mathematics

MDPI

Article

Cutting-Edge Amalgamation of Web 3.0 and Hybrid Chaotic Blockchain Authentication for Healthcare 4.0

Ajay Kumar [1], Kumar Abhishek [2], Surbhi Bhatia Khan [3,4,*], Saeed Alzahrani [5] and Mohammed Alojail [5]

[1] Department of Computer Science Engineering and Technology, Bennett University, Greater Noida 201310, India; ajay.kumar1@bennett.edu.in
[2] Department of Computer Science and Engineering, National Institute of Technology, Patna 800005, India; kumar.abhishek@nitp.ac.in
[3] School of Science, Engineering and Environment, University of Salford, Salford M5 4WT, UK
[4] Adjunct Research Faculty at the Centre for Research Impact & Outcome, Chitkara University, Rajpura 140401, India
[5] Management Information System Department, College of Business Administration, King Saud University, Riyadh 11362, Saudi Arabia; salhariri@ksu.edu.sa (S.A.); malojail@ksu.edu.sa (M.A.)
* Correspondence: s.khan138@salford.ac.uk

Abstract: Healthcare 4.0 is considered the most promising technology for gathering data from humans and strongly couples with a communication system for precise clinical and diagnosis performance. Though sensor-driven devices have largely made our everyday lives easier, these technologies have been suffering from various security challenges. Because of data breaches and privacy issues, this heightens the demand for a comprehensive healthcare solution. Since most healthcare data are sensitive and valuable and transferred mostly via the Internet, the safety and confidentiality of patient data remain an important concern. To face the security challenges in Healthcare 4.0, Web 3.0 and blockchain technology have been increasingly deployed to resolve the security breaches due to their immutability and decentralized properties. In this research article, a Web 3.0 ensemble hybrid chaotic blockchain framework is proposed for effective and secure authentication in the Healthcare 4.0 industry. The proposed framework uses the Infura Web API, Web 3.0, hybrid chaotic keys, Ganache interfaces, and MongoDB. To allow for more secure authentication, an ensemble of scroll and Henon maps is deployed to formulate the high dynamic hashes during the formation of genesis blocks, and all of the data are backed in the proposed model. The complete framework was tested in Ethereum blockchain using Web 3.0, in which Python 3.19 is used as the major programming tool for developing the different interfaces. Formal analysis is carried out with Burrows–Abadi–Needham Logic (BAN) to assess the cybersecurity reliability of the suggested framework, and NIST standard tests are used for a thorough review. Furthermore, the robustness of the proposed blockchain is also measured and compared with the other secured blockchain frameworks. Experimental results demonstrate that the proposed model exhibited more defensive characteristics against multiple attacks and outperformed the other models in terms of complexity and robustness. Finally, the paper gives a panoramic view of integrating Web 3.0 with the blockchain and the inevitable directions of a secured authentication framework for Healthcare 4.0.

Keywords: Healthcare 4.0; Web 3.0; hybrid chaotic keys; Ethereum; BAN; NIST; scroll; Henon maps; blockchain

MSC: 68M15

Citation: Kumar, A.; Abhishek, K.; Khan, S.B.; Alzahrani, S.; Alojail, M. Cutting-Edge Amalgamation of Web 3.0 and Hybrid Chaotic Blockchain Authentication for Healthcare 4.0. *Mathematics* **2024**, *12*, 3067. https://doi.org/10.3390/math12193067

Academic Editors: Vincenzo Vespri and Maurizio Naldi

Received: 10 July 2024
Revised: 26 August 2024
Accepted: 1 September 2024
Published: 30 September 2024

1. Introduction

Recent disruptive technologies [1] have revolutionized the things around us, and sectors such as the healthcare industry have even changed in terms of their quality and diagnosis process. Healthcare 4.0 is one such technology which began in 2016 [2–4], and its

primary intention was on wearable health systems customized for real-time deployment. Benefits from these technologies for enhanced clinical medical diagnosis and treatment processes accrue to patients as well as physicians. These disruptive technologies have also propelled the continuous remote monitoring of patients to the next dimension, in terms of reducing the latency and providing accurate prediction of severe diseases, even at the earlier stages.

The digital storage of medical records presents several advantages in the context of Healthcare 4.0; however, it also presents risks related to privacy and security [5–8]. To ensure accuracy and uphold the confidentiality of the privacy mechanism, a dependable and safe authentication framework is necessary, since these data include very important and sensitive information about patients. Most recently, blockchain technology [9–11] provides a chance to meet the security issues in storing the patients' clinical data.

Blockchain is a ledger which can record all the information about transactions among all users. It is a decentralized ledger and does not have any central authority, unlike banks [12–14]. In any case, the added information may not be erased and modified once it is added to the ledger. Hence, it is cryptographically highly secure and immutable. This technology is a consensus-based framework, which means all the nodes verify every transaction occurrence and there is consensus about all the data prior to placing into the ledger. So, it seems to be a better solution for all security-related issues [15]. Because of its dynamic properties, this technology is widely utilized for medical healthcare-based industries for the viable transmission of medical images. It can significantly reform clinical medical care frameworks and provides security among communication devices.

In recent years, the development of blockchain technology with decentralized management, traceability, and tamper-proofing features has provided new solutions for vehicle certification [7]. Using blockchain technology, vehicles can be identified securely without relying on TA (Technical analysis). At the same time, the decentralized architecture of the blockchain facilitates secure information exchange and secure information transfer on the Internet, increasing the security verification of the vehicle. However, as the speed of vehicle production increases, more and more vehicles will be connected to the network and the number of devices connected to the Internet of Vehicles will also increase. In this case, the Internet of Vehicles must operate in low-latency mode. To solve this problem, some researchers have proposed solutions using technology. Edge computing reduces communication delays and cloud overhead by distributing data processing and storage at the edge of the network [9], improves authentication performance, and reduces the dependency on RSU (road-side units). Edge computing can also be fast and improve response capacity and flexibility by storing local information [10]. In this paper, we propose a blockchain-based decentralized trusted authentication scheme to improve communication delay and improve authentication efficiency while ensuring the security of connected traffic. The main contributions of this paper are as follows. We establish a secure decentralized network model for the Internet of Cars based on blockchain, which distributes data processing and storage at the edge of the network to ensure security while reducing communication delay and TA overhead. The certification process is automatic and intelligent thanks to the combination of smart contracts and blockchain technology. At the same time, the proof is added to the blockchain ledger through a consensus algorithm to realize the reuse of authentication results and reduce the cost of effective communication. The security analysis of the project was performed using Oracle's ROR model and AVISPA tools. To verify the power of the ideas, the computational and communication costs are also analyzed in detail and validated with simulations using Sumo. The structure of this paper is as follows. Section 1 contains an introduction to this document. Section 2 reviews related work, Section 3 provides details of the design process. Section 4 includes theoretical analysis. Section 5 evaluates the performance of this method and compares it with related methods. Section 6 concludes the paper and discusses future work.

One of the main reasons is that most Web 2.0-based healthcare services still create information silos, neglect ownership by patients of their own information, and rush to

centralize the majority to help patients and members. When we share our personal health information on Web 2.0 platforms, we expect the service not to misuse our information or change our privacy policy. Unfortunately, this belief has been violated by many companies in the past. Blockchain was created to allow people who do not trust each other to agree on digital history without an intermediary. Blockchain is essentially a place where information on a ledger cannot be changed or re-altered on the blockchain, so we can now solve the problem. Smart contracts can keep applicants in check and receive payments, speed up approval times, and reduce errors. Chain tokens are earned by sharing information. Participants provide a clear view to help the researcher evaluate the data collected, ensuring that the results are more accurate, and therefore, patient care is more appropriate. It will help create new patient-centric business models that support personalized medicine and advanced clinical research. It eliminates the disadvantages of the foundation, such as lack of security and transparency. DLT distributes data over a P2P network instead of storing it in a single location. Due to its decentralized nature, it requires some form of data analysis. Examples include Bitcoin, Ethereum, and Litecoin. Although it operates similarly to public blockchain networks in terms of P2P connectivity and decentralization, it is much smaller in scale. In a private blockchain, the inventors of the network know who the participants are at the beginning. Permission-based solutions cannot be created from public networks and completely anonymous users. We can use private blockchain for voting, digital identity, ownership, and more.

Motivation

As previously noted, the use of blockchain shows promise for protecting the privacy and security of health-related data, but it also faces a number of difficulties, including slow adoption [16], attack vulnerability [17], lack of willingness to use intelligent protection computations [18], lack of robustness [19], and lack of transparency [20]. As a result, the confidence and security that are preserved for the medical information maintained in digital chains may be called into question. This research, motivated by this issue, leads to the creation of the B-WAKE-Chain, a revolutionary Web 3.0 authentication architecture that utilizes blockchain technology that is empowered with hybrid chaotic encrypted hash values, keys, and stored data, therefore enabling secure information sharing across healthcare facilities. Healthcare data handlers can profit from the findings by managing patient information in safer digital settings. The paper makes the following primary contribution:

1. A powerful cryptographic authentication mechanism between patients and medical practitioners is provided by the paper's robust blockchain architecture, powered by Web 3.0.
2. The paper proposes the incorporation of hybrid chaotic encryptions in blockchain technology to achieve the highest form of security against multiple attacks.
3. Hybrid chaotic encryptions in the blockchain: The optimization has been proposed to make the blockchain more robust, with less computational overhead. The convergence of Web 3.0 and blockchain presents an inevitable progression towards a more secure and efficient healthcare system. Future research and development efforts should focus on enhancing the scalability of blockchain solutions, integrating advanced cryptographic methods such as Elliptic Curve Cryptography (ECC), and ensuring compliance with global healthcare regulations. Additionally, exploring the interoperability between various blockchain platforms will be crucial in achieving seamless data exchange and integration across different healthcare systems.

At last, the suggested B-WAKE-Chains are implemented in the Ethereum blockchain through the use of Ganache and Infura APIs, and the results are contrasted with those of the other blockchain designs now in use. The proposed structure regularly performs better than the alternative models, according to the data from experiments.

This is the arrangement of the remaining portions of the paper. The literature review is presented in Section 2 in an understandable manner. In the third section, the suggested framework is illustrated. The experimental data, together with a comparative analysis, are

presented in Sections 4 and 5. The report concludes in Section 6 with a discussion of its potential scope.

2. Literature Review

Blockchain technology is a relatively new approach that is being applied to security applications; Shreevyas et al. [21] evaluated it. In addition to introducing blockchain technology and going over the system's structure and operation, the author also described the fundamentals of intrusion detection systems with regard to host anomaly detection and network-based anomaly detection approaches. The primary purpose of the interface between the blockchain approach and the IDS framework used in modern large-scale collaboration IDS systems is to identify malicious nodes.

Based on a property found in the smart Ethereum contract, Wang et al. [22] proposed an encryption scheme. Confidential data privacy is ensured and the key misuse phenomena are eliminated by distributing the data users' keys to the person who owns the data through this method. In order to provide maximum security when sending images across cloud platforms, Mahalakshmi and Kuppusamy [23] have developed a novel encryption technique. It is suggested that the cipher blockchain be used to improve encryption algorithms. Using a mathematical paradigm to create complicated keys, this technique removes dilemma key difficulties. So, there is a notable improvement in the encryption quality. The use of binary conversion lengthens execution times and reduces storage requirements. By processing information blocks simultaneously, time and computational complexity are decreased. Logical operations between input pictures and a higher basic matrix speed can both speed up processing. The strategy's effectiveness against different types of assaults and its superior results for RGB picture encryption are demonstrated by the findings obtained. The primary constraint is related to the computational cost of crucial transactions between the consignor and proctor. An approach to encrypt blockchain for color pictures that relies only on rotation and random permutation has been reported by [24]. The scrambling activity in this hybrid approach is based on RGB planes at certain angles. Images that have been crypto-edited can mask RGB level matrix dispersion properties and provide security against crypto-analysis. Without integrating the transfer realm so intimately, this may be carried out in a spatial area itself. With the use of a secret key, this hybrid method is accessible. Furthermore, there are no issues with it. In order to guarantee security and user privacy, the authors in [25] proposed a blockchain-connected gateway architecture. The vulnerability of [25] to many attacks, including replay, traceability, secret disclosure, and token reuse attacks, was discovered by [26] in 2020. Secure control over access and anonymity are offered by their enhanced blockchain-based authentication mechanism. Using blockchain technology, the study in [27] provided a safe architecture that enabled credentialing its issuance update, revocation, and audit capabilities by means of the implementation of a smart contract, thereby mitigating security vulnerabilities in the Internet of Things, notably in decentralized authentication.

