# Blockchain-Inspired Lightweight Dynamic Encryption Schemes for a Secure Health Care Information Exchange System

**Etikala Aruna**
VELS Institute of Science, Technology & Advanced Studies, India
arunae.phd@velsuniv.ac.in (corresponding author)

**Arun Sahayadhas**
VELS Institute of Science, Technology & Advanced Studies, India
arun.se@velsuniv.ac.in

*Received: 31 March 2024 | Revised: 22 April 2024 | Accepted: 1 May 2024*

 *DOI: https://doi.org/10.48084/etasr.7390*

## ABSTRACT

**The telemedicine sector has entered a new phase marked by the integration of Internet of Things (IoT) devices to identify and then send patient health data to medical terminals for additional diagnostic and therapeutic procedures. Today, patients can receive prompt and expert medical care at home in comfortable settings. Due to the unique nature of these services, it is essential to verify patient healthcare data, as it contains a greater amount of personal information that is vulnerable to privacy violations and data breaches. Blockchain technology has attracted interest in addressing security concerns due to its decentralized, immutable, shared, and distributed characteristics. This study proposes lightweight dynamic blockchain-enabled encryption schemes to secure physiological data during authentication and exchange processes. The proposed scheme introduces the logistic Advanced Encryption Scheme (AES) that combines chaotic logistic maps to secure the data in the blockchain network and mitigate different attacks. The model was deployed on the Ethereum blockchain and performance metrics, such as computation and transaction time, were calculated and compared with other current blockchain-inspired encryption models. Furthermore, the NIST test was conducted to prove the strength of the proposed scheme. The proposed model exhibits high security and a shorter transaction time (0.964 s) than other existing schemes. Finally, the proposed model generates high-dynamic keys that are suitable for defending against unpredictable attacks on blockchain.**

***Keywords-telemedicine; Internet of things; Logistic AES; Etherum blockchain; NIST; authentication; exchange process***

## I. INTRODUCTION

With the growing demand for IoT, telemedicine has changed and entered a brand-new application stage. Telemedicine, with the integration of IoT devices, plays a vital role in transmitting physiological data to medical terminals for follow-ups, health guidance, and clinical treatment [1-3]. Reducing the number of in-person hospital visits facilitates prompt and expert advice while also reducing medical care costs. Given that healthcare data are more sensitive than other data types, there is a greater chance of security holes and issues with data privacy. Many standard encryption algorithms, such as AES, RCA [4], ECC [5], and DES [6], are used to protect the data against various attacks. However, security threats persist, making the data vulnerable to different attacks.

Blockchain [7] provides a technology to address security concerns in the storage of patient clinical data. Blockchain is a ledger that records all the information about transactions among users. It is a decentralized ledger and does not have any central authority. In any case, information cannot be deleted or modified once it has been added to the ledger. Thus, it is cryptographically highly secure and immutable. This technology is a consensus-based framework, meaning that all nodes verify every transaction and consent before placing it in the ledger. Thus, it seems to be a better solution for security-related and privacy issues. Due to its dynamic properties, blockchain is widely used in healthcare for viable and secure transmission of medical images. It can significantly reform clinical medical care frameworks and provide security between communication devices.

Although blockchain offers more data security and privacy, computational complexity and integrated strong defensive encryption schemes remain real challenges. This study proposes a lightweight blockchain-inspired AES encryption scheme to protect data against multiple attacks during the authentication process, making the following contributions:

- A lightweight blockchain-inspired architecture for a patient-centric method to provide a strong security framework to mitigate different attacks is proposed.
- A logistic-influenced AES encryption scheme is incorporated to achieve the highest form of security against multiple attacks.
- The proposed system is implemented on the Ethereum blockchain and its functionality is assessed by comparing it with existing encryption schemes. The experimental data show that the proposed encryption architecture works better than the existing ones.

