ISSN: 2633-4828 Vol. 5 No.3, September, 2023

International Journal of Applied Engineering & Technology

# ELEVATING INFORMATION SECURITY IN IOT COMMUNICATIONS WITH A HYBRID APPROACH

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

## ABSTRACT

*The Internet of Things (IoT) is a concept that encompasses a network of interconnected items, including as household appliances, physical objects, and cars. These devices are equipped with software, sensors, electronics, and network connectivity, enabling them to establish connections and facilitate the exchange of data. The transmission of data between devices via the internet is facilitated by use of Internet Protocol (IP) addresses. The Internet of Things (IoT) is still in its nascent phase. In the next years, it is anticipated that there will be a significant impact on our daily lives. As the integration of becomes more pervasive within our daily routines, the corresponding risk of its potential abuse amplifies. Ensuring robust data protection measures during data transfers is of utmost importance. This research study presents a novel hybrid encryption technique called HAR (Hybrid AES Rail Fence) that aims to enhance the security of data transmission among IoT devices. The Encryption method being suggested offers a high level of secrecy, preventing attackers from deciphering the encrypted text. Furthermore, it demonstrates superior performance when compared to traditional encryption algorithms.*

*Keywords: Internet of Things, security, encryption, decryption*

## 1. INTRODUCTION

The emergence of the IoT is occurring at a significant juncture, driven by the fast advancements in embedded technology, computer technology, mobile communication networks, and the Internet. The fundamental characteristics of the IoT include the ability to perceive and comprehend data on a global scale, provide dependable transmission, and facilitate intelligent analysis and manipulation of information. It is crucial to acknowledge the dynamic exchange of information that occurs between people and machines, as well as between different machines. The IoT has had significant global implications since its inception, since substantial investments in research and development have been made, yielding noteworthy outcomes. The sector has seen substantial transformations due to the fast expansion of the IoT, which is often regarded as the third wave of the global information industry, after the advent of computers and the Internet. Smart gadgets have become pervasive in contemporary society. The advent of the Internet of Things (IoT) paradigm has led to a significant increase in the use of smart, diverse networked devices and applications. The Internet of Things (IoT) is a rapidly expanding network characterized by increasing complexity. In this context, blockchain technology has emerged as a significant catalyst for the IoT, primarily due to its decentralized nature and its ability to boost security and enable the accommodation of many devices inside the IoT paradigm [1]. Both possess the capacity to convert abstract ideas into tangible outcomes and provide novel prospects for the creation of sophisticated and safeguarded applications. The Internet of Things (IoT) has gained significant traction across several sectors, including supply chain management, agriculture, farming, transportation, insurance, and health. However, the widespread implementation of IoT has also exposed several prominent security vulnerabilities, leading to a surge in recent cyber assaults [2]. The security needs of an Internet of Things (IoT) network are mostly dependent on the particular applications it facilitates. Each application has its own unique set of security requirements, including but not limited to the need for privacy, data integrity, and user authentication. In order for the IoT to function properly, authentication has been identified as a crucial need.The establishment of trust among the many devices involved in an IoT network is of paramount importance for ensuring the smooth operation and effectiveness of the network. The potential for a single hacked node to exhibit malicious behavior and subsequently disrupt the whole system or induce catastrophic events is a significant concern[3][4].