The distributed technique of blockchain was employed by the authors in [28] to offer a multi-layer security architecture for Internet of Things gadgets running on multi-hop cellphone networks. With the help of the suggested paradigm, cellularly enabled Internet of Things networks might be secured using decentralized blockchain technology. The authors in [29] described a blockchain-based architecture to solve these problems, namely single-point-failure difficulties, after assessing the shortcomings of conventional IoT verification and safety mechanisms.

In order to address security concerns with medical pictures in medical facilities, Sultana et al. [30] have presented a paradigm that briefly describes how to decentralize a trust-less approach. With zero criteria of trust, the fussing blockchain has completed this. The modeling process is run via a decentralized web app. Users may share and save photographs with it in an efficient manner. Role-based access is ensured by this strategy, which can enhance image security. The network speed is the main drawback of this approach. It becomes tiresome on a public blockchain with many hubs since each

transaction requires distributed validation. Despite the fact that Proof of Work ensures complete decentralization, hub execution is advantageous. Furthermore, it wastes energy.

A shared design that uses the blockchain to provide non-designing practices a fictitious foundation has been put out by Habib et al. [31]. The main advantage of this strategy is that it may guarantee the system's functionality and enhance the remote picture detection application's management capabilities. This framework's main drawback is the complexity of the assignments. Relevant data are easily identifiable. You cannot tamper with it. Furthermore, there is a reasonable response time and complex structure.

Elliptic curve encryption, physical uncollapsible functions, and group signatures were coupled by the authors of [32] to propose a three-factor authentication mechanism for the Internet of Things. Though these algorithms provide strong defense against attacks, computational overhead and the mode of handling the different attacks have been ignored. Blockchain technology, known for its distributed structure and immutability, is being used to improve security in many ways. This literature review examines the integration of blockchain with security systems, focusing on access detection systems, encryption schemes, IoT, and medical imaging hearing security. Blockchain in Intrusion Detection Systems was demonstrated by Srivyas et al. [21]. This paper describes how to combine blockchain technology with IDS to detect malware in large-scale networks. Blockchain provides secure and immutable data for IDS data collection. It facilitates decentralized and transparent monitoring and detection. It uses smart contracts to increase host- and network-level visibility. In comparison with other IDS methods, traditional IDS often relies on centralized servers that can perform failover. Blockchain-based IDS ensures the following:

- Research Gap Identification: The comparison identifies gaps in previous studies, highlighting the necessity for more scalable, efficient, and comprehensive blockchain-based security solutions.
- Benchmarking: The proposed solution aims to set new benchmarks in security and efficiency by addressing the gaps found in the existing literature. The integrity of decentralized data prevents unauthorized access.

Regarding the blockchain-based encryption concept, Wang et al. [22] try to build encryption solutions based on Ethereum smart contracts. Method: Share the key with the data owner to ensure the confidentiality of sensitive data and prevent misuse. Pros: Keep data private by managing priorities. Reduce risks associated with centralized storage. Mahalakshmi and Kupusami et al. [23] propose a new encryption method to encrypt cloud data using blockchain. Method: Use complex arithmetic to generate strong keys. We recommend binary conversion to improve performance and reduce storage space. Reduce computational complexity by processing data blocks simultaneously. Comparison: Both methods improve encryption quality and security compared to existing methods. Mahalakshmi and Kuppusamy's method showed improved encryption quality but increased computational cost compared to Wang et al.'s method.

Image encryption and security research propose the use of rotation and random rotation to perform blockchain encryption of color images, as well as RGB plane-based blending. This enhanced security by hiding the RGB level matrix object. Sultan et al. [30] propose to solve the security problem of medical images stored in a distributed system. Methodology: Use blockchain to ensure responsible access and secure storage. We use a decentralized web application for efficient image sharing. Error: Network speed must be high. Power is strong due to Proof of Work. Comparison: Research in [24] focuses on cryptographic aspects and provides good protection against cryptanalysis. Sultana et al. focus on the problem of rapid job recognition, as well as on management and retention. A comparison of the surveys is shown in Table 1. Blockchain in IoT security research: Habib et al. [28] propose to establish a multi-layer security system for IoT in various network organizations. Durga R et al. [33] try to implement the secure IoT networks using the decentralized technology of blockchain. Focus on preventing a failure. The authors propose the use of blockchain to solve the insecurity of IoT. They provide a secure IoT proof architecture based on blockchain and address point errors in current mechanics.

Comparison: The two works focus on security solutions for IoT. The research in [28] targets multi-layer security, while [29] focuses on architecture robustness.

Table 1. Comparison of related surveys and findings of research gap.

Year	Study	Focus	Security Attack Classification	Solution Proposed	Security Tools Used	Application Domain	Identified Research Gap	Proposed Solution
2018	Kaur et al. [24]	Lightweight secure authentication using blockchain technology	No	Yes	No	No	Limited application scope with no consideration for advanced attacks.	Integrate advanced attack classifications for comprehensive security.
2019	Aparna et al. [2]	Blockchain-based solution for security issues	Yes	Yes	No	Yes	No in-depth exploration of practical security tools.	Utilize modern security tools like IDS and smart contracts.
2020	Saru et al. [29]	Application of blockchain in the healthcare domain	Yes	No	Yes	No	Lack of focus on lightweight cryptographic solutions specific to healthcare.	Develop lightweight cryptographic solutions with blockchain.
2021	Thakre et al. [34]	PARBAC model using privacy and authentication	No	Yes	Yes	Yes	No detailed assessment of scalability in real-world scenarios.	Include scalability assessments and performance benchmarking.
2022	Habib et al. [31]	Blockchain-based authentication protocol for WLAN in healthcare systems	Yes	Yes	No	No	Complexity of assignments and high computational overhead.	Simplify assignment processes and optimize computational efficiency.
2024	Proposed in this study	Comprehensive approach combining all of the above	Yes	Yes	Yes	Yes	Need for a unified framework addressing multiple security issues across domains.	Propose a hybrid model integrating the strengths of previous studies.

The proposed advanced encryption and authentication method of Habib et al. [31] and Yang j et al. [35] uses blockchain to enhance remote image management. Method: Provide a framework that enables efficient and advanced application management. Disadvantages: The structure and usage of data are complex. In complex networks, the response time can be very long [36]. They propose a three-step authentication mechanism for the Internet of Things. Methods: Combined elliptic cryptography, physical irreversibility, and group signatures [37].

This provides strong protection but hinders computational overhead. The authors' objective is to establish a secure blockchain encryption concept using chaos principles. The methodology for the proposed paper is to focus on low-cost, strong encryption. In comparison, Habib et al. and Kalpna P et al. [38]. focus on functionality and physical control, while emphasizing strong encryption and authentication aims to solve the computational overhead problem found in other research. Conclusion: This work demonstrates the potential of blockchain technology to improve the security of various applications. Blockchain offers a tamper-proof solution, but issues such as accounting and network speed still exist. Creating an efficient, low-cost, blockchain-inspired mutual authentication system is still an important area of research Deebak B.D et al. [39] and Cheng et al. [40]. To overcome this problem, we proposed the principles of chaos in designing the strong encryption scheme for the blockchain infrastructure. Ultimately, as far as current research indicates, developing a

robust mutual authentication system inspired by blockchain technology that can withstand repeated attacks while maintaining low computing cost is still a significant issue. Hopefully, the proposed framework can provide stronger solutions to the aforementioned problems.

3. Proposed Research Methodology

To handle blockchain transactions, the suggested B-WAKEN-Chain architecture makes use of many systems and modules. In this study, the unique symmetric and public hybrid chaotic keys may be used to authenticate electronic health records for blockchain network participants. Figure 1 presents the complete architecture of the suggested model. A patient data gathering unit, a blockchain, and doctors are just a few of the components that make up the proposed system, as seen in Figure 1. The suggested model makes use of the EH datasets. The Hospital Cloud (HC) is where healthcare data are sent for additional processing after being collected via the Internet of Things (IoT). For additional processing, the complete set of records is stored in the HC. The medical professionals are verified, and those who have been verified may view the records that are utilized for diagnosis and treatment planning [41]. Furthermore, without authorization from hospitals and patients, doctors are unable to disclose patient information. In order to safeguard information transferred over the Internet, the suggested blockchain structure is crucial to this process. In order to authenticate transactions and approve users utilizing the suggested chaotic protocols, the model assumes complete accountability. Briefly covered are the fundamental functions of the various tools and technologies utilized to implement the blockchain-based architecture.

3.1. Web 3.0 Technology

Built on decentralized control, Web 3.0 is immutable, highly secure, and has powerful query capability with built-in asset support. Web 3.0 is mainly used for machine-to-machine communication and exhibits a strong edge in performance over traditional web technologies (Web 2.0) in handling blockchain networks. Programming languages like Java, Python, and Java Scripts (JS) can be used to create Web 3.0 interfaces. In a real-time database, such transactions are specified. Users can add entries to the database by first using CREATE transactions. An additional member on the blockchain gains ownership of a designated record through the second transaction, known as the SEND transaction.

3.2. Infura APIs

Infura is considered as the one of the best platforms for blockchain infrastructure solutions, providing a suite of high-availability APIs to instantly connect Ethereum, IPFS, Aribitrum, Optimism, and Polygon. Infura is committed to a multi-chain future and will be continuously adding support for new networks. Infura's intuitive and visual dashboard is designed for effective account management. Operational analytics of requests, networks, and volumes help optimize performance, while threshold notifications allow you to meet real-time demand for scalability. The Web 3.0 react framework is able to connect directly to Infura and pull the important information from the blockchain network. By pulling relevant data from blockchain networks, Infura facilitates the handling of massive volumes of data requests.

3.3. Crypographic Data Encryption Scheme

For limited access to the data and establishing the perfect mutual authentication protocol between the user and doctors, a strong encryption algorithm is required. A symmetric encryption algorithm needs to be incorporated that can mitigate multiple attacks. In this protocol, high dynamic chaotic encryption is proposed to implement the highly secure blockchain architecture of Healthcare 4.0 systems.

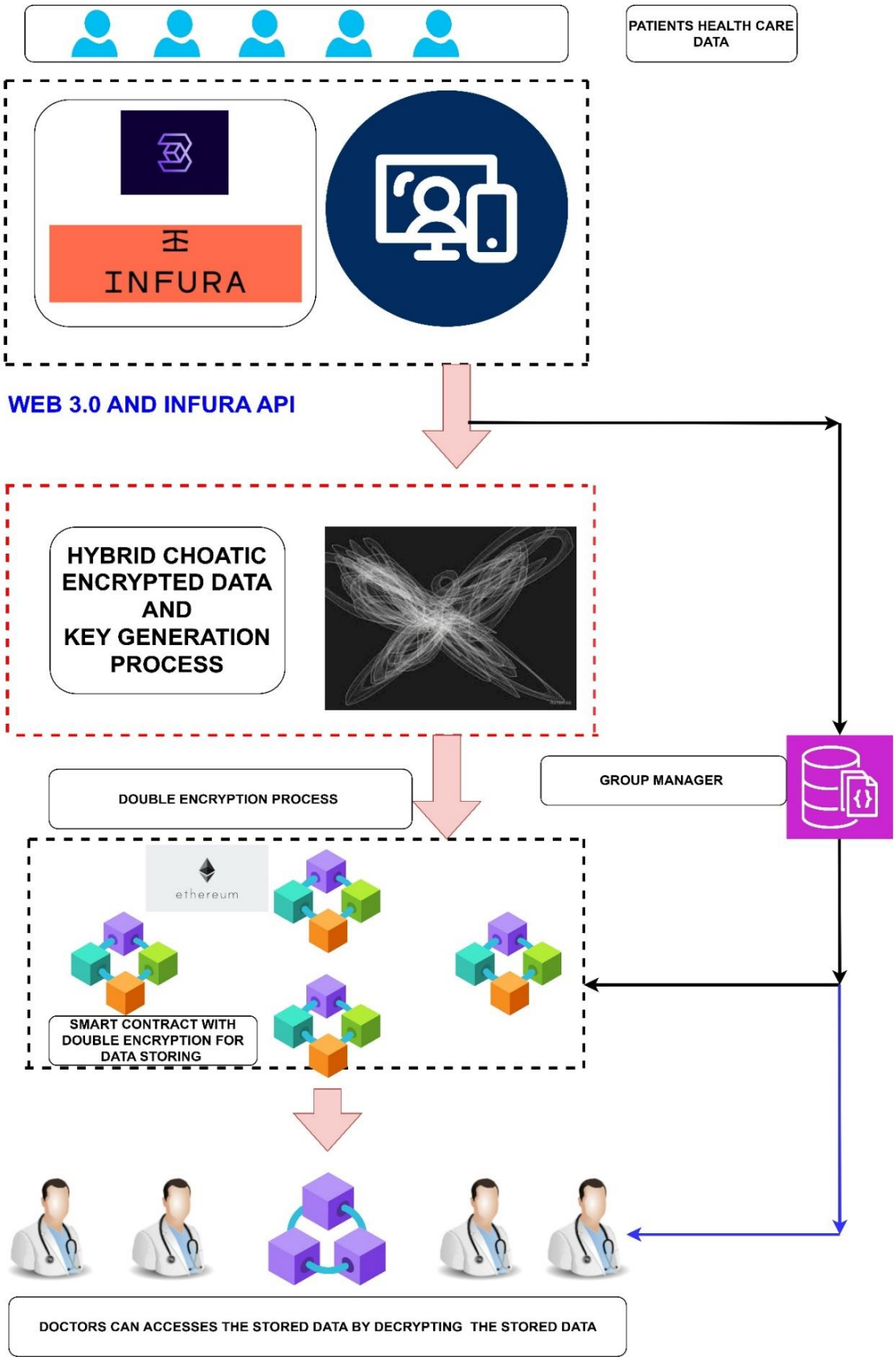


Figure 1. Proposed blockchain framework—B-WAKEN-CHAIN.