## II. BACKGROUND WORK

### *A. Advanced Encryption Scheme (AES)*

AES is a commonly used cryptographic method that uses symmetric ciphers to provide the highest level of security. AES is easy to deploy (hardware and software) and offers robust security features. AES has become a competitive option to address security issues in IoT-based medical equipment due to its effective implementation. AES is one of the most widely used and consistently reliable encryption algorithms. As technology advances, novel and innovative modification techniques have been developed and applied to improve AES. Today, it is commonplace to encounter intruders and unauthorized access to information. Chaos-based privacy has been a promising approach in security research, due to its unpredictable nature. It might be challenging for the user to locate the right key if he lacks prior knowledge of the original conditions. Chaos-based cryptosystems are more flexible for handling large amounts of data, including audio and video. Many efforts have included chaotic elements in existing cryptosystems [8-10]. Therefore, AES may be safer if key generation is performed using a chaos-based approach.

### *B. Chaos-Based Encryption Schemes*

Chaos theory focuses on the behavior of dynamic, non-linear systems that are highly sensitive to beginning conditions. As a result, a substantial change in output is caused by a minimum change in the beginning conditions [11]. The starting condition's sensitivity is tested using Lyapunov exponents. The positive Lyapunov is a symptom of chaotic conditions. This crucial characteristic increases output unpredictability, encouraging many research efforts to employ chaotic systems in cryptographic encryptions [12]. Besides Lorentz maps, logistic maps are predominantly used for encryption to achieve lightweight and highly secured data transmission.

### *C. Blockchain Mechanism*

Because of its flexible structure and advantages, blockchain has become a reliable method in cryptosystems and other industries. Blockchain was developed for cryptocurrencies to track and avoid third-party transactions [13]. These days, it is used in a wide range of real-time applications, including medical, industry 4.0, automotive, energy trading systems, smart cities, industrial IoT, safe communications, cryptosystems, etc. The design of the blockchain is akin to a peer-to-peer network made up of nodes, or blocks, that have been assigned hashes. Every block is an example of a digital ledger that contains historical information derived from earlier network transactions. Every piece of information on the blockchain is permanent and unchangeable. Figure 1 shows the elements of the blockchain architecture, which is made up of blocks.

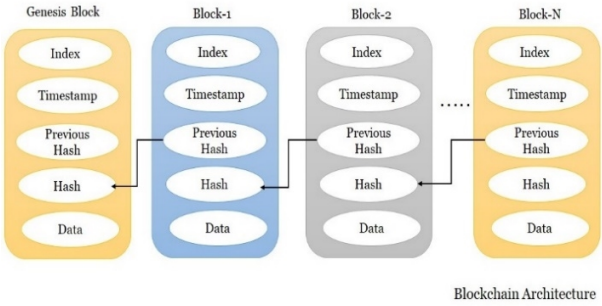


Fig. 1. The basic structure of the blockchain technology.

In this structure, the initial block is and will always be the genesis node. Every block contains the following constant features: data, hash, index, timestamp, and prior hash. Since every block has a timestamp, changing the data would be almost strange. The two most important block topographies that are updated for each transaction or change in data within the block are the current and prior hashes. As a result, every block that is attached to the network is given a chain structure. A blockchain configuration resembles a decentralized system that includes every node and its data. These blocks are smart contracts that are self-executing programs to prevent fraud. Blockchain technology falls into two important categories: public and private networks. Commercial examples of public blockchain networks are Ethereum and Bitcoin.

## III. RELATED WORKS

In [14], pediatric chest X-ray images were used to detect pneumonia. The X-ray images were encrypted using three encryption algorithms, and their performance was evaluated based on execution time. After encryption, a CNN was used for image classification, employing the VGG16 transfer learning model. However, this approach is incompatible with large-scale frameworks. In [15], a secure cloud-based architecture was proposed to handle patient data collected from IoT devices and sensors. The data were safely sent to cloud storage using public key encryption. Subsequently, the predictive algorithm used real-time data to determine if the patient anticipates developing diabetes or not. Authors in [16] focused on managing large-scale data analytics using real-time data from various IoT devices while protecting their security and integrity. This framework has a generic architecture that makes it easier to collect and store heterogeneous data from various IoT devices. However, this approach cannot be used in dense networks.