In contemporary times, the IoT has garnered significant attention from scholars, researchers, and business professionals due to its ability to provide novel services across several domains[5][6][7]. The IoT facilitates the seamless interconnection of diverse devices and things, resulting in the establishment of a physical network. Within this network, the activities of sensing, processing, and communication are autonomously controlled and managed, eliminating the need for human involvement. The emergence of smart homes, smart cities, and other intelligent technologies has propelled the IoT into a domain of significant impact, prospects, and advancement. It is projected that the number of interconnected devices will exceed 50 billion by the year 2020[8]. Various network technologies, such as Wireless Sensor Networks (WSNs), Machine-to-Machine (M2M), and Cyber-Physical Systems (CPS), have been recognized as essential components within the wider context of the IoT in scholarly literature. As a result, the IoT has security challenges in relation to WSN, M2M communication, and CPS[9][10]. These challenges stem from the use of the standard IP network protocol, which necessitates safeguarding the whole network infrastructure against potential security breaches. In addition, it is important to note that malevolent assaults have the potential to impede the functionality of IoT services, so posing a significant threat to the security of data, the privacy of users, and the overall secrecy of the network.The existing issues pertaining to security in the Internet of Things (IoT) are shown in Figure 1. The aforementioned factors, including data integrity, security, privacy, automation, updating, a common framework, and encryption capabilities, are identified as the primary concerns.


**Figure 1:** Recent security challenges in IoT

## 2. REVIEW OF LITERATURE

**Sharma et al.,(2023)[11]**examined that one of the cutting-edge methods now available for protecting consumers' private information is blockchain technology. Blockchain technology is essential in several fields, including AI, supply chain management, and many more besides. Its numerous cutting-edge qualities, like anonymity, decentralization, security, and privacy, are all to the advantage of the healthcare sector. The healthcare sector's application software also has two-way communication with the IT sector, and IoT devices are connecting with healthcare networks. Improving healthcare's security, privacy, openness, and efficiency, blockchain-based IoT solutions have opened up new avenues for business. In addition, there are other security and privacy issues plaguing conventional healthcare institutions, including as phishing, masquerades, and identity theft. To that end,

we propose a Proposed Application (PA) built on blockchain technology for the issuance, storage, and verification of medical credentials. Using the idea of smart contracts, it also assures a number of security aspects, such as privacy, authentication, and permission management. Analyses of the suggested work's performance and comparison to current systems demonstrate its superiority.

**Ganeshan et al., (2023)[12]**analyzed that blockchain technology has been identified as a viable solution for safeguarding data inside WSNs. The conventional authentication system is dependent on the presence of trusted third parties, a condition that is not often feasible in the context of WSNs. Consequently, this limitation gives rise to a single-point failure scenario within the WSN paradigm. Occasionally, the authentication procedure exhibits reduced speed, leading to a detrimental impact on the user's overall experience. Consequently, people tend to gravitate towards alternative solutions that include the option of multi-factor authentication. In order to address these challenges, a robust identity key and authentication framework is developed using a hybrid blockchain system inside a multi-WSN environment, hence augmenting the security of the system. The nodes inside the network collaborate to execute designated activities, whereby the interaction among nodes guarantees the validation of each node's identification. The use of hybrid blockchain technology involves the authentication and storage of nodes' identification information inside the network subsequent to verification. This process facilitates the establishment of communication channels between ordinary nodes, as well as between ordinary nodes and end users. The suggested methodology demonstrates enhanced security via reduced computing time, increased detection rate, and restricted memory use of 0.072 seconds, 92.48%, and 3.925 megabytes, respectively. The efficacy of the implemented authentication technique has been shown in its ability to withstand various network assaults.

**Alghamdi et al., (2023)[13]**stated that the term IoT is used to describe the global system of products that are linked together and enabled for online interaction and data exchange. There are significant security concerns for the communication of smart devices due to their growing usage inside IoT networks. Because of its decentralized and distributed nature, blockchain technology may provide answers to these problems via its use in consensus-based authentication for IoT networks. The approach makes use of clustering to set up a local-global architecture, with cluster chiefs being in charge of authorization and authentication on their respective nodes. A local private blockchain makes it easier for cluster leaders to talk to relevant base stations. By increasing network authentication efficiency and bolstering security, this blockchain application improves trustworthiness. The suggested approach has been shown to improve upon previously published techniques in simulation. The suggested model outperformed the baseline models with an average coverage per node of 0.90. In addition, compared to more conventional global blockchain techniques, the lightweight blockchain architecture suggested in this study displays improved capabilities in attaining balanced network latency and throughput.