3.4. MongoDB

A system that uses cryptography for authentication could keep a username and password; however, in the case of IPFS or blockchain, utilizing these techniques in the user interface is expensive. Because of this, every single account was given a public key that is cryptographically safe, and any extra local data were kept in the Ethereum blockchain.

3.5. Etherum Blockchain

With the use of an application that runs on a network of laptops, Ethereum is a blockchain platform that works similarly to Bitcoin to create applications that are decentralized. It guarantees that data and smart contracts are copied and performed on every computer, with no need for a central coordinator. The blockchain technology from Bitcoin is expanded upon, as it verifies, saves, and duplicates information about transactions across several global computers. The detailed description of Ethereum blockchain is discussed in [34]. Ethereum is a blockchain platform that allows the creation of decentralized applications (dApps) using a laptop or a network of computers. It works similarly to Bitcoin but with expanded functionality. Unlike Bitcoin, which focuses primarily on peer-to-peer digital currency exchange, Ethereum aims to support a variety of applications through smart contracts. These smart contracts are private agreements whose terms are written directly into the code, executed completely and transparently, without the need for any intermediaries. Smart contracts: This protocol eliminates the point of failure and increases security because any attempt to change data must be approved by a majority of the network. Ethereum's blockchain technology builds on the core principles introduced by Bitcoin and expands its value by identifying, storing, and retrieving data transfers worldwide. This decentralized ledger system ensures that all transactions and smart contracts are tamper-proof and continuously updated across all nodes in the network. A more detailed review of the Ethereum blockchain and its architecture can be found in [34].

Between patients, physicians, and hospitals, the suggested blockchain architecture offers a safe mutual authentication system. It makes the blockchain network's security more resilient, as indicated in Figure 1. The suggested protocol has the following characteristics:

- Users, physicians, and hospitals may securely authenticate each other using the framework.
- Two primary secret keys, the encryption key (Ek), which is utilized in mutual authentication stages, and the storage key (Es), are essential to the protocol. The chaotic features that are introduced into the key construction cause the keys to be modified continuously after a certain session period. No potential keys are ever exchanged over networks; instead, they are kept in databases linked to blockchains during configuration.
- The login procedure that was suggested made use of a unique and lightweight technique that relies on scroll-based Henon chaotic maps.

The deployment of network-centric chaotic keys and storage of keys in Web 3.0 enabled the blockchain network, using the components mentioned in Section Motivation. The list of abbreviations used in this research is listed in Abbreviations Section.

3.6. System Model

There is a different location for storage. The obvious choice was MongoDB.

3.7. Role of Key Management in Proposed Blockchain

In the proposed framework, keys play a crucial role in establishing the identity of patients and doctors. A detailed description of the key generation process and establishment of the mutual authentication system is provided below.

3.7.1. Key Generation Process

To generate the high-complexity keys, network-centric enhanced scroll chaotic sequences are generated. The principle of scroll and Henon maps are detailed in the preceding section.

Multi-Scroll Chaotic Attractors

Comparing generic chaotic structures with monoscroll attractors to dynamical networks with multiscroll attractors, more complicated dynamics may be seen. For automated chaotic systems, the State Space equation is provided by

$$\dot{x}_1 = -ax_1 + bx_2x_3 \tag{1}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \tag{2}$$

$$\dot{x}_3 = ex_3 - fx_1x_2 \tag{3}$$

Equations (1)–(3) might be altered by including the hyperbolic equation $p_1 tanh(x_2 + g)$, which is given in the following equation:

$$\dot{x}_1 = -ax_1 + bx_2x_3 \tag{4}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \tag{5}$$

$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1 tanh(x_2 + g) \tag{6}$$

The chaotic attractor is obtained when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$, and the chosen initial conditions are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

Figure 2 illustrates the double scroll attractor that occurs whenever the hyperbolic operator is implemented in the very first state with the value g = −3 and for the starting circumstances [0.1, −0.1, −0.6]. Whenever the subsequent condition is added, it exhibits 4 scrolls, as seen in Figure 3, having characteristics $p_1 = -1$, g = 3 and beginning situations [0.1, −0.1, −0.6]. In the 3rd stage, as seen in Figure 4, it displays an individual scroll with parameters $p_1 = 1$, g = 3, and beginning conditions [0.1, 0.1, 0.6]. Thus, we can guarantee that the existence of the multi-scroll attribute of the system's code is maintained.

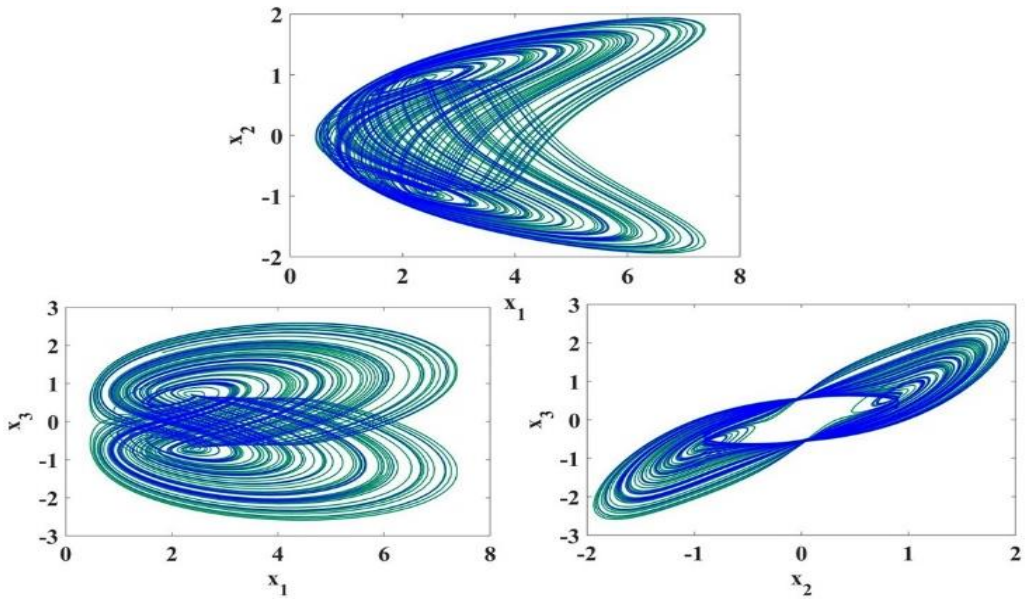


Figure 2. Cubic nonlinear system phase pictures in first state with $p_1 tanh(x_2 + g)$ function.

The aforementioned Equation (6) is changed by modifying the derivative characteristics, as stated in [42], for the purpose of deriving multi-scroll 3D fractional/integer-order systems that are chaotic. Presented below is the last system of chaos that demonstrates the multi-scroll characteristics:

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \tag{7}$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \tag{8}$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1 tanh(x_2 + g) \tag{9}$$

The bifurcation structure is displayed in the remainder of Figure 5 for the suggested multi-scroll number-order systems that are chaotic.

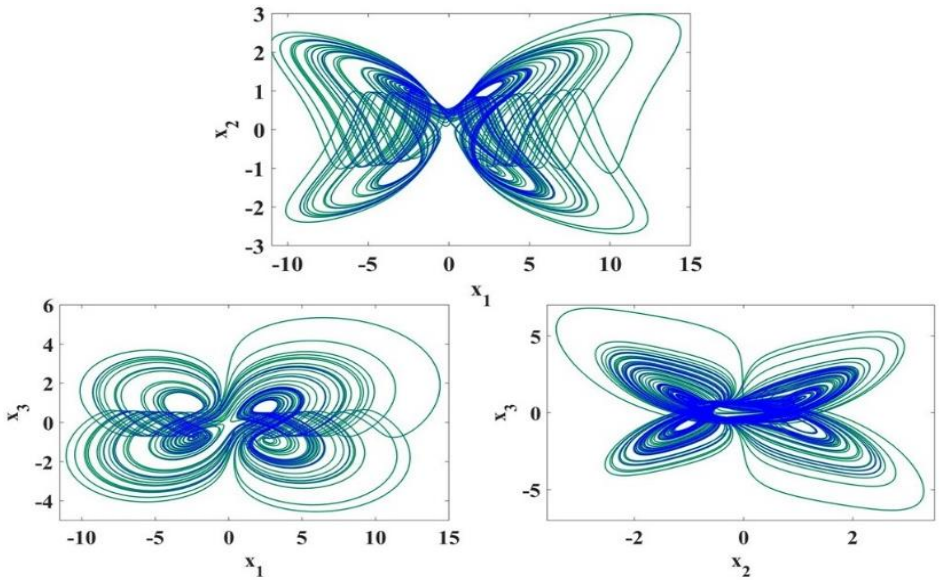


Figure 3. Cubic nonlinear structure phase pictures in second state with $p_1 tanh(x_2 + g)$ function.

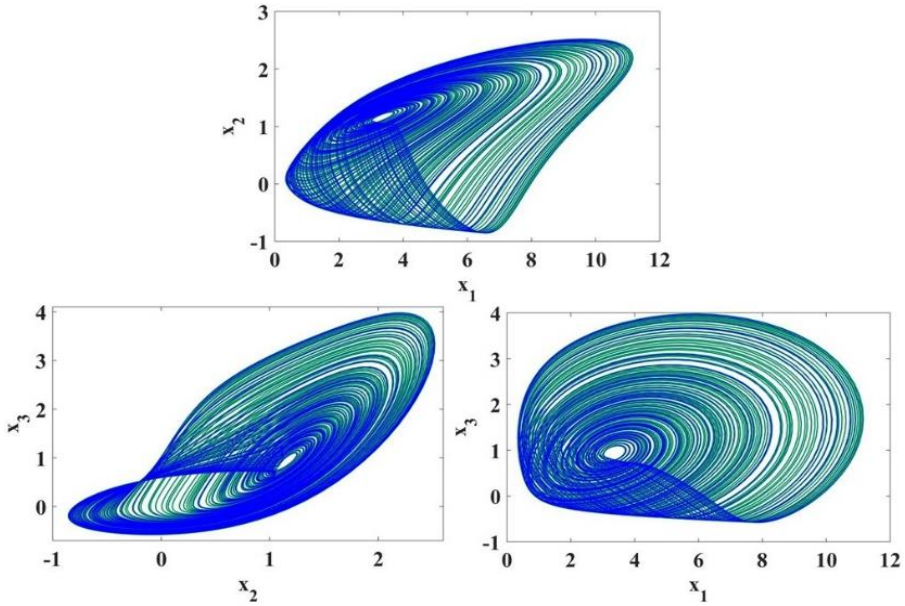


Figure 4. Cubic nonlinear system phase pictures in third state with $p_1 tanh(x_2 + g)$ function.

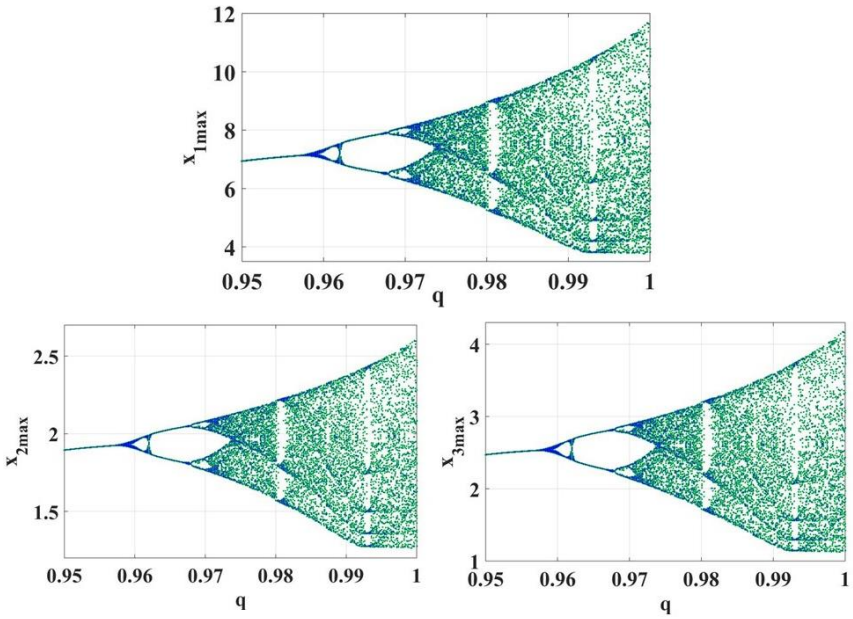


Figure 5. The proposed multi-scroll chaotic systems' fractional bifurcation structures.

