic flows in a dynamic manner. This capability plays a crucial role in the identification of potential security assaults by analyzing and identifying suspicious network traffic flows. Furthermore, it effectively mitigates security attacks by impeding the progress of these suspicious flows. The collected findings demonstrate that the suggested security framework is capable of effectively and efficiently addressing the difficulties associated with data confidentiality arising from the combination of blockchain, edge cloud, and SDN paradigm.

3. Proposed methodology

The following section will provide an explanation of the system that will be developed in this research endeavor.



“Figure 2. IoT System without Blockchain Technology

The first IoT system, shown in Figure 2, employed the MQTT communication protocol, without the integration of blockchain technology. The intelligent refrigerator will transmit data through the MQTT broker by publishing it on a designated topic. Subsequently, the intelligent television establishes a subscription to the subject matter, therefore enabling the acquisition of data from the intelligent refrigerator. The process of encrypting data involves the use of the Advanced Encryption Standard (AES). Furthermore, the encryption key is secured by using a hash algorithm, namely SHA256.

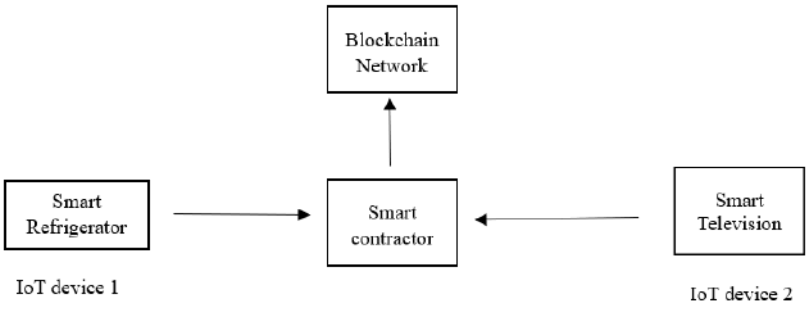


Figure 3. IoT System using Blockchain Technology

In contrast, the second Internet of Things (IoT) system shown in Figure 3 utilizes blockchain technology, whereby the MQTT protocol is substituted with a blockchain network and a smart contract. The present smart contract serves as an intermediate between two Internet of Things (IoT) devices, facilitating the storage and retrieval of data inside the blockchain network. The use of blockchain technology is employed by the smart refrigerator to store data via the implementation of a smart contract. Similarly, the smart television leverages the smart contract to retrieve data that has been previously saved inside the blockchain network.

There are two systems will be developed: one is an Internet of Things (IoT) system without blockchain technology, and the other is an IoT system containing blockchain technology. For the purpose of simplifying the experiment, just two Internet of Things (IoT) devices were used in the simulation. In this particular instance, the simulation conducted pertains to a smart home environment, whereby the first Internet of Things (IoT) device is a smart refrigerator, followed by a smart television as the second item. The intelligent refrigerator is capable of accessing and retrieving data related to food inventory, which is then sent and shown on the intelligent television.

The blockchain platform employed in this study is Ethereum. Specifically, the Ethereum Virtual Machine (EVM) implemented is Go Ethereum, with the Golang programming language. Additionally, the smart contract framework utilized is truffle, with the Solidity programming language. The use of the Elliptic Curve Digital Signature method (ECDSA) encryption method is employed for cryptography on the Ethereum platform. Furthermore, the transaction procedure on the Ethereum platform employs the use of the hash function and encoding techniques. The hash function used in this particular instance is Keccak-256."

4. RESULT AND DISCUSSION

4.1 Testing

The evaluation of IoT systems involves the execution of attack simulations. The process of conducting simulations involves the implementation of sniffer attacks against IoT systems. "The objective of this sniffer attack is to assess the security measures used in the connection between two interconnected IoT devices, namely the smart refrigerator and smart television. The Wireshark program is used for the purpose of network packet sniffing. Furthermore, an examination of the security elements of the hash function and encryption method was conducted by the observation of the avalanche effect during testing.

According to the findings shown in Figure 4, it can be seen that the Keccak-256 hash function exhibits a more pronounced avalanche effect in comparison to SHA-256. The Keccak-256 algorithm is considered superior in terms of hash result quality because to its property of exhibiting a pronounced sensitivity to even little variations in input, resulting in a substantial alteration in its corresponding output. This implies that Keccak-256 has a greater degree of security in comparison to SHA-256.