**Sharma et al., (2022)[14]**examined that two areas of the IT business that are seeing rapid growth are blockchain and the Internet of Things. Supply chain management, logistics, and the automotive industry are just a few of the numerous fields that may benefit from these two developing spheres. Users' medical records are often kept in a centralized third-party organization, such a clinical repository or a cloud computing environment, due to the limited computational capabilities and storage capacity of IoT devices. As a result, it is common to see that individuals feel powerless in the face of a centralized barrier and security risks associated with their personal health data. Improving the data transfer process while adding security measures requires a cutting-edge solution. The healthcare industry stands to benefit greatly from the combination of blockchain and the IoT.This impact manifests via enhanced operational efficiency, heightened security measures, increased transparency, and the creation of new avenues for economic growth. Efficient exchange of Electronic Health Records (EHR) has the potential to enhance several aspects of healthcare, including the treatment process, accuracy of diagnoses, as well as security and privacy measures. This article presents a proposal for an IoT architecture that utilizes blockchain technology to increase the security of healthcare data. Numerous tests are conducted to assess the efficacy of the suggested methodology. The findings indicate that the suggested approach outperforms established schemes already in use.

**Pant et al., (2022)[15]**studied that the global world is progressing towards a novel era characterized by digitalization, wherein one may find some of the most potent technologies ever seen in the annals of human civilization. The advent of these technologies has enabled humanity to manifest items that were once confined to the realm of fairy tales. This study presents a theoretical framework that incorporates the most recent and very influential technologies of the current decade. This research endeavor included the integration of the 5G network with the Industrial Internet of Things (IIoT), a system grounded on artificial intelligence, with the objective of creating an intelligent machine that had the ability to imitate human behavior. This system has significant capabilities, but it is also susceptible to many issues such as hacking and cyber-attacks. The solution to this issue is addressed via the use of blockchain technology. The study incorporates blockchain technology into the existing model in order to enhance its security and efficiency. By using a decentralized system, blockchain ensures transparency inside the model. Previous studies have examined the integration of blockchain technology with the IoT. However, this study represents an enhanced iteration that incorporates the industrial IoT, using the capabilities of Artificial Intelligence (AI) to enable intelligent decision-making inside the realm of IoT.

**Latif et al., (2022)[16]**analyzed that the IoT is a rapidly developing technology that serves as a foundation for CPSs in the manufacturing sector. It has begun to play a role in nearly all aspects of our daily lives, from commerce to health care, from communication to national security, from the battlefield to the smart home, and so on. Yet, there are also problems associated with the widespread implementation of IoT. These include problems with compatibility, reliability, heterogeneity, enormous amounts of data, processing of diverse information, etc. The most pressing problems are energy efficiency and security. Information exchange over the edge or IoT network is hampered by the limited computational power of IoT devices. Interference with IoT data, whether accidental or malicious, may be quite worrying. In this research, the author takes use of blockchain's potential advantages by integrating it with SDN, all the while providing a rationale for the associated energy and security concerns. In order to improve routing in IoT networks, the researcher suggested a novel protocol based on a cluster structure and a blockchain-based SDN controller architecture. The suggested architecture eliminates the need for proof-of-work (PoW) in P2P communication between SDN controllers and IoT devices by making use of both private and public blockchains. In addition, blockchain's distributed trust-based authentication approach increases its usability for low-power IoT gadgets. The findings from experiments verify that the proposed cluster structure-based routing protocol provides better performance than the current best practices. The proposed protocol aids in solving the problems associated with the future generation of industrial cyber physical systems, most notably those associated with energy management and security.