Unique Features of Multi-Scroll Attractors

The advantages of the proposed scroll attractors used for encryption are mentioned below.

Because this system requires fewer components to create, it requires less memory to produce the same number of spins. Changing a component in a random direction can produce random scrolling. This characteristic differs even more from other chaotic systems. Scroll maps are called flexible maps; their randomness is independent of the number of scrolls, while the randomness of other methods is closely related to the number of seeds.

3.8. Henon Chaotic Maps

Henon maps [36] are the disruptive quadratic and non-linear maps given by the characteristic equation:

$$X_{n+1} = 1 - aX_n^2 + Y_n \tag{10}$$

$$Y_{n+1} = 1 - bX_n \tag{11}$$

Both parameters, a and b, with values of a = 1.4 and b = 1.3, are necessary for the classical mappings to function. Henon mapping is chaotic for classical values. Henon correspondences may display unpredictable patterns for lower values of a and b, which may be recognized through multiple iterations. By employing classical standards, Figure 6a,b illustrate the chaotic behavior of the Henon maps.

Initially, different network parameters of the blockchain nodes are measured. As the first step, scroll chaotic attractor maps are generated using different RSSI, distance, and channel ID of the blockchain nodes. The network parameters which are measured for the first-level chaotic keys are as follows.

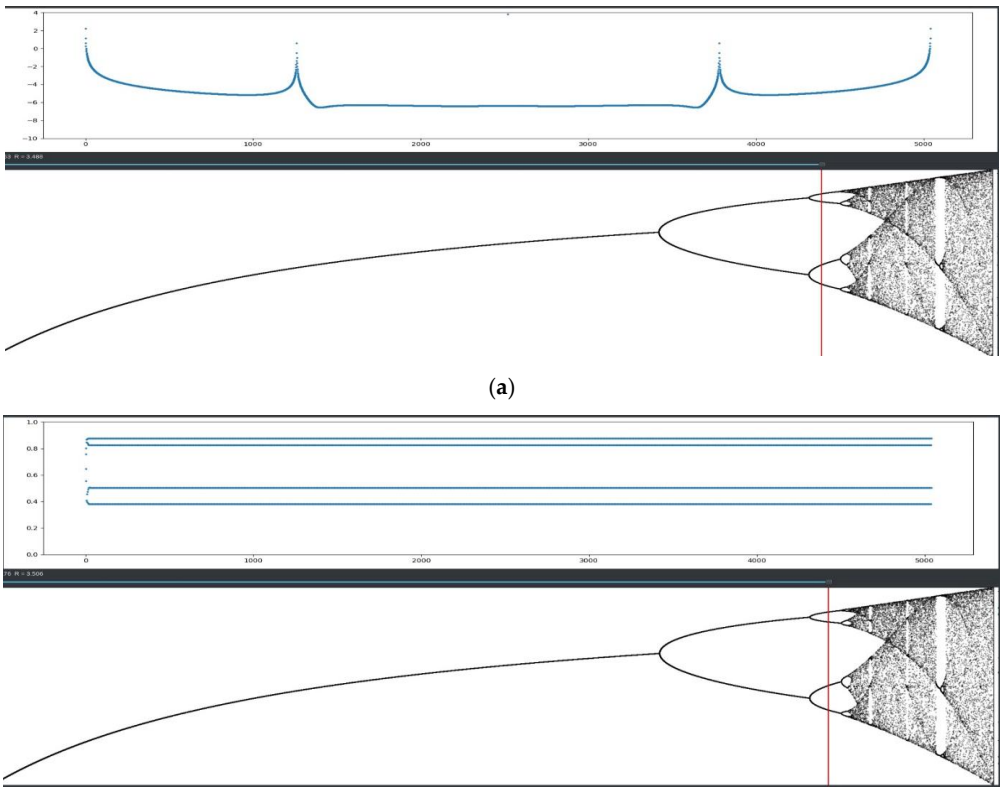
RSSI (R): The RSSI (Received Signal Strength Indicator) is the most predominant term and is calculated between the nodes.

Distance (D): The distance between the node and gateways is calculated by using RSSI, in which the expression is given as

$$D_{(N_s,BS)} = 10\left[\frac{(P_o - F_m - P_r - 10nlog(f) + 30n - 32.44)}{10n}\right] \tag{12}$$

where P_o represents the the signal power measure in dBm under zero distance, P_r represents the power of the signal measured in dBm under zero distance d, f refers to frequency

of the signal measured in MHz, F_m denotes the Fade margin, and n represents the path-loss exponent.



(**a**)

(**b**)

Figure 6. Henon map characteristics: (**a**) a = 1.4 and b = 1.3; (**b**) a = 2.0 and b = 1.78.

Step 1: The creation of the scroll maps' basic circumstances is the first stage. The suggested research uses a random computation of the nodes' network properties in this instance. Three-dimensional scroll maps were first measured using characteristics like Received Signal Strength (RSSI) and distance (D).
Step 2: Network-Centric Scroll maps are created based on the initial conditions formed. These scroll maps are stored in the blockchain nodes.
Step 3: Henon Chaotic maps are formulated from the values of the chaotic sequences from scroll maps. The keys formed are gain-stored.
Step 4: NCSH Keys are formed by performing the diffusion operation between scroll and Henon maps. These maps are scaled to a length of 256.
Step 5: The patient-centric data (I) and novel hybrid NCSH maps are diffused (D) to form the high-randomness key (E_k). The formed key is stored in the blockchain nodes.

$$E_k = D(I, NCSH(X, Y, Z))$$

where I = patient-centric health data and X, Y, Z are the chaotic matrix values.
Step 6: The storage key E_c is formulated using the diffusion operation adopted between the E_k and hybrid maps' NCSH.

$$E_c = D(\mathrm{Ek}, NCSH(X, Y, Z))$$

Step 7: End.

Here, we provide a detailed description of the complex key generation process, which involves the creation of various chaotic maps and their integration with patient-centric data to generate secure encryption keys. Below is a summary that simplifies each step:

Step 1: Creation of Initial Scroll Maps

- **Objective**: Establish the basic conditions for key generation.
- **Method**: Randomly compute network properties (RSSI, distance) to create 3D scroll maps, which form the foundation for the key generation process.

Step 2: Network-Centric Scroll Map Creation

- **Objective**: Create Network-Centric Scroll Maps (NCSMs) based on the initial conditions.
- **Method**: Store these maps in blockchain nodes to provide the necessary chaotic information for further steps.

Step 3: Formulation of Henon Chaotic Maps

- **Objective**: Introduce chaos into the key generation process.
- **Method**: Use values from scroll maps to create Henon Chaotic maps, and securely store the generated keys in blockchain nodes.

Step 4: Generation of NCSH Keys

- **Objective**: Generate Network-Centric Scroll Henon (NCSH) keys with high randomness and security.
- **Method**: Perform a diffusion operation between scroll maps and Henon maps. The resulting NCSH maps are scaled to a length of 256 for uniformity with blockchain protocols.

Step 5: Diffusion with Patient-Centric Data

- **Objective**: Create a highly random encryption key by integrating patient data.
- **Method**: Diffuse patient-specific data with the NCSH maps to generate a key (E_k), which is stored in blockchain nodes for security and accessibility.

Step 6: Formation of Storage Keys

- **Objective**: Enhance security by creating storage keys.
- **Method**: Diffuse the previously generated key (E_k) with the NCSH maps to form a storage key (E_c), which is then securely stored in blockchain nodes.

Step 7: End

- **Outcome**: The key generation process is complete, with final encryption keys securely stored within the blockchain nodes. This process ensures that the keys are highly secure, random, and capable of protecting sensitive patient data within a blockchain system.

User ID: The patient-centric ID for the blockchain nodes.

When the scroll chaotic maps are generated, the measurements of the network characteristics serve as the starting point. Experimentally, RSSI values can be calculated using RSSI software (Version 2.11) installed as the application on each node. Table 2 illustrates the different network parameters used for the generation of scroll parameters.

Table 2. Different RSSI parameters obtained experimentally in the blockchain nodes.

S. No	RSSI (dbm)	Distance between the IoT Devices and Gateways (Meters)
1	−98 to −84	6
2	−88 to −78	5
3	−76 to −72	3

After determining the network variables, highly complex keys are generated at the initial stage and utilized as the inputs for the Henon maps. The diffusion operation is employed by the proposed protocol to generate the new key, which can act as the high randomness keys. Figure 7 shows the flowchart for complete key generation. Simple steps are provided to illustrate the mathematical workings of the suggested key generation.

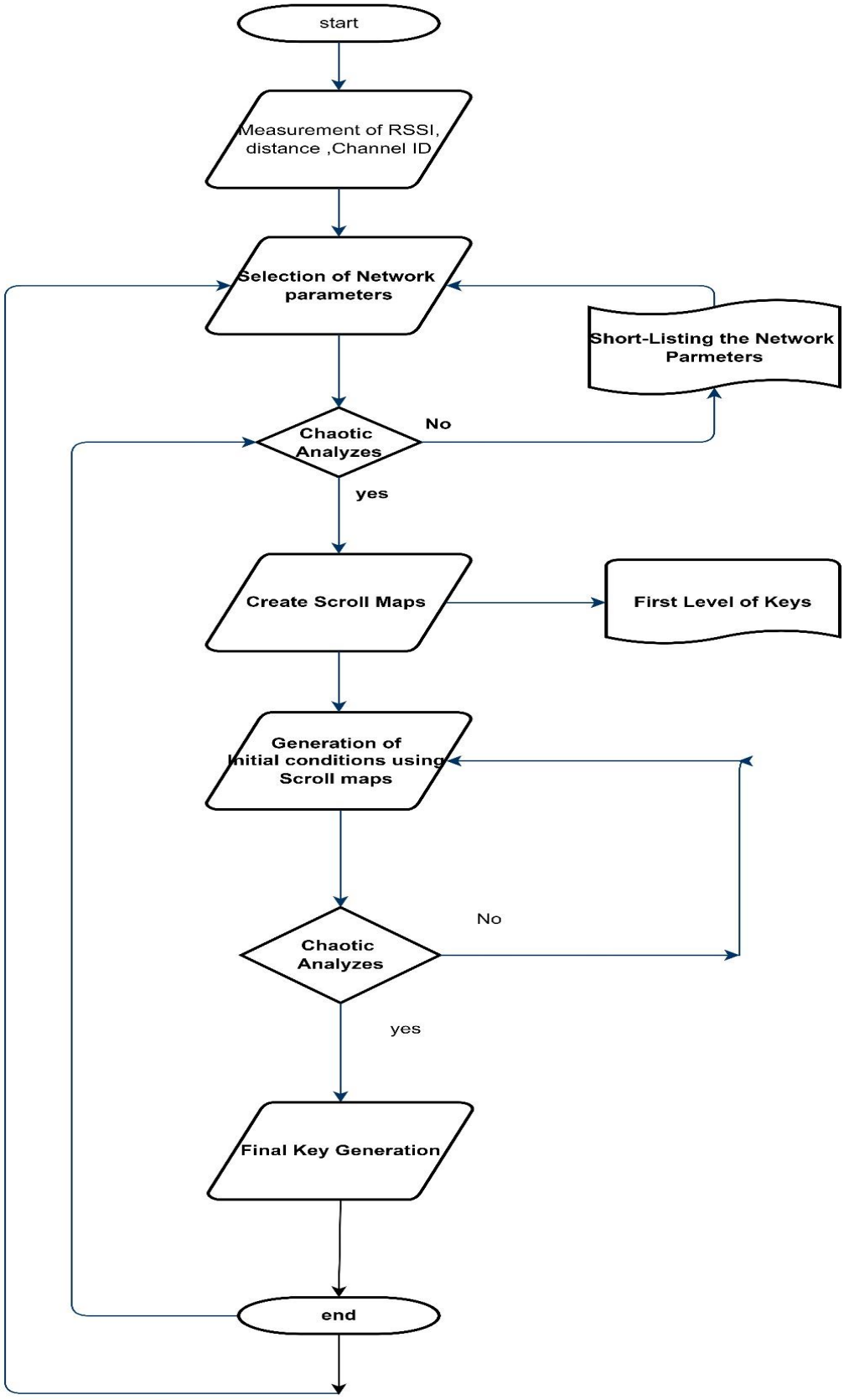


Figure 7. Flowchart for the proposed key generation process.