In [17], a Deep Reinforcement Learning (DRL)-based data analytics framework was introduced for edge-based IoT devices to allow them to perform activities jointly by utilizing proximity and resource complementarity. Data scheduling optimization was used to optimize data input in parallel and enhance the management of overall communication overhead.

This method does not require a priori IoT node information but instead leverages DRL to maximize execution speed and accuracy. In addition, the costs of awards, failures, and average delay time were calculated. However, this framework did not address real-time data-leaking threats [18]. In [19], a novel IoT-enabled intelligent agriculture system was proposed for safe data exchange between numerous actors, taking advantage of deep learning and smart contracts. To ensure safe data transfers, this framework first created a new authentication and key management system. Then, the cloud server used a cutting-edge deep learning architecture to analyze and find other breaches using encrypted transactions. However, this approach is not appropriate for real-time settings.

## IV. THE PROPOSED FRAMEWORK

Figure 2 shows the operational architecture of the encryption model. The proposed structure operates in three stages: (i) Patient-centric Data Collection Unit (PDCU), (ii) Light-Weight Encryption System (LWES), and (iii) Blockchain implementation.

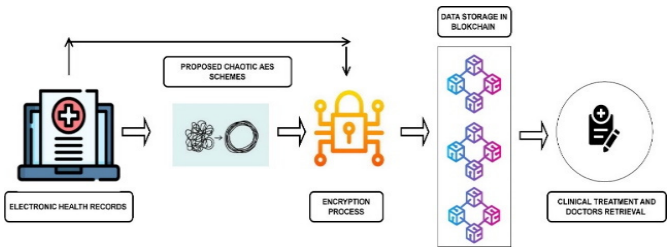


Fig. 2. Proposed framework for blockchain-enabled encryption schemes for medical health records.

Patient-Centric Data Collection Unit (PCDU): Patient data is a physiological data stream. Electronic Health Records (EHRs) are collected, encrypted, and stored on the blockchain network. Access to patient-specific information is facilitated for authorized users, and all the clinical data inside the EHR is critical to the patient's care. However, there is a greater chance that intrusion attempts will focus on EHR data that contain more sensitive information.

Light Weight Encryption Schemes (LWES): The proposed encryption system uses the AES procedures with minor adjustments. These adjustments decrease the time needed for encryption and decryption while maintaining strong protection features. Strong encryption is constructed using logistic maps. Encryption operates in two stages. In the first level, the first S-box (S1) of AES is built using three-dimensional (3D) logistic maps. The initial conditions of the second-level 3D logistic maps are constructed and used to build the hybrid S-box (S2) based on the S1 output. S3 is the hybrid S-box formed by diffusion and permutation of the two S-boxes to encrypt the data. By concurrently cutting down encryption and decryption times, this process seeks to make AES lightweight while maintaining its power to fend off attacks.

Blockchain-enabled diagnosis center: Patient data are kept in distinct databases after encryption. Additionally, encrypted data is re-encrypted and stored on the Ethereum blockchain. Once the patient's data have been successfully stored in Ethereum, the doctor uses the patient's unique ID and address to log into the blockchain. Furthermore, the proposed chaotic algorithms are used to decode encrypted data, which are then downloaded for additional clinical processing.

### A. Logistic Maps

3D logistic chaotic maps have more chaotic features than 1D chaotic maps. The mathematical equations for 3D logistic maps are:

$$X = \mu x(1 - x(i)) + \beta y'X + \alpha Z \quad (1)$$

$$Y = \mu y(1 - y(i)) + \beta x'Z + \alpha Y \quad (2)$$

$$Z = \mu z(1 - z(i)) + \beta z'y + \alpha X \quad (3)$$

where $0.35 < \mu < 0.381$, $\beta < 0.0022$, and $\alpha = 0.0015$. Figure 2 shows the proposed chaotic systems' chaos phenomena for these values.