**Khanna et al., (2021)[17]**in contemporary times, there has been a prevailing trend in the adoption of wireless communication systems via the implementation of a fixed spectrum allocation policy. This policy entails the distribution of wireless spectrum to licensees by administrative bodies, often on a long-term basis, with a focus on expansive geographical coverage. Cognitive radio networks (CRN) are anticipated to provide a substantial increase in bandwidth allocation for mobile users. Nevertheless, CRN networks present significant hurdles arising from security concerns and spectrum management considerations. Therefore, this study presents a novel approach to enhancing security and spectrum sensing in cognitive radio networks (CRNs) via the use of blockchain technology. The proposed technique aims to effectively manage the spectrum allocation while also identifying and mitigating the presence of harmful users inside the network. Spectrum sensing is an essential need in CRNs that may be significantly impacted by the presence of malevolent users. The malevolent individual is engaging in an assault on the overall signal detecting capabilities of the network, so disrupting the precision of the system's functioning. The presence of a malevolent user inside a CRN result in the transmission of inaccurate sensing data, hence diminishing the overall performance of the system. The CRN network utilizes blockchain technology to enhance security and spectrum sensing, hence improving the overall performance of the system. An Adaptive threshold spectrum energy detection technique is used in the identification of malevolent users in the CRN via the utilization of a blockchain-based approach. The method under consideration has been implemented using the

MATLAB software platform. The suggested technique is evaluated in comparison to current methods, namely Friend or Foe and Tidal Trust Algorithm.

**Rahman et al., (2021)[18]**evaluated that both Software-Defined Networking (SDN) and the Blockchain have emerged as dominant technologies for ensuring secure network communication and infrastructure. Security, privacy, adaptability, scalability, and secrecy are just some of the dangers and obstacles they help you overcome with their solid and dependable platform. Based on these premises, this article introduces a Blockchain-based software-defined IoT architecture for smart networks that is both energy-efficient and safe. Across the IoT ecosystem, SDN and Blockchain technologies have shown to be capable of managing resources effectively and developing secure network communication. Nevertheless, there is a scarcity of research that sufficiently delineate a framework capable of meeting the requirements of the Internet of Things (IoT) ecosystem, namely in terms of low power consumption and minimum end-to-end latency. In this research, we propose a hierarchical design that facilitates the deployment of a decentralized Blockchain-enabled SDN-IoT framework. This architecture ensures efficient cluster-head selection and secure network communication by effectively detecting and isolating malicious switches. Furthermore, the flow-rules record offered by Blockchain technology serves the purpose of monitoring the rules imposed by switches, so ensuring consistency throughout the whole controller cluster. The evaluation of the proposed framework's performance is conducted in a simulated environment. Through this evaluation, we show that the framework exhibits superior capabilities in optimizing energy usage, end-to-end latency, and throughput when compared to baseline methods.

**Hui et al., (2020)[19]**intended thatIoT in industry exemplifies the current trend in the development of factories and is a necessary component for the production of intelligent factories. It is of the utmost need to make certain that the data transmissions in the context of industrial Internet of Things (IoT) are kept secure. The key contribution made by this research is the implementation of an innovative chaotic safe communication approach with the goal of reducing the risks associated with data transfer security. The proposed method focuses on the study of the synchronizing of fractional-order chaotic systems that have a variety of topologies and orders. In order to achieve synchronicity between the fractional-order drive system and the response system, the usage of the Lyapunov stability theory is utilized. The n-shift encryption idea is used to carry out the practice of encrypting and decrypting the principal data signals before they are sent over the network. The key space of the scheme is computed and examined. The efficiency of the theoretical method we have provided is shown by the use of numerical simulations.

**Al Hayajneh et al., (2020)[20]**examined that the use of IoT has seen a notable surge, garnering significant attention due to its widespread adoption across several domains. The prioritization of expeditious introduction of new Internet of Things (IoT) goods in the market sometimes leads to the neglect of security considerations, as the comprehensive examination of potential vulnerabilities requires a significant amount of time. Given that Internet of Things (IoT) devices operate via internet connectivity and handle sensitive and secret data, there has been a growing apprehension over security. Consequently, several researchers are actively investigating various approaches to enhance the security measures used in these devices. Therefore, the use of SDN presents a clear and evident resolution for enhancing the performance of IoT networks and addressing the existing limitations. This paper introduces a system model that aims to optimize the utilization of SDN in IoT networks. Additionally, a solution is proposed to address the challenge of mitigating man-in-the-middle attacks specifically targeting IoT devices that are limited to using the HTTP protocol. These attacks pose a significant threat and are notoriously difficult to defend against. The results of our system deployment and assessments demonstrate that the suggested approach exhibits greater resilience against cyber-attacks.