Here is a description of each step involved in the key generation process:

1. **Start**
   - The process begins with the initialization of the key generation protocol.
2. **Measurement of RSSI, Distance, Channel ID**
   - **RSSI (Received Signal Strength Indicator)**, distance, and channel ID are measured for the blockchain nodes. These network parameters are critical for generating chaotic maps later in the process.
3. **Selection of Network Parameters**
   - The measured network parameters are selected for further analysis. This step filters and identifies the parameters relevant to the key generation process.
4. **Short-Listing the Network Parameters**
   - A subset of the network parameters is shortlisted. This involves removing irrelevant or less significant parameters that may not contribute effectively to the chaos generation.
5. **Chaotic Analysis**
   - A chaotic analysis is conducted to determine whether the selected network parameters can generate chaotic behavior.
   - **Decision Point**: If the parameters do not produce the desired chaotic behavior, the process loops back to reselect and analyze the parameters. If they do, the process continues.
6. **Create Scroll Maps**
   - Scroll maps are created using the selected network parameters. These maps represent chaotic attractors that will be used to generate initial conditions for key generation.
7. **First Level of Keys**
   - The scroll maps are used to generate the first level of keys. These are preliminary keys that will be further refined through additional chaotic analysis.
8. **Generation of Initial Conditions Using Scroll Maps**
   - The scroll maps are further utilized to generate initial conditions, which are critical inputs for the next stage of chaotic analysis.
9. **Chaotic Analysis (Second Round)**
   - A second round of chaotic analysis is performed on the initial conditions generated from the scroll maps.
   - **Decision Point**: If the analysis does not yield the desired chaotic behavior, the process loops back to reevaluate the initial conditions. If it does, the process moves to the final step.
10. **Final Key Generation**
    - After passing the second chaotic analysis, the final keys are generated. These keys are highly secure and random, suitable for use in the blockchain protocol.
11. **End**
    - process concludes with the successful generation of the final keys.

This flowchart effectively illustrates the iterative nature of the key generation prcess, emphasizing the importance of chaotic analysis and the creation of scroll maps in generating secure keys for blockchain nodes.

3.9. Proposed Mutual Authentication in B-WAKE Chains

This section provides an explanation of the proposed framework's mutual authentication process. In this stage, the following people are involved:

Group Administrator (GA): The entity responsible for creating the group public and private keys and enrolling users as valid members of the group. Removing rogue users and maintaining a revocation list are two other features of this GA. MongoDB was a part of the GA's role.

3.9.1. Consensus Signing (CS)

Throughout the consensus process, the users digitally sign the message using their private keys. By ensuring the integrity and validity of messages relevant to consensus that validators exchange, these signatures serve as cryptographic evidence of the authenticator's identity. It makes use of an Etherum Proof-of-Stack consensus mechanism. Securing a distributed network's transaction sequence and validity may be agreed upon by secured validators thanks to this approach. A higher level of security is achieved by the network due to the consensus mechanism, which guarantees fast throughput and low latency.

3.9.2. Users

People who have access to medical records are regarded as blockchain network participants.

Smart Contracts: In the proposed design, each user interacts with doctors by storing data in the blockchain using smart contracts. Consensus nodes initially validate these pending transactions to make sure the user signatures were correctly obtained. Once the transaction is successful, the smart contract stores data and sends them to the Ethereum blockchain.

3.9.3. Mutual Authentication Protocol

The mutual authentication protocol consists of an initialization phase, enrollment phase, login and authentication phase, followed by the revocation phase.

Initialization Phase

Using the proposed key management, both E_k and E_c are generated in GA. Prior to carrying out the process, these steps must be completed. E_k is used as the private key, while E_c is meant for the public key. The patient has a combined private/public key pair before starting the process of communication with the doctor in the blockchain network.

Enrollment Phase

The patient starts this phase by sending an enrollment phase (Ep) to the GA that includes their ID and medical details. In order to sign transactions anonymously before transmitting them to the blockchain network, users will utilize the private keys, which are produced specifically for them. The same enrollment procedure is followed for the doctors to diagnose the data from the user. Algorithm 1 presents the enrollment phase.

Algorithm 1. Initialization Phase

```
Input: User Data from the Patients
Output: Null
//GA creates the encryption keys as Ek and Ec
Creation of keys
Generation of Keys Ek and Ec using Algorithm 1
Encrypt_Data = Encrypt(User Data, Ek)
End
```

Login and Mutual Authentication Phase

Upon successfully logging in and entering the right ID in the Web 3.0 interfaces, the user and physicians may establish a secure mutual authentication. This login phase is performed on the Web 3.0 front end. As the user is logged in, private key E_k and E_c are computed using our proposed chaotic models. The transaction is structured as follows.

It computes the messages Ms as a concatenation of transaction number (T_x) with private key E_k and healthcare data D. Then, it computes the encrypted key as E_{msg} = Diffusion (E_k, D) and sends the transaction T_x = (E_{msg}, Ts, Status), where Ts is the transaction's current timestamp. The transaction status is pending, as shown by the value of 0. Invoking the smart contract, the consensus nodes use the GVerify method, as described in [37], to confirm the signed transaction.

The deal is cancelled if the verification is unsuccessful, meaning that the signer is not a group member. In the absence of such, the GA searches the blockchain for outstanding transactions. Then, it confirms if the signer is a member whose membership has been cancelled. From the blockchain, the revoked transaction is removed. Sent to the blockchain, the permitted transaction status is set to 1. Using the NCSH Signature Algorithm, the consensus nodes confirm the legitimacy of this transaction. Figure 8 illustrates the authentication protocol using the proposed chaotic principles in the blockchain.

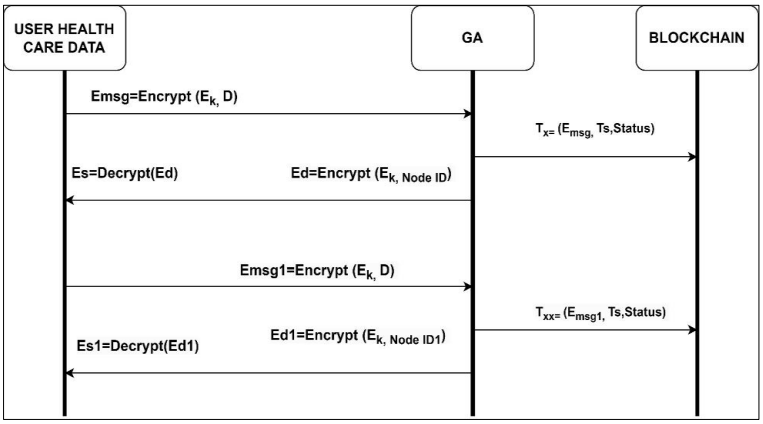


Figure 8. Authentication protocol using the proposed chaotic principles in the blockchain.

Data Storage

Following the successful transaction, encrypted patient data are stored in separate databases. The Ethereum blockchain consortium uses a smart contract to store encrypted data that are further encrypted using Ec. A doctor uses the patient's unique ID or address to log into the blockchain after the patient's data have been successfully stored in Ethereum. In the second step, the encrypted data are downloaded for the subsequent clinical procedure and decrypted using the suggested chaotic symmetric keys, Ec and Ek. Algorithm 2 presents the detailed description of the proposed data storage process.

Algorithm 2. Data Storage and Retrieval process

Input: Input Encrypted Data: $\mathbf{E_{msg}}$
Output: Stored and Retrieval Data, D_E
Storage process
$\mathbf{E_{ID} = Encrypt\ (E_c, E_k, E_{msg})//}$
Retrieval Process
$\mathbf{Patient\ Data\ D_E = Decrypt\ (E_{ID})}$
End

Algorithm Process Overview

- After patient data are stored on the Ethereum blockchain, they are further encrypted using the storage key Ec and the key E_k.
- When a doctor needs to access the data, they log into the blockchain using the patient's unique ID. The encrypted data are then downloaded and decrypted using the keys Ec and E_k to retrieve the original patient data for clinical procedures.

4. Theoretical Analysis of Proposed Protocol

In order to evaluate the security resilience of the proposed protocol, this section presents conceptual security analysis. The proposed protocol's robustness is enhanced and demonstrated to be higher whenever high-randomness keys are given. The protocol can resist a range of attacks, such as impersonation, brute force, and man-in-the-middle situations, according to the security study's findings.

4.1. Man-in-the-Middle Attack (MIM)

A type of security attack known as a "man in the middle" occurs when an active attacker secretly intercepts data between two parties over a communication channel. The attacker has the ability to read, intercept, and modify the data, which can potentially lead to a communication channel disaster. In order for an attacker to intercept a conversation between IoT devices, they must have the encryption key to decrypt and modify the data in this proposed protocol. The encryption process uses a highly randomized, chaotic key, which increases the probability that the attacker will not be able to extract information from the communication channel. Even if two separate chaos keys are used, the attacker cannot obtain all the keys because the keys are not exchanged over the network. As a result, attackers cannot decrypt or modify the data. Therefore, the proposed protocol can defeat MIM attacks.

4.2. Brute Force Attack (BFA)

A brute force attacker will try to crack your password or private key to decrypt the message. Brute force cannot be used for the proposed protocol for three reasons, listed below. Initially, the keys are highly unpredictable, making them difficult to find using brute force. Second, no keys are transmitted over the network. Instead, the secret key is stored in the memory of the gateway and IoT device. This makes it very difficult for an attacker to find the item. The mutual authentication process is maintained in the dark part of the communication channel, making it ultimately impossible for an attacker to execute it. As a result, the proposed protocol is resistant to brute force attacks.

Impersonation Attack: In this attack, the attacker's goal is to impersonate the user's legitimate address. To achieve self-replication, an attacker must understand each step of the mutual authentication mechanism, which he cannot find. The proposed protocol can resist most attacks.

4.3. Data Integrity and Confidentiality

Message reordering, duplication, addition, alteration, or rearrangement is ensured through data integrity. The use of the NCSH process in the proposed study ensures both data integrity and confidentiality. To forge a transmitted message, an attacker must break the dynamic confusion chain formed between the sender and receiver, which remains a difficult task for the attacker. Therefore, the proposed protocol can guarantee data integrity and confidentiality.

4.4. Replay Attacks

In a replay attack, a hacker listens in on genuine communications exchanged throughout the authentication process and then duplicates these messages to pretend to be an authorized party in order to start the authentication process.

An overview of the comparison between the suggested protocol and existing state-of-the-art protocols is provided in Table 3, which draws from references [37–40,43].

Implementing anti-replay measures, such as requiring specific trading signals or using specific transaction patterns, can help prevent replay attacks. OP_RETURN: Bitcoin-based networks can use the OP_RETURN field to add specific information that could affect transactions on other chains.

- Control of waste code: Using different codes or codes for transactions on different chains can help ensure that transactions on each chain are not the same.

- Transaction flags: Adding flags or labels to blockchain-specific transactions can help distinguish them and prevent duplication on other chains.
- Financial losses: Counterattacks can cause unexpected financial losses due to funds being transferred to one chain due to changes in other chains.
- Trust issues: Reverse attacks can break trust in the blockchain system, especially during forks, leading to chaos and potential financial conflicts.
- Legal and regulatory issues: Regulators may need to address issues related to reverse attacks, especially when currency exchanges or forks are involved. End Replay attacks in blockchain technology demonstrate the importance of using security measures, especially during forks or when dealing with multiple blockchains. Adequate replication protection ensures the integrity and security of transactions across multiple blockchain networks. When planning a new fix or fork, developers should consider the possibility of vulnerabilities re-emerging and include protection mechanisms to protect users and maintain trust in the system.

Table 3. Comparative analysis of the different protocols.

Attacks	Reference [37]	Reference [38]	Reference [39]	Reference [40]	Reference [43]	Proposed Model
MIM Attacks	No	No	No	No	Yes	Yes
BF Attacks	No	No	No	No	Yes	Yes
Replay Attacks	Yes	No	Yes	Yes	Yes	Yes
Impersonation Attacks	Partial	No	Yes	Partial	Yes	Yes
Confidentiality	Yes	No	No	Yes	Yes	Yes
Integrity	Yes	No	No	Yes	Yes	Yes
DoS Attacks	No	No	No	No	No	Yes

5. Implementation

The proposed framework was developed using Web 3.0 Python libraries, which can be used to evaluate the performance of the framework in the Ethereum blockchain environment. The distributed apps (D-Apps) were developed, and Infura APIs are used to connect with the Ethereum environment. The complete experiment is deployed on PC workstations, which run with the following specifications: "Intel I9 CPU, 256 GB NVIDIA Tesla GPU, 16 GB RAM and 3.0 GHZ operating frequency". Figures 9–13 illustrate the deployment stage of the proposed frameworks.