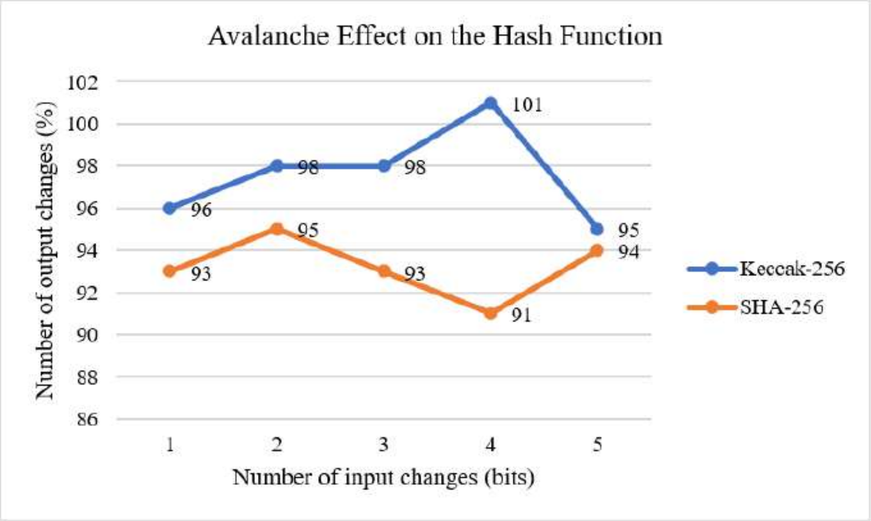


Figure 4. Avalanche Effect on the Hash Function

According to the observations made in Figure 5, it is evident that the AES-256 and ECDSA encryption algorithms exhibit comparable avalanche effects. In some scenarios, AES-256 may exhibit superior performance compared to ECDSA, and conversely, ECDSA may outperform AES-256 in other cases. This implies that the two encryption techniques provide a comparable degree of security.

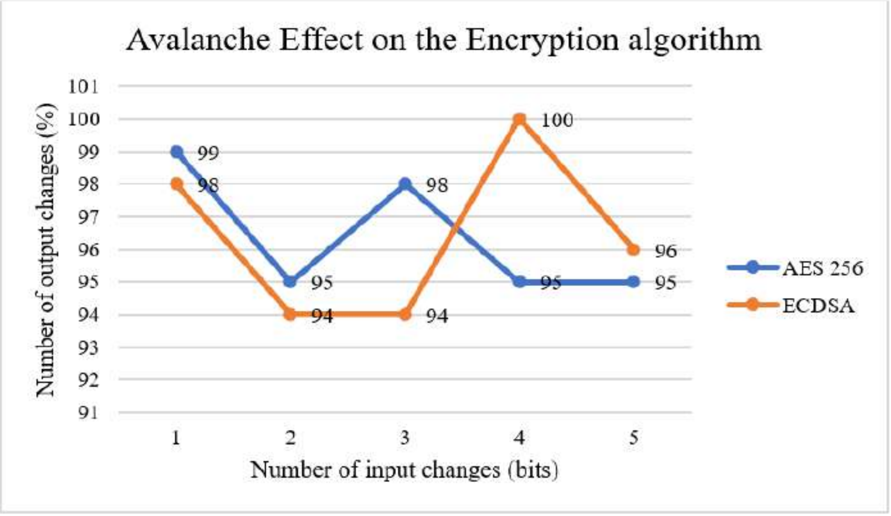


Figure 5. Avalanche Effect on the Encryption Algorithm"

5. CONCLUSION

In recent years, there has been a rapid acceleration in the growth of the IoT; nevertheless, this has been accompanied with an increase in security concerns. The insecure nature of the communication that takes place between different IoT devices is one of the security issues that might develop. In this study, the design and execution of the IoT system have been carried out both without and with the assistance of blockchain technology so that the findings may be compared. The use of MQTT as the communication protocol inside the IoT system is seen in instances when blockchain technology is not employed. Meanwhile, the integration of blockchain technology into the IoT system involves the use of Ethereum as the underlying foundation for the blockchain network. Furthermore, the storage and retrieval of user data inside the blockchain network may be facilitated by the use of smart contracts. Through extensive testing, it has been empirically shown that the use of blockchain technology inside the IoT system effectively addresses any security concerns that may arise during inter-device communication. The use of blockchain technology in an IoT system enhances its security level compared to an IoT system that does not include blockchain technology. The increased security of Internet of Things systems using blockchain technology is evident via the conduct of attack simulations and observations of avalanche effects.