## 3. RESEARCH METHODOLOGY

The AES standard implementation is responsible for carrying out the process of key creation. The AES and Rail Fence ciphers are combined in order to carry out the process of hybrid encryption.

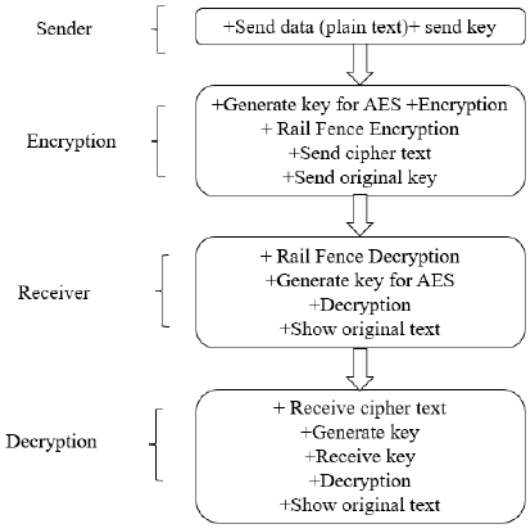


**Figure 2:** Flow diagram

As the number of rounds is raised by the integration of two encryption standards, the task of decrypting the original message becomes more difficult for potential intruders. The flow diagram shown in Figure 2 illustrates the suggested HAR concept. The primary motivation for proposing the HAR encryption standard, despite the existence of a superior encryption standard like AES, is due to the fact that AES employs a uniform encryption method for each block and has a straightforward algebraic structure. The algebraic structure of HAR is characterized by a certain level of complexity. This complexity is further enhanced by the implementation of dual encryption, which significantly increases the difficulty for unauthorized individuals to decipher the encrypted data."

### 3.1 Proposed HAR Model

The HAR (Hybrid AES Rail Fence) implementation involves the dual encryption of the input plaintext. After the encryption process is performed using the Advanced Encryption Standard (AES), the resulting output will thereafter serve as the input for the Rail Fence algorithm. The Rail Fence algorithm is used once again to encrypt the resulting output of the Advanced Encryption Standard (AES). Therefore, dual encryption occurs. The flow of work goes like:

1. Giving the plain text as input to AES
2. Key generation process
3. Sub bytes and shift row process
4. Mix columns and add round key process
5. Cipher text generated by AES encryption
6. Cipher text from AES becomes input to Rail fence
7. Cipher text will be generated as a part of Rail fence encryption.

The input for the AES encryption algorithm will consist of the original message, which is provided as plain text. The key generation procedure for AES, which offers key lengths of 128, 192, and 256 bits, is performed by the block cipher. Following the key creation procedure, the further stages to be executed include sub bytes, shift rows, mix columns, and add round keys. As a result of using the AES encryption algorithm, a cipher text will be

produced. The cipher text acquired will be used as input for the rail fence algorithm, which will then execute encryption once again, resulting in a double encryption of the original plain text."

The flow chart shown in Figure 3 illustrates the workflow of HAR, commencing with the first input of plain text. It demonstrates the process by which the plain text is transformed into cipher text via the use of AES encryption. Additionally, it showcases the integration of Rail Fence cipher, resulting in the occurrence of dual encryption.