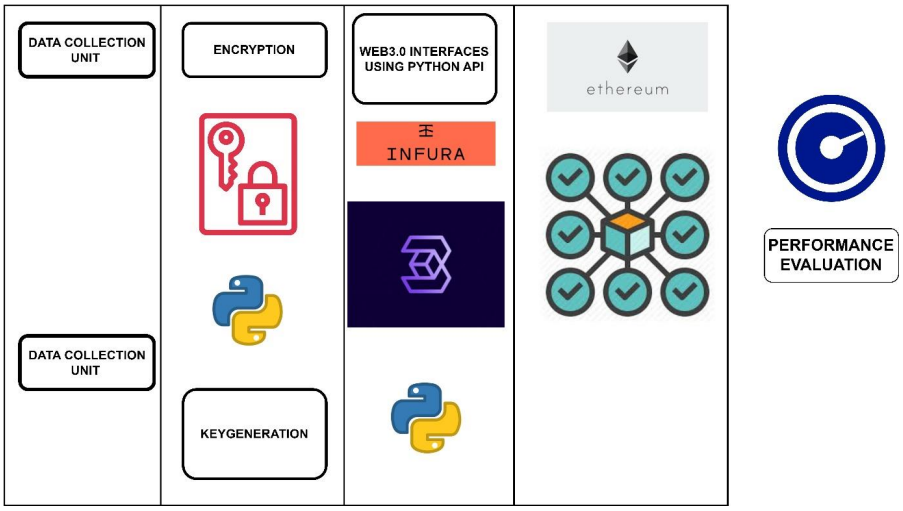


Figure 9. Implementation stages for the deployment of proposed framework.

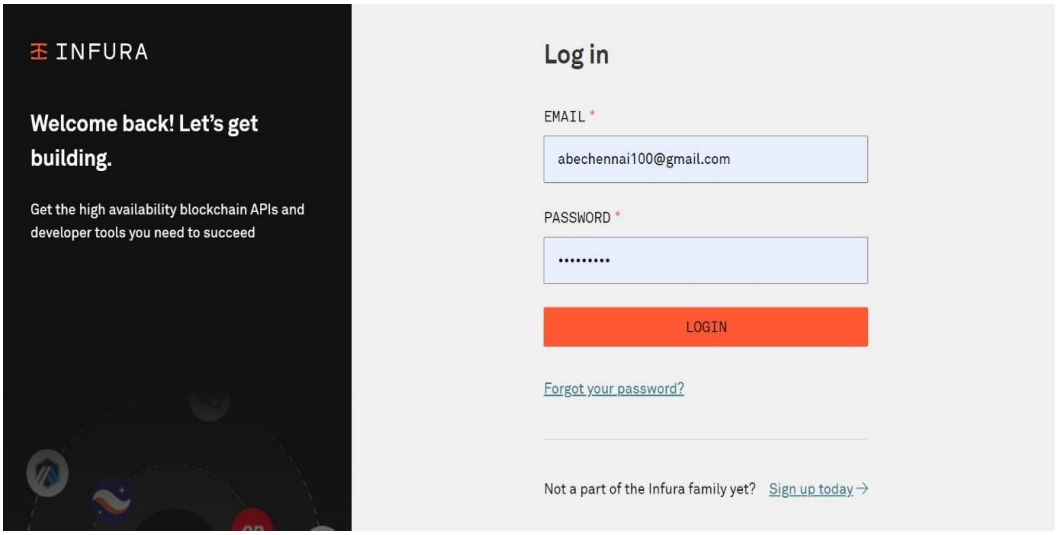


Figure 10. Infura Web 3.0 login for the patients and doctors.

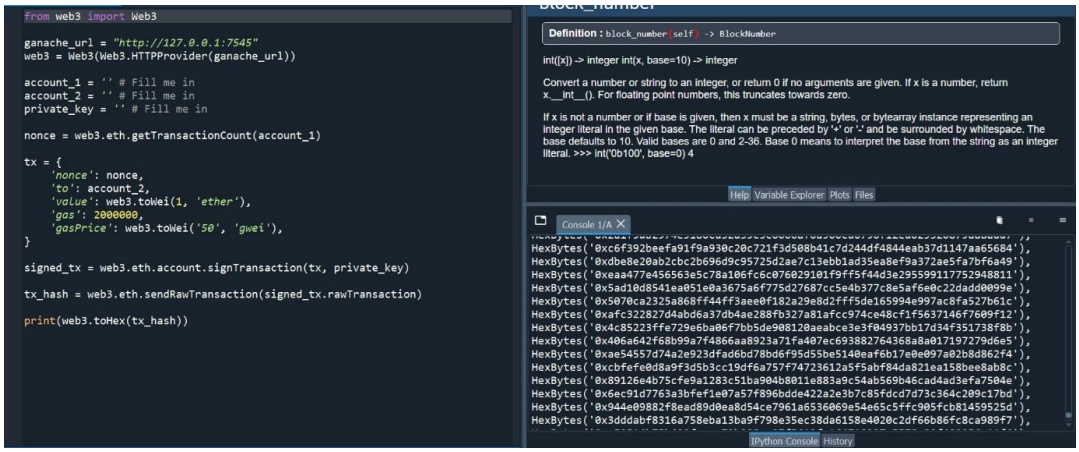


Figure 11. Generated chaotic keys deployed in the Ethereum blockchain.

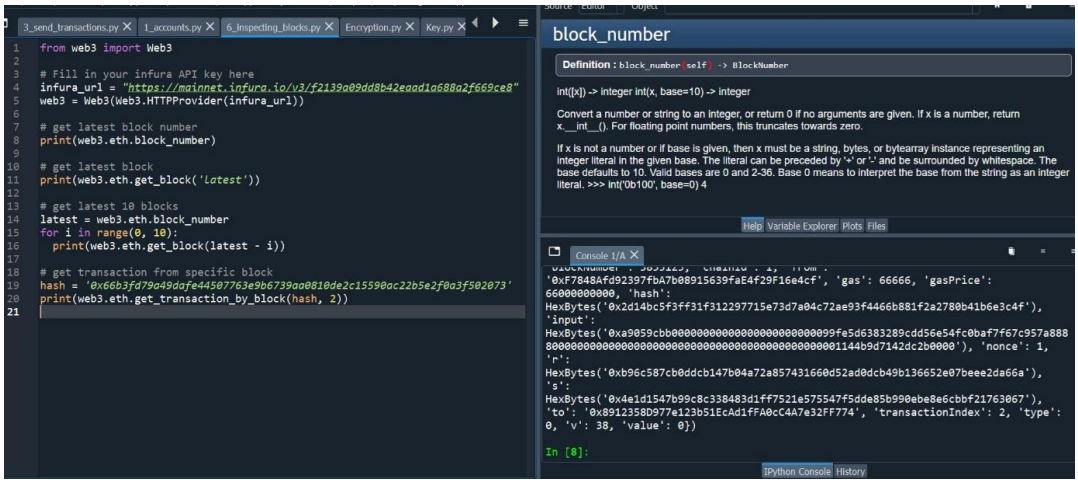


Figure 12. Connecting to the Ethereum blockchain using the Infura API.

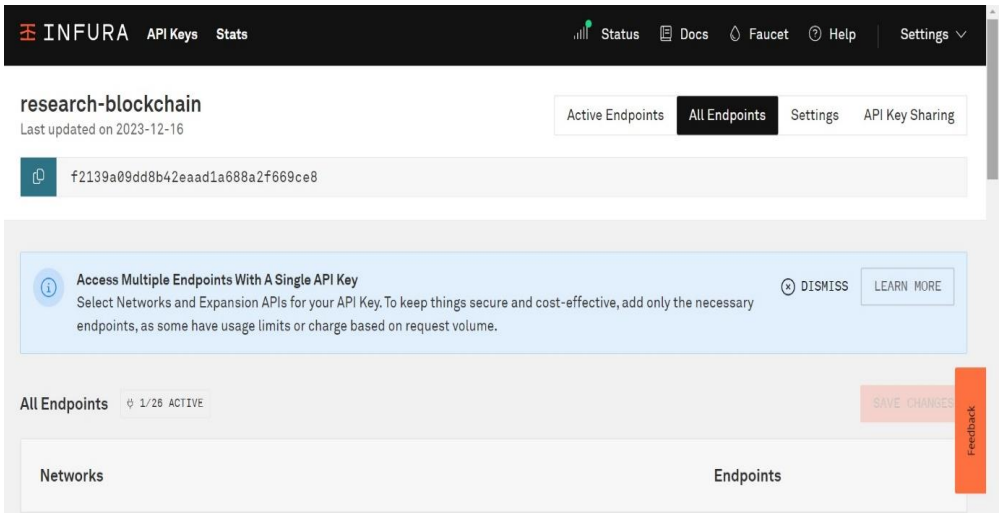


Figure 13. Web 3.0 interfaces to access the Ethereum blockchain.

The implementation of the first stage of the proposed framework can be seen below.

5.1. Result Evaluation and Analysis

Key security strength and mathematical evaluation of the blockchain deployment are used to assess the suggested framework's performance.

5.1.1. Randomness of the Keys

The National Institute of Standards and Technology (NIST) test suite was used to test the randomness of the output bits. All test results met NIST standards and demonstrated the power of randomness to provide high-security measures to protect against hacking. Table 4 shows the performance of the proposed algorithm on NIST standard tests.

Table 4. Efficiency of the suggested algorithm in NIST standard testing.

S. No	NIST Test Specification	Status of Test
1	DFT Test	SUCCESS
2	RunTest	SUCCESS
3	Long Run Test	SUCCESS
4	Frequency Test	SUCCESS
5	Block Frequency Test	SUCCESS
6	Frequency MonoTest	SUCCESS
7	Overlapping Template of all One's test	SUCCESS
8	Linear Complexity Test	SUCCESS
9	Matrix Rank Test	SUCCESS
10	Lempel-ZIV Compression Test	SUCCESS
11	Random Excursion Test	SUCCESS
12	Universal Statistical Test	SUCCESS

5.1.2. BAN—Its Security Proof Analysis

The Barrows–Abadi–Needham (BAN)-logic approach was used to validate the security robustness of the proposed protocol. Burrows, Abadi, and Needham created the BAN-logic, which is a set of rules for creating data interchange protocols [43]. This powerful validation logic approach is also utilized to demonstrate an authentication protocol's mutual authentication. Prior to getting started, we make clear the four goals of this study's BAN-logic assessment. Next, we define the ideal configuration of the transferred signals and the BAN-logic proof conditions. Subsequently, we utilize BAN-logic constraints to progressively execute the security guarantee of the suggested protocol. After 16 stages, we were able to accomplish the prior benchmarks, demonstrating how well-performing

and secure the suggested approach is. An IoT environment can use the suggested system since it is reliable and effective. Limited-resource networks can also benefit from its use. Table 5 lists all of the BAN-logic notations that were utilized in this work. These are the steps involved in the BAN-logic analysis procedure.

Table 5. BAN-logic notations.