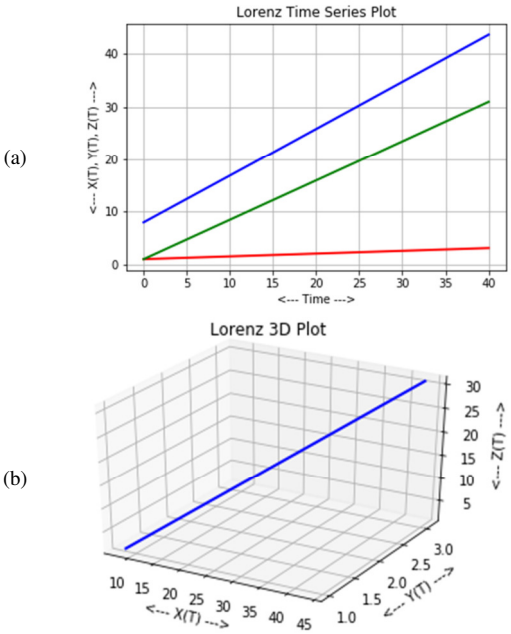


Fig. 3. Lorentz maps of 3D characteristics of the logistic maps.

### B. Encryption Process

The first step in reducing the complexity of the encryption process is to consider the placement of sensor input bytes. Logistic maps are first created at random. The intermediate S1 box is formed using the logistic maps. With the aid of the input EHR (M) and 3D logistic maps (I), the intermediate S-box is created. Diffusions and permutations are used to create a robust encryption method. Algorithm 1 shows how S1 is formulated.

$$I = 3d\ \text{logistic maps}(X, Y, Z)\ \text{for}\ J = 1, 2, \ldots, L \quad (4)$$

$$S1 = \{(I)\ \text{permutated}\ M\}\ \text{for}\ i = 0,1,2, \ldots . L \quad (5)$$

ALGORITHM 1: FORMULATION OF INTERMEDIATE S1-BOX

```
1: Input: The 3D logistic map sequences with input
   sensor bytes K
2: Output: A sizeable S1-box
```

```
3: Begin
4: As beginning conditions for 3D logistic maps,
   generate the random sequences.
5: Using (1)-(4), create the 3D logistic maps.
6: Determine the K sensor bytes' missing values and
   add zeros in their place.
7: Maps and k-bytes should be resized to 16
8: Use (5) to create the intermediate S1-box.
9: End
```

Following the formulation of the S1-box, an intermediate S2-box is generated again using 3D logistic maps (L). Again, permutation and diffusion are adopted to form the S2-box. Algorithm 2 illustrates the formulation of S2.

$$M = 3d\ \text{logistic maps}(X, Y, Z)\ \text{for}\ J = 1, 2, \dots, L \quad (6)$$

$$S2 = (\{\{L)\text{permutated M}\})\ \text{for}\ i = 0, 1, 2, \dots, L \quad (7)$$

ALGORITHM 2: FORMULATION OF S2 INTERMEDIATE BOX

```
1: Input: outgoing sequences from input or S1-box,
   bytes from sensors
2: Output: Intermediate S2-box
3: Begin
4: Create the initial conditions using the S1-box
   output sequences
5: Use (6) to generate the 3D logistic maps. Find
   the missing values in the O sensor bytes and
   replace them with zeros.
6: Maps and O-bytes should be rescaled to 16
7: Use (7) to create the intermediate S2-box.
8: Finish
```

After repeating the process multiple times, the input data and the hybrid S-box keys are formed utilizing a permutation operation, which results in the creation of strong encrypted byte values that vary by themselves each time. Algorithm 3 describes the entire S-box encryption framework. Ultimately, each of the intermediates is combined to form the new hybrid S-boxes.