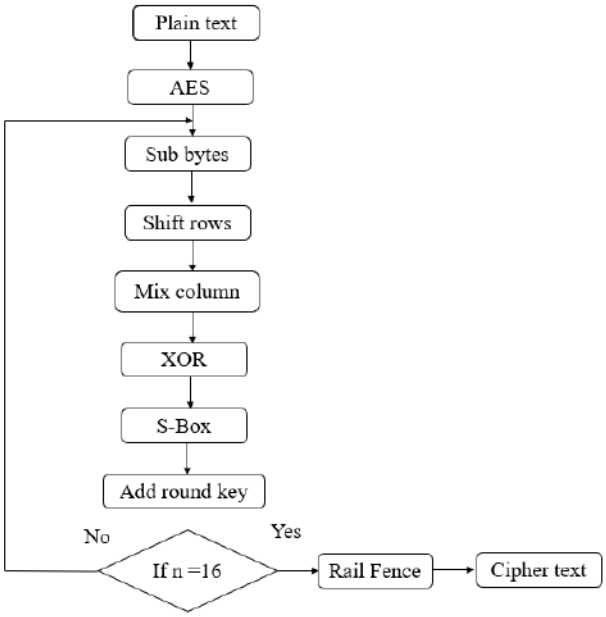


**Figure 3:** Flow of work

In the HAR encryption standard, the subsequent procedure after the completion of the encryption process performed by AES involves using the result of AES as the input for the Rail Fence cipher. The Rail Fence cipher is a transposition cipher that rearranges the letters of a word in a zigzag pattern, offering a straightforward and practical method. The task of deciphering the original message becomes challenging due to the use of the rail fence cipher, which leverages the robustness of the encryption key to safeguard the message. In the rail fence cipher, spaces are included as part of the encryption process. "

**Encryption:**Rail fence encryption is a technique whereby the characters of the original message are rearranged in a zigzag pattern across the page, and afterwards read row by row. Firstly, it is necessary to establish the key, which refers to the depth of the rail fence and determines the number of rows to be used. The writing process will start by forming the letters in a diagonal fashion, proceeding downwards and to the right until the desired number of rows is achieved. Subsequently, the direction will shift to an upward diagonal trajectory until the first row is once again reached. This procedure continues until the simple text reaches its end point.

For instance, consider

Plain text = "EDUCATION"

Key = 2

Cipher Text = "EUAINDCTO"

**Decryption:**The decryption method involves the use of the diagonal grid, which is employed for encrypting the message. The first step involves constructing a grid with a number of rows according to the length of the key, and a number of columns equivalent to the length of the cipher text. Next, the first letter is positioned in the upper left

square, and thereafter, it is moved diagonally downwards while inserting the following characters. This process continues until the top row is reached again. This procedure continues until an ending is reached."

### 3.2 HAR Analysis

The evaluation of the HAR encryption standard is conducted by considering key factors such as diffusion and the avalanche effect. The concept of diffusion pertains to the characteristic whereby the statistical redundancy present in the plaintext is dispersed across the statistical properties of the ciphertext. The unevenness in the arrangement of individual letters within the original text should be reorganized to create an uneven distribution of bigger parts within the encrypted text, making it more challenging to discern. The cryptographic robustness of a method is contingent upon the characteristic known as diffusion. In the event of a little alteration in the input, the resulting output will undergo a substantial transformation, even if the modification in the input is limited to a single bit change. The term "avalanche effect" is used to describe this phenomenon. The calculation of the avalanche effect will be performed using a quantity known as the Hamming distance. The Hamming distance is often computed by performing a bitwise XOR operation on each corresponding bit, and then summing the resulting values. This approach is commonly used due to its ease of implementation and programming. A significant level of diffusion is required. This observation suggests a significant level of avalanche effect, which serves as an indicator of the effectiveness of the cryptographic method.

In general avalanche effect is calculated using formulae

[Avalanche effect = Hamming distance/File size]

The hamming distance is often defined as the count of differing bits between two binary strings. The purpose of using encryption techniques is to obfuscate any discernible disparities in the plaintext from unauthorized individuals who only have access to the ciphertext.The rate of dissemination of information is solely determined by the avalanche effect parameter.