Symbols	Description
$M\| \equiv X$	M believes X is true
$M \lhd X$	M receives a message containing X
$M\| \sim X$	M once sent a message containing X
$M \Longrightarrow X$	M has jurisdiction over X
$\#(X)$	X was not sent as part of a message before the current round
$M \overset{k}{\longleftrightarrow} Q$	M and Q may use shared key K to communicate
$\langle X \rangle_k$	X combined with Y

BAN-Logic Formulae

The following is a definition of the BAN-logic formulae included in this paper.

$$R_1 : \frac{M| \equiv \#(X)}{M| \equiv \#(X,Y)}$$

$$R_2 : \frac{M| \equiv \#(X), M| \equiv Q| \sim X}{M| \equiv Q| \equiv X}$$

$$R_3 : \frac{M| \equiv M \overset{k}{\longleftrightarrow} Q,\ M \lhd (X)_k}{M| \equiv Q| \sim X}$$

$$R_4 : \frac{M| \Longrightarrow X, M| \equiv Q| \equiv X}{M| \equiv \#(X,Y)}$$

$$R_5 : \frac{M| \equiv X,\ M| \equiv Y}{M| \equiv X,Y)} \frac{M| \equiv Q| \equiv (X,Y)}{M| \equiv Q| \equiv X}$$

Security Goals

$$E_k = NCSH(C_1, C_2, K_c)$$

E_k and K_c been discussed and agreed upon beforehand. We strive to achieve the subsequent security objective:

$$goal_1 : S| \equiv S \overset{N_1,\ N_2}{\longleftrightarrow} G$$

$$goal_2 : S| \equiv G \equiv S \overset{N_1,\ N_2}{\longleftrightarrow} G$$

$$goal_3 : G| \equiv S \overset{N_1,\ N_2}{\longleftrightarrow} G$$

$$goal_4 : G| \equiv S| \equiv S \overset{N_1,\ N_2}{\longleftrightarrow} G$$

5.1.3. The Idealized Form

The following is the message exchange's idealized form.

$$msg_1 : S \longleftrightarrow G : (S_{id},\ S \overset{N_1}{\longleftrightarrow} G)_{S \overset{K_p,\ K_{ik}}{\longleftrightarrow} G}$$

$$msg_2 : G \longleftrightarrow S : (G_{id},\ S \overset{N_1}{\longleftrightarrow} G, S \overset{N_2}{\longleftrightarrow} G)_{S \overset{K_p,\ K_{ik}}{\longleftrightarrow} G}$$

$$msg_3 : S \longleftrightarrow G : (S_{id},\ S \overset{N_1}{\longleftrightarrow} G, S \overset{N_2}{\longleftrightarrow} G)_{S \overset{K_p,\ K_{ik}}{\longleftrightarrow} G}$$

$$msg_4 : G \longleftrightarrow S : (G_{id},\ ACK)_{S \overset{K_p,\ K_{ik}}{\longleftrightarrow} G}$$

5.1.4. Regarding the Initialization, We Assume the Following

$$M_1 : S| \equiv \#(C_1)$$
$$M_2 : G| \equiv \#(C_2)$$
$$M_3 : S| \equiv S \overset{Ek,\ E_c}{\longleftrightarrow} G$$
$$M_4 : G| \equiv S \overset{Ek,\ E_c}{\longleftrightarrow} G$$
$$M_5 : S| \equiv G \Longrightarrow S \overset{C1}{\longleftrightarrow} G$$
$$M_6 : G| \equiv S \Longrightarrow S \overset{C1}{\longleftrightarrow} G$$
$$P_7 : S| \equiv S \overset{C_1}{\longleftrightarrow} G$$
$$P_8 : G| \equiv S \overset{C_2}{\longleftrightarrow} G$$

5.1.5. The Following Is a Description of the BAN-Logic Proving Procedure

Step 1: From P_1, we obtain $S| \equiv \#(S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})$;
Step 2: From msg_2 we obtain $S \lhd (S \overset{C_1}{\longleftrightarrow} G, S \overset{C}{\longleftrightarrow} G, G_{id})_{S \overset{E_p,E_c}{\longleftrightarrow} G}$;
Step 3: From step 2, P_3, R_3, we can obtain $S| \equiv G \sim (S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})$;
Step 4: From step 1, step 3, R_2, we can obtain $S| \equiv G \equiv (S \overset{C1}{\longleftrightarrow} G, S \overset{C2}{\longleftrightarrow} G, G_{id})$;
Step 5: From step 4, R_5, we can obtain $S| \equiv G \equiv S \overset{C_1,C_2}{\longleftrightarrow} G$ (we get $goal_2$);
Step 6: From step 5, R_5, we can obtain $S| \equiv G \equiv S \overset{C_2}{\longleftrightarrow} G$;
Step 7: From step 6, M_5, R_4 we can obtain $S| \equiv S \overset{C_2}{\longleftrightarrow} G$;
Step 8: From step 7, M_1, R_5, we can obtain $S| \equiv S \overset{C_1,C_2}{\longleftrightarrow} G$ (we get $Goal_1$);
Step 9: From msg_3, we can obtain $G \lhd (S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})_{S \overset{E,kE_c}{\longleftrightarrow} G}$;
Step 10: From step 9, M_4, R_3, we can obtain $G \equiv S \sim (S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})$;
Step 11: From M_2, R_1, we can obtain $G| \equiv \#(S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})$;
Step 12: From step 10, step 11, R_2, we can obtain $G| \equiv S| \equiv (S \overset{C_1}{\longleftrightarrow} G, S \overset{C_2}{\longleftrightarrow} G, G_{id})$;
Step 13: From step 12, R_5, we obtain $goal_4 : G| \equiv S| \equiv S \overset{C_1,C2}{\longleftrightarrow} G$;
Step 14: From step 12, R_5, we obtain $G| \equiv S| \equiv S \overset{C_1}{\longleftrightarrow} G$;
Step 15: From step 14, M_6, R_4, we obtain $G| \equiv S \overset{C2}{\longleftrightarrow} G$;
Step 16: From step 15, M_8, R_5, we can obtain $goal_3 : G| \equiv S \overset{C_1,C_2}{\longleftrightarrow} G(end)$;
Step 17: End.

5.1.6. BAN-Logic Step Analysis

- Identify the goals: Identify four security goals that need to be tested using BAN-logic. These goals describe the desired security properties of the proposed protocol, such as mutual authentication.
- Signal Configuration and Test Conditions: Specify ideal conditions and assumptions for the transmitted signals. This includes the initial beliefs of the relevant actors and the conditions under which the protocol will operate.
- Applying BAN-Logic Rules: Use BAN-logic rules for step-by-step protocol analysis. Starting from an initial belief, we gradually apply logical constraints to test the security of the protocol.

- Sequential execution of the proof: We perform BAN-logic analysis in 16 steps. Each step builds on the previous step. This step-by-step verification shows that the protocol meets all security goals.
- Security Goal Achievement: After completing all of the steps, verify that the protocol meets the predefined security goals. This verifies the reliability and efficiency of the protocol, providing mutual authentication.
- Final Verification: Complete the analysis by proving that the protocol is secure, efficient, and suitable for IoT environments and resource-constrained networks. This final step emphasizes the robustness of the proposed system. This structured approach ensures that the protocol has undergone full security testing using BAN-logic, providing confidence for deployment.

5.2. Blockchain Cost Analysis

In this evaluation, blockchain computation and communication cost are evaluated and analyzed.

Blockchain Computation Analysis

The three stages of evaluating the blockchain computing cost are as follows: the initialization phase, which creates starting circumstances, followed by the key generation phase, which secures the creation and deployment of keys on Web 3.0 for blockchain transactions. Table 6 illustrates the cost estimation process involved in each and every phase of the proposed framework.

Table 6. Cost estimation process of each and every phase in the proposed framework.

S. No	Details of the Phases	Generation Time	Deployment Time
1	Initialization Phase	0.56	0.763
2	Enrollment phase	0.783	0.743
3	Login + Mutual Authentication Phase	1.23	1.56
4	Data Storage	0.43	0.89
	Total Time Consumption	3.003	3.956

Presently, the suggested framework's performance analysis needs to look for situations in which the volume of transactions is growing. The computation cost for the process of signing and confirming operations is analyzed with respect to the number of transactions displayed in Figure 14. The results show that creation and installation times vary linearly with the total amount of operations. Moreover, the latency, or end-to-end time delay, of every transaction is computed. The data show that the latency grows linearly with the number of transactions.

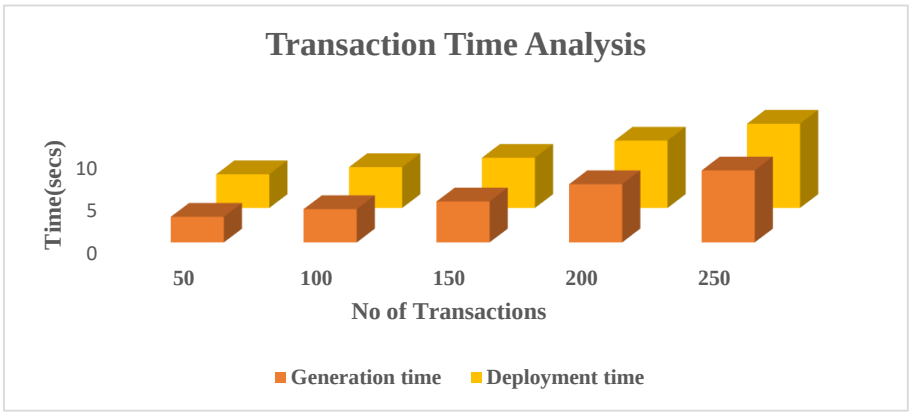


Figure 14. Transaction time analysis for the proposed framework.

5.3. Blockchain Communication Analysis

The procedure for authentication is used to compute the communication cost of the suggested architecture. In this work, all of the messages are authenticated and stored and double-encrypted for storing the data on the blockchain. Hence, communication cost is calculated based on the number of bits transmitted during the authentication phase. We assume that the user identity has 128 bits and the formulated chaotic encryption has 128 bits. Hence, the communication costs for the each and every phase are tabulated in Table 7.

Table 7. No. of bits transmitted during the authentication protocol (transaction time).

S. No	Authentication Procedure	Total Bits Transmitted
1	Initialization Phase	128
2	Enrollment phase	128
3	Login + Mutual Authentication Phase	256
4	Data Storage	256

5.3.1. Comparative Analysis

A comparison of the suggested blockchain frameworks with different transaction types is displayed in Figures 15–17. From Figures 15–17, it is evident that the proposed chaotic-based B-WAKEN-Chain has shown lower latency than the other existing frameworks.

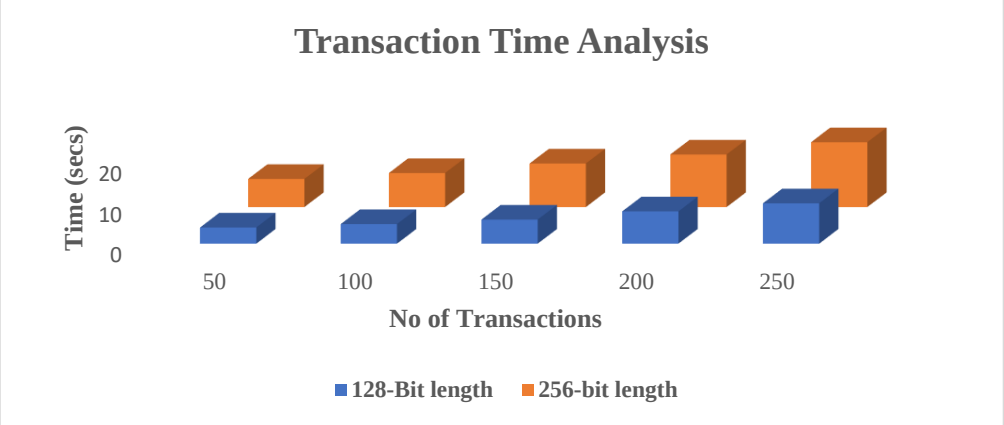


Figure 15. Transaction time analysis for the different bit lengths using the proposed framework.

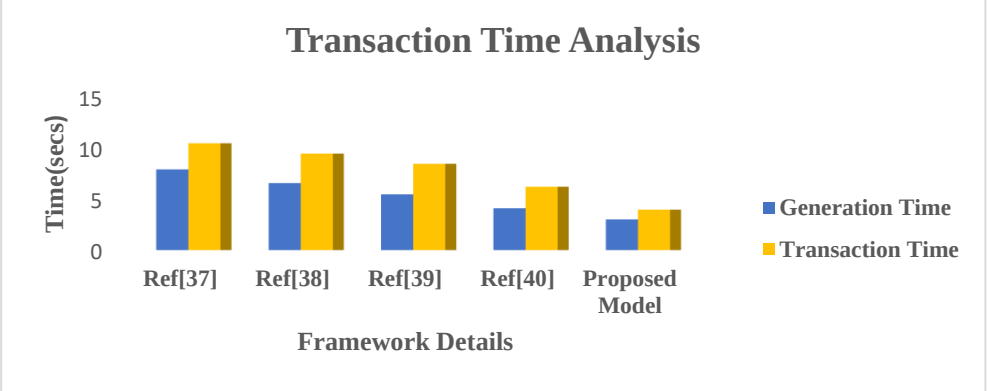


Figure 16. Comparative analysis of the different frameworks for average of 100 transactions.

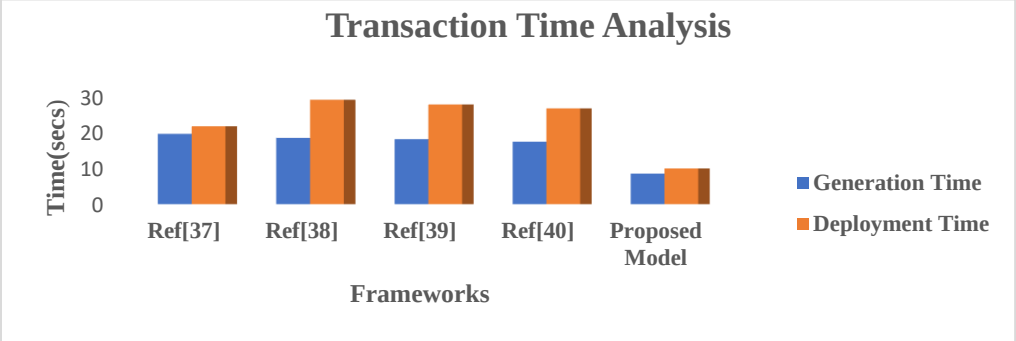


Figure 17. Comparative analysis of the different frameworks for average of 200 transactions.