$$S = S1\ \text{concatenate}\ S2 \quad (8)$$

Finally the complete encrypted data is formulated as:

$$\text{Encrypted Data} = S\ \text{permutated EHR data} \quad (9)$$

ALGORITHM 3: COMPLETE ENCRYPTION PROCESS

```
1: Input: Record EHR data input
2: Output: Encrypted data
3: Start:
4: Split the EHR data records
5: Create random 3D logistic map sequences
6  Use (1)-(4) to create the 3D logistic maps.
7  Create the intermediate S1-box using (5)
8  Use the S1-box output sequences to create the 3D
   logistic maps
9  Formulate the Intermediate S2-box
10 S-box(keys)= S1 concatenates S2
11 Equation(9) is used to construct encrypted data.
12 End
```

### C. Blockchain-Enabled Diagnosis Center

Following the encryption process, encrypted data are stored for every transaction by concatenating the transaction time stamps with them. The smart contract is enabled, and nodes verify each transaction using the GVerify algorithm. If the verification fails, the encrypted data is not stored in the chains and the transaction is discarded from the blockchain network. Then the allowed transaction is set to 1 and uploaded to the blockchain network. Verified transaction data are stored in the smart contract. Doctors can log into the blockchain network and monitor patient records by decrypting the data using the proposed schemes.

(a)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 302 | 122 | 23 | 100 | AAD | CE | 450 | 73 | 12 | 90 |
| 090 | 87 | 34 | 89 | 102 | CEE | 823 | 120 | 90 | 120 |
| 123 | 22 | 12 | AEE | 103 | 78 | 903 | 110 | 89 | 89 |
| 901 | 120 | 903 | 128 | 231 | 90 | DE2 | 64 | 192 | 74 |
| 120 | 08 | 121 | 113 | 190 | 123 | 643 | 239 | 201 | 92 |
| 112 | 92 | 902 | 103 | 120 | 190 | 232 | 112 | 139 | 102 |
| 101 | 20 | 120 | 120 | 112 | 90 | 093 | 903 | 120 | 112 |
| 89 | 12 | ACD | 112 | FEA | 110 | AED | 21 | AEA | 563 |

(b)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 282 | 903 | ACD | 893 | 903 | 902 | 536 | 532 | 902 | 997 |
| 73 | 87 | 34 | 120 | 90 | ABD | FEE | 230 | 323 | E29 |
| 233 | 560 | 234 | 90 | 89 | 92 | 124 | 90 | 67 | 90 |
| 90 | 12 | 789 | 56 | 234 | EED | DE2 | 654 | 890 | AEF |
| 345 | 06 | 089 | 74 | 90 | 23 | 32 | 89 | 340 | 231 |
| 123 | AB | 342 | 89 | 88 | 190 | 231 | AE2 | 765 | 908 |
| 34 | 89 | 090 | 90 | 45 | 112 | 342 | 3423 | 212 | 902 |
| 90 | 90 | 231 | 1234 | ABC | 754 | 909 | 743 | 90 | 432 |

Fig. 4. S-box Formation used for the encryption process (a) S1-box, (b) S2-box.

## V. IMPLEMENTATION DETAILS

The proposed framework was tested in the Ethereum blockchain ecosystem using Python 3.0 modules. The distributed apps (D-Apps) were developed and Influra APIs were used to connect with the Ethereum environment. The complete experiment was deployed in a PC workstation with an Intel i9@3.0 GHz CPU, 256 GB NVIDIA Tesla GPU, and 16GB RAM.

## VI. STATISTICAL ANALYSIS

### A. Balance Criterion (BC)

A fundamental need for S-Box testing is a balanced distribution of bits in the output sequence. This test indicates that the proposed S-Box is balanced since the numbers of zeros and ones are equal or nearly equal.

### B. Completeness Criterion (CC)

The CC is used to measure the dependency of the output bits on the input. Since the designed S-box is based on the initial conditions of dual-level chaotic maps, the generated S-box exhibits bits with high randomness as the initial conditions change. This means that slight changes in the input lead to massive changes in the output.