Among the several encryption standards available, the Advanced Encryption Standard (AES) has been extensively studied and shown to possess a notable degree of diffusion. This is evidenced by its ability to display a high avalanche effect, which is a desirable characteristic in cryptographic algorithms. TheHAR is characterized by a greater number of rounds, resulting in a substantial alteration in the output when a single bit manipulation occurs in the plain text. This phenomenon is known as the high avalanche effect. As a result of this characteristic, data may be maintained in a secret manner, hence augmenting security measures.

## 4. RESULT AND DISCUSSION

According to the bar plot shown in Figure 4, our implementation of HAR exhibits a significant level of diffusion, leading to a pronounced avalanche effect. This finding suggests that HAR outperforms existing encryption algorithms such as DES, RSA, Blowfish, and several others. Increased rates of diffusion have been seen to enhance the security of data by obfuscating the variations in plain text, so impeding unauthorized individuals from deciphering the original message, since they are only able to perceive the cipher text.

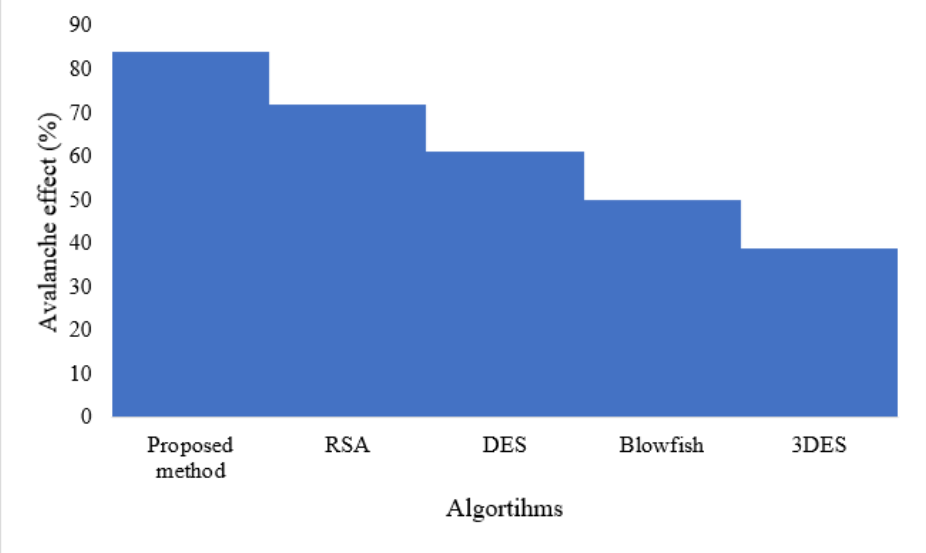


**Figure 4:** Avalanche effect for different encryption standards.

## 5. CONCLUSION

This work presents a novel hybrid encryption strategy that combines the Advanced Encryption Standard (AES) with the Rail Fence algorithm. The aim of this approach is to bolster security in a range of real-time applications, including the protection of account passwords and the secure transmission of messages containing secret words exclusive to bank account users (one-time passwords, or OTPs), among others. When compared to the conventional AES algorithm, this hybrid technique exhibited a significant increase in the avalanche effect. The HAR model offers enhanced security via the use of a diffusion strategy, which increases the difficulty involved in identifying data.

## REFERENCES

[1]. Zhou, Junlong, Yufan Shen, Liying Li, Cheng Zhuo, and Mingsong Chen. "Swarm intelligence based task scheduling for enhancing security for IoT devices." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2022).

[2]. Kalyani, G., and Shilpa Chaudhari. "An efficient approach for enhancing security in Internet of Things using the optimum authentication key." *International Journal of Computers and Applications* 42, no. 3 (2020): 306-314.

[3]. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805.

[4]. El-Hajj, Mohammed, Maroun Chamoun, Ahmad Fadlallah, and Ahmed Serhrouchni. "Analysis of authentication techniques in Internet of Things (IoT)." In *2017 1st Cyber Security in Networking Conference (CSNet)*, pp. 1-3. IEEE, 2017.

[5]. Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "Integration of blockchain and cloud of things: Architecture, applications and challenges." *IEEE Communications surveys & tutorials* 22, no. 4 (2020): 2521-2549.

[6]. Ellouze, Fatma, Ghofrane Fersi, and Mohamed Jmaiel. "Blockchain for internet of medical things: a technical review." In *The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020, Hammamet, Tunisia, June 24–26, 2020, Proceedings 18*, pp. 259-267. Springer International Publishing, 2020.

[7]. Yaqoob, Ibrar, Khaled Salah, Muhammad Imran, Prem Prakash Jayaraman, and Charith Perera. "The role of big data analytics in industrial Internet of Things." *arXiv preprint arXiv:1904.05556* (2019).

[8]. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future generation computer systems* 82 (2018): 395-411.

[9]. Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." *IEEE Signal Processing Magazine* 35, no. 5 (2018): 41-49.

[10]. Al Shahrani, Ali M., Ali Rizwan, Manuel Sánchez-Chero, Carmen Elvira Rosas-Prado, Elmer Bagner Salazar, and Nancy Awadallah Awad. "An internet of things (IoT)-based optimization to enhance security in healthcare applications." *Mathematical Problems in Engineering* 2022 (2022).

[11]. Sharma, Pratima, SuyelNamasudra, Ruben Gonzalez Crespo, Javier Parra-Fuente, and Munesh Chandra Trivedi. "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain." *Information Sciences* 629 (2023): 703-718.

[12]. Ganeshan, Arulkumaran, Santhosh Jayagopalan, Balamurugan Perumal, and Velliangiri Sarveshwaran. "Secure identity key and blockchain-based authentication approach for secure data communication in multi-WSN." *Concurrency and Computation: Practice and Experience* (2023): e7861.

[13]. Alghamdi, Saleh, AiiadAlbeshri, and Ahmed Alhusayni. "Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager." *Electronics* 12, no. 17 (2023): 3721.

[14]. Sharma, Pratima, Nageswara Rao Moparthi, SuyelNamasudra, Vimal Shanmuganathan, and Ching-Hsien Hsu. "Blockchain-based IoT architecture to secure healthcare system using identity-based encryption." *Expert Systems* 39, no. 10 (2022): e12915.

[15]. Pant, Piyush, Anand Singh Rajawat, S. B. Goyal, Pradeep Bedi, Chaman Verma, Florentina Magda Enescu, Maria Simona Raboaca, and Traian CandinMihaltan. "Blockchain for AI-Enabled Industrial IoT with 5G Network." In *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1-4. IEEE, 2022.

[16]. Latif, Sohaib A., Fang B. Xian Wen, Celestine Iwendi, F. Wang Li-Li, Syed Muhammad Mohsin, Zhaoyang Han, and Shahab S. Band. "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems." *Computer Communications* 181 (2022): 274-283.

[17]. Khanna, Ashish, Poonam Rani, Tariq Hussain Sheikh, Deepak Gupta, Vineet Kansal, and Joel JPC Rodrigues. "Blockchain-based security enhancement and spectrum sensing in cognitive radio network." *Wireless Personal Communications* (2021): 1-23.

[18]. Rahman, Anichur, Md Jahidul Islam, Antonio Montieri, Mostofa Kamal Nasir, Md Mahfuz Reza, Shahab S. Band, Antonio Pescape, Mahedi Hasan, Mehdi Sookhak, and Amir Mosavi. "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot." *IEEE Access* 9 (2021): 28361-28376.

[19]. Hui, Hongwen, Chengcheng Zhou, Shenggang Xu, and Fuhong Lin. "A novel secure data transmission scheme in industrial internet of things." *China Communications* 17, no. 1 (2020): 73-88.

[20]. Al Hayajneh, Abdullah, Md Zakirul Alam Bhuiyan, and Ian McAndrew. "Improving internet of things (IoT) security with software-defined networking (SDN)." *Computers* 9, no. 1 (2020): 8.