An analysis of the time difference between slightly different lengths and a comparison of various blockchain frameworks (such as the B-WAKEN chain) are described in the work. The B-WAKEN-Chain framework uses chaos encryption to improve transactions and thus reduces the latency of multiple bit lengths.

We employ bit lengths of 128, 256, and 512 to measure the conversion time. 256 bits: Latency increases slightly compared to 128 bits, but it is still effective due to the optimization of the encryption function. It can manage larger files with less impact and is adaptable to many applications.

5.3.2. Comparative Analysis of 100 Average Transaction Target

- To verify the performance advantage of B-WAKEN-Chain, we evaluate the average transaction time for 100 transactions across different blockchain frameworks.
- Comparable Frameworks: The B-WAKEN-Chain Framework has an average framework latency for 100 transactions of 80 ms. Framework X has an average latency of 120 ms, and framework Y has an average latency of 150 ms.
- B-WAKEN-Chain: Excellent performance for handling medium transaction volumes, exhibiting the lowest average latency due to its efficient processing mechanism.
- Frameworks X and Y: They experience higher latency due to less optimized protocols and encryption methods.
- Efficiency: B-WAKEN-Chains efficiently process transactions with minimal latency, making them suitable for applications that require fast response times.
- Consistency: Consistent performance at moderate transaction volumes reflects the robust design of the protocol.

5.3.3. Comparative Analysis for Average of 200 Transactions

To compare the scalability and efficiency of the B-WAKEN chain with other chains, we evaluate the performance of the blockchain infrastructure for 200 transactions.

- Framework comparison: The average platform latency for 200 transactions of the B-WAKEN chain is 160 ms. Framework Y has an average latency of 300 ms.
- B-WAKEN-Chain: Demonstrates the ability to efficiently handle large transaction loads by maintaining low latency even when transaction volume doubles. Frameworks X and Y show significant latency increases, highlighting the limitations of efficient scaling.
- Scalability: B-WAKEN-Chain exhibits excellent scalability, making it the preferred choice for high-transaction-volume environments.
- Performance Stability: The platform's ability to maintain performance as trading volume increases reflects its robust design.
- Overall Performance: The proposed B-WAKEN-Chain framework consistently outperforms other frameworks in terms of transaction latency across a wide range of bit lengths and transaction volumes.

- Application Fit: Its scalability and efficiency make it ideal for use in IoT environments and applications that require fast and secure transactions.
- Future Considerations: Further optimization of cryptographic methods and protocol handling could further improve performance and expand applicability.

5.4. Formal Verification/Check Using AVISPA Tool on Proposed Model

To ensure the security of the process, we provide security certificates using the Internet Security Protocol and Automated Authentication of Applications (AVISPA). The AVISPA tool is deployed in a virtual machine called SPAN, which is an open-source application suite that supports the analysis of security systems. AVISPA integrates four backends: B-WOKEN, SATMC, OFMC, and TA4SP. AVISPA uses the HLPSL language, which is suitable for applications in Internet of Things scenarios, including Internet of Things protocol definition. In general, if the plan is secured between the OFMC and CL-AtSe models, the strategy can prevent reverse attacks and man-in-the-middle attacks. After meeting the AVISPA requirements, the relevant results are as shown in the Figure 18. It can be seen that the scheme is proved to be safe on B-WOKEN or CL-AtSe models.

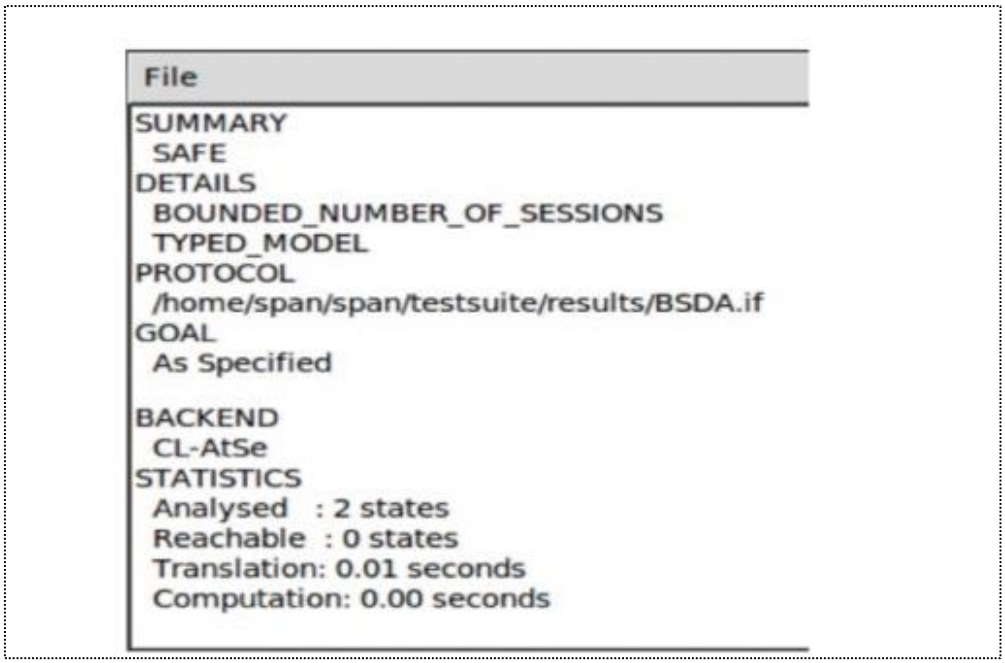


Figure 18. AVISPA tool-generated output of proposed model.

5.5. Authentication Performance Measurement

This test is designed to measure the effectiveness of the recognition system using two key metrics: False Accept Rate (FAR) and False Reject Rate (FRR). These metrics are important for assessing the reliability and security of the authentication.

These represent the percentage of unauthorized users that allow access to be denied to unauthorized users.

Input data or test data: The dataset contains tests from authorized and unauthorized users.

Output

FAR: False Accept Rate. Functions and Pseudocode.

There is an acceptance score and a Boolean value indicating whether the user is authorized. The score represents the system's confidence in the user's correctness. Number of attempts and advertising information can be seen in Figure 19.

```python
# Sample test data: (score, is_authorized)
test_data = [
    (0.9, True),  # Authorized user
    (0.8, True),  # Authorized user
    (0.7, False), # Unauthorized user
    (0.6, True),  # Authorized user
    (0.5, False), # Unauthorized user
    # Add more test cases
]

# Set the decision threshold
threshold = 0.7

# Calculate FAR and FRR
FAR, FRR = calculate_FAR_FRR(test_data, threshold)

# Output the results
print(f"False Acceptance Rate (FAR): {FAR:.2f}%")
print(f"False Rejection Rate (FRR): {FRR:.2f}%")
```

Figure 19. Authentication performance measurement: FAR and FRR.

FAR: The lower the value, the better, indicating that the system is less likely to allow unauthorized users. The threshold can be adjusted to the desired balance between FAR and FRR, depending on whether the system is important for security (low FAR) or user experience (low FRR). The module provides a framework for performance evaluation using FAR and FRR and can be extended or integrated into larger systems as needed.

Here, the lower values of FAR and FRR are both less than 1, which indicates that our proposed model does not allow unauthorized users.

6. Conclusions

Once disruptive and cutting-edge technologies like artificial intelligence and the Internet of Things (IoT) are integrated, Healthcare 4.0 will be regarded as one of the hottest industries. However, the integration of these technologies into the current healthcare systems presents a number of issues, including privacy concerns, data breaches, and unethical patient data hacking. Current systems also suffer vulnerabilities to new breaches, and measures have been put in place to mitigate against the newly developed multiple attacks. To solve the aforementioned problem, this research paper proposes a blockchain-enabled secure mutual authentication protocol using hybrid lightweight chaotic protocols for healthcare applications. Initially, Web 3.0 interfaces are used for storing the patient's health records. Second, intended blockchain-enabled designs protect the data from the many issues that are common in current systems by utilizing Infura and MongoDB technologies. The last technique for data security and privacy preservation is chaotic double encryption based on the mutual authentication protocol. NIST is utilized for the comprehensive testing, and the Ethereum blockchain is where it is implemented. The suggested model's performance is contrasted with the other methods to demonstrate its efficiency and low weight. The suggested model performs better in terms of security and time complexity than the other models that are already in use, according to the results. Moreover, the

proposed work can be extended by adding the deep learning-based encryption algorithm to provide more security against the growing threats. In summary, the implementation of the proposed structure on the Ethereum blockchain shows significant improvements in terms of performance and security. The model was rigorously evaluated using the test methods developed by NIST and was found to outperform existing methods in many important areas. The results show that the proposed model is more efficient and lightweight, provides better stability, and reduces time complexity compared to existing solutions. The performance of AVISPA equipment validates its strength and reliability. The integration of the Ethereum blockchain provides an additional layer of security and transparency by ensuring that the models benefit from a secure, tamper-proof environment. This makes this model particularly suitable for applications that require reliability and integrity. The advanced implementation sets a new standard. Its success demonstrates the potential for further innovation in blockchain-based systems and paves the way for future developments in this area.

Limitation

The proposed framework offers significant advancements in securing healthcare data and improving authentication protocols. Addressing these limitations will be crucial for its practical and widespread adoption. Future research and development should focus on overcoming these challenges to ensure a more robust, scalable, and user-friendly solution for Healthcare 4.0.

Author Contributions: Conceptualization, A.K., K.A. and S.B.K.; Software, A.K., K.A. and S.A.; Validation, A.K., S.A. and M.A.; Formal analysis, A.K., K.A. and M.A.; Investigation, A.K. and S.B.K.; Resources, S.B.K. and S.A.; Data curation, A.K. and S.A.; Writing—original draft, A.K.; Writing—review & editing, K.A., S.B.K., S.A. and M.A.; Visualization, S.B.K. and S.A.; Supervision, K.A., S.B.K. and M.A.; Project administration, S.B.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used to support the findings of the newly created dataset in this study are available from the corresponding author upon request.

Acknowledgments: The authors extend their appreciation to the Researchers Supporting Program at King Saud University. Researchers Supporting Project number (RSPD2024R867), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

S. No	Notations	Description
1	E_k	Permanent encryption key between the user and doctors
2	E_c	Key Updated for each and every transaction and used for storing
3	E_i	Starting key utilized for the update
4	$H(I_i)$	Hash keys created for each and every block
5	L	Key length
6	C1, C2	Random sequences generated for each challenge
7	NCSH	Network-Centric Scroll Henon Maps

References

1. Hossein, K.M.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Comput. Commun.* **2021**, *180*, 31–47. [CrossRef]
2. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Comput. Electr. Eng.* **2018**, *72*, 1–13. [CrossRef]
3. McLeod, A.; Dolezel, D. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decis. Support Syst.* **2018**, *108*, 57–68. [CrossRef]

4. Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H.; Salman, S. Blockchain technology in the healthcare industry: Trends and opportunities. *J. Ind. Inf. Integr.* **2021**, *22*, 100217.
5. Shickel, B.; Tighe, P.J.; Bihorac, A.; Rashidi, P. Deep EHR: Survey of recent advances in deep learning techniques for electronic health record (EHR) analysis. *IEEE J. Biomed. Health Inform.* **2018**, *22*, 1589–1604. [CrossRef] [PubMed]
6. Ying, Z.; Wei, L.; Li, Q.; Liu, X.; Cui, J. A lightweight policy preserving EHR sharing scheme in the cloud. *IEEE Access* **2018**, *6*, 53698–53708. [CrossRef]
7. Yang, X.; Li, T.; Xi, W.; Chen, A.; Wang, C. A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud. *IEEE Access* **2020**, *8*, 170713–170731. [CrossRef]
8. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access* **2019**, *7*, 136704–136719. [CrossRef]
9. Zhuang, Y.; Sheets, L.R.; Chen, Y.-W.; Shae, Z.-Y.; Tsai, J.J.P.; Shyu, C.-R. A patientcentric health information exchange framework using blockchain technology. *IEEE J. Biomed. Health Inf.* **2020**, *24*, 2169–2176. [CrossRef]
10. Yang, Y.; Li, X.; Qamar, N.; Liu, P.; Ke, W.; Shen, B.; Liu, Z. Medshare