### *C. Avalanche Criterion (AC)*

The avalanche effect describes how a tiny change in the input bits can result in a big change in the output and is a crucial need for block encryption. Strong cipher techniques benefit from having this condition. The avalanche value falls in [0, 1]. The ideal value is 0.5, meaning that the S-box meets the requirements to pass an avalanche test. The mathematical expression for calculating the avalanche test is:

$$\text{Avalanche Criteria} = \frac{\text{No of Swap bits in Ciphers}}{\text{No of total bits in Ciphers}} \quad (10)$$

### *D. Strict Avanlache Criterion (SAC)*

The Strict Avalanche Criterion (SAC), which combines the completeness and avalanche requirements, is satisfied by the S-box if every bit in its output changes by a probability of half whenever one bit is generated. The SAC was satisfied, as the proposed S-box fulfills the requirements for this criterion.

### *E. NIST Randomness Test*

NIST statistical tests were performed on the proposed encryption system to verify the results of bit unpredictability. The test findings were all in compliance with the NIST requirements and demonstrated the robustness of the randomization defense versus network attacks. Table II displays the proposed algorithm's full NIST test performance.

TABLE I. EFFICIENCY OF THE PROPOSED ALGORITHM IN NIST STANDARD TESTING

| NIST test specification | Test result. |
|---|---|
| DFT Test | PASS |
| Run_Test | PASS |
| Long_Run | PASS |
| Frequency | PASS |
| Block_Frequency_Test | PASS |
| Frequency_MonoT | PASS |
| Overlapping_Template_of_all_One's | PASS |
| Linear_Complexity | PASS |
| Matrix_Rank | PASS |
| Lempel-ZIV_Compression | PASS |
| Random_Excursion | PASS |
| Universal_Statistic | PASS |

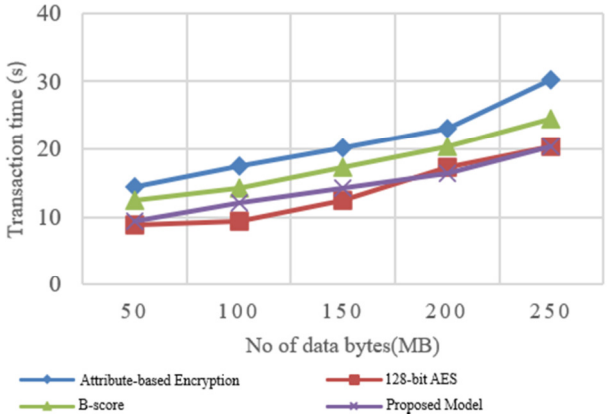


Fig. 5. Transaction time analysis for different blockchain frameworks for supported encryption schemes.

### *F. Transaction Time Analysis*

Transaction time was calculated and analyzed for increasing healthcare datasets. The transaction times of different blockchain frameworks such as Attribute-based encryption, 128-bit AES, and B-score were used for comparison, and the results are shown in Figure 5. The results in Figure 5 show that the proposed chaotic AES blockchain requires less transaction time as the data size increases, which is far better than existing blockchain-based schemes

## VII. CONCLUSION AND FUTURE WORK

This study introduced a novel lightweight blockchain-inspired encryption scheme to protect electronic health records against multiple attacks. The proposed solution encrypts healthcare data using double-layered logistic chaotic algorithms before storing them on a blockchain, therefore ensuring the confidentiality and authenticity of user information. The complete framework was developed using Python 3.19 and deployed on Ethereum. Various statistical and transaction time analyses were performed and compared with other existing frameworks. The results showed that the proposed scheme passed all statistical test analyses and required less transaction time compared to other blockchain-based encryption schemes. In the future, the proposed scheme should be further enhanced and tested against multiple attacks.