REFERENCES

[1]. Cheng, Yongliang, Yan Xu, Hong Zhong, and Yi Liu. "Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication." *IEEE Internet of Things Journal* 8, no. 1 (2020): 144-155.

[2]. Xu, Rongbin, Yongliang Cheng, Zhiqiang Liu, Ying Xie, and Yun Yang. "Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services." *Future Generation Computer Systems* 112 (2020): 228-242.

[3]. Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "Multi-objective-based feature selection for DDoS attack detection in IoT networks." *IET Networks* 9, no. 3 (2020): 120-127.

[4]. Parra, Gonzalo De La Torre, Paul Rad, Kim-Kwang Raymond Choo, and Nicole Beebe. "Detecting Internet of Things attacks using distributed deep learning." *Journal of Network and Computer Applications* 163 (2020): 102662.

[5]. Wu, Di, Zhongkai Jiang, Xiaofeng Xie, Xuetao Wei, Weiren Yu, and Renfa Li. "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT." *IEEE Transactions on Industrial Informatics* 16, no. 8 (2019): 5244-5253.

[6]. Vlacheas, Panagiotis, Raffaele Giaffreda, Vera Stavroulaki, Dimitris Kelaidonis, Vassilis Foteinos, George Poulios, Panagiotis Demestichas, Andrey Somov, Abdur Rahim Biswas, and Klaus Moessner. "Enabling smart cities through a cognitive management framework for the internet of things." *IEEE communications magazine* 51, no. 6 (2013): 102-111.

[7]. Kumar, B. N., and M. V. P. Rao. "A novel cognitive security approach for internet of things." *International Journal of Engineering and Technology* 9, no. 3S (2017): 579-584.

[8]. Says, Gartner. "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020." *Gartner,[online] Available: https://www. gartner. com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io* (2019).

[9]. Bhattacharjya, Sairath, and Hossein Saiedian. "Establishing and validating secured keys for IoT devices: using P3 connection model on a cloud-based architecture." *International Journal of Information Security* 21, no. 3 (2022): 427-436.

[10]. Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." *Computer* 50, no. 2 (2017): 76-79.

[11]. Van Oorschot, Paul C., and Sean W. Smith. "The internet of things: security challenges." *IEEE Security & Privacy* 17, no. 5 (2019): 7-9.

[12]. Awajan, Albara. "A novel deep learning-based intrusion detection system for IOT networks." *Computers* 12, no. 2 (2023): 34.

[13]. Yazdinejad, Abbas, Ali Dehghantanha, Reza M. Parizi, Gautam Srivastava, and Hadis Karimipour. "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks." *Computers in Industry* 144 (2023): 103801.

[14]. Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0." *Infrastructures* 8, no. 2 (2023): 22.

[15]. Kumar, Randhir, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, AKM Najmul Islam, and Mohammad Shorfuzzaman. "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems." *IEEE Transactions on Industrial Informatics* 18, no. 11 (2022): 8065-8073.

[16]. Rathore, Manjari Singh, M. Poongodi, Praneet Saurabh, Umesh Kumar Lilhore, Sami Bourouis, Wajdi Alhakami, Jude Osamor, and Mounir Hamdi. "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography." *Computers and Electrical Engineering* 102 (2022): 108205.

[17]. Bhaskar, KosurBojji Raju, Aruchamy Prasanth, and Paramasivan Saranya. "An energy-efficient blockchain approach for secure communication in IoT-enabled electric vehicles." *International Journal of Communication Systems* 35, no. 11 (2022): e5189.

[18]. Cui, Lei, Youyang Qu, Gang Xie, Deze Zeng, Ruidong Li, Shigen Shen, and Shui Yu. "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures." *IEEE Transactions on Industrial Informatics* 18, no. 5 (2021): 3492-3500.

[19]. Garre, José Tomás Martínez, Manuel Gil Pérez, and Antonio Ruiz-Martínez. "A novel Machine Learning-based approach for the detection of SSH botnet infection." *Future Generation Computer Systems* 115 (2021): 387-396.

[20]. Casola, Valentina, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. "A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach." *Journal of Systems and Software* 163 (2020): 110537.

[21]. Medhane, Darshan Vishwasrao, Arun Kumar Sangaiah, M. Shamim Hossain, Ghulam Muhammad, and Jin Wang. "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach." *IEEE Internet of Things Journal* 7, no. 7 (2020): 6143-6149.