## ACKNOWLEDGEMENT

The authors want to thank the VELS Institute of Science, Technology & Advanced Studies, for supporting this research work.

## REFERENCES

[1] B. E. Dixon and C. M. Cusack, "Measuring the value of health information exchange," in *Health Information Exchange*, 2nd ed., B. E. Dixon, Ed. Academic Press, 2023, pp. 379–398.

[2] X. Liu, K. Li, G. Min, Y. Shen, A. X. Liu, and W. Qu, "Completely Pinpointing the Missing RFID Tags in a Time-Efficient Way," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 87–96, Jan. 2015, https://doi.org/10.1109/TC.2013.197.

[3] S. Jiang, J. Cao, Y. Liu, J. Chen, and X. Liu, "Programming Large-Scale Multi-Robot System with Timing Constraints," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Waikoloa, HI, USA, Aug. 2016, pp. 1–9, https://doi.org/10.1109/ICCCN.2016.7568563.

[4] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare:'MedRec' prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, 2016, vol. 13.

[5] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 276–286, Jan. 2018, https://doi.org/10.1109/TCC.2015.2491933.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, Jan. 2013, https://doi.org/10.1109/TPDS.2012.97.

[7] Y. J. Choi, H. J. Kang, and I. G. Lee, "Scalable and Secure Internet of Things Connectivity," *Electronics*, vol. 8, no. 7, Jul. 2019, Art. no. 752, https://doi.org/10.3390/electronics8070752.

[8] M. Shen, B. Ma, L. Zhu, X. Du, and K. Xu, "Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT," *IEEE*

*Internet of Things Journal*, vol. 6, no. 2, pp. 1998–2008, Apr. 2019, https://doi.org/10.1109/JIOT.2018.2871607.

[9] S. Dowling, M. Schukat, and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour," in *2017 28th Irish Signals and Systems Conference (ISSC)*, Killarney, Ireland, Jun. 2017, pp. 1–6, https://doi.org/10.1109/ISSC.2017.7983603.

[10] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017, https://doi.org/10.1109/JIOT. 2017.2740569.

[11] H. Hou, "The Application of Blockchain Technology in E-Government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, Canada, Jul. 2017, pp. 1–4, https://doi.org/10.1109/ICCCN.2017.8038519.

[12] P. Kalpana and R. Anandan, "A Capsule Attention Network for Plant Disease Classification.," *Traitement du Signal*, vol. 40, no. 5, 2023, https://doi.org/10.18280/ts.400523.

[13] Z. Shae and J. J. P. Tsai, "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, USA, Jun. 2017, pp. 1972–1980, https://doi.org/10.1109/ICDCS.2017. 61.

[14] M. Jakobsson and A. Juels, "Proofs of Work and Bread Pudding Protocols(Extended Abstract)," in Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99), Leuven, Belgium, Sep. 1999, pp. 258–272, https://doi.org/10.1007/978-0-387-35568-9_18.

[15] U. Farooq and M. F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 3, pp. 295–302, Jul. 2017, https://doi.org/10.1016/j.jksuci.2016.01.004.

[16] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *2017 21st Conference of Open Innovations Association (FRUCT)*, Helsinki, Nov. 2017, pp. 321–329, https://doi.org/10.23919/FRUCT.2017.8250199.

[17] D. Derler, K. Samelin, D. Slamanig, and C. Striecks, "Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based," in *Proceedings 2019 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2019, https://doi.org/10.14722/ndss.2019.23066.

[18] P. Kalpana, R. Anandan, A. G. Hussien, H. Migdady, and L. Abualigah, "Plant disease recognition using residual convolutional enlightened Swin transformer networks," *Scientific Reports*, vol. 14, no. 1, Apr. 2024, Art. no. 8660, https://doi.org/10.1038/s41598-024-56393-8.

[19] I. Puddu, A. Dmitrienko, and S. Capkun, "μchain: How to Forget without Hard Forks." 2017, [Online]. Available: https://eprint.iacr.org/ 2017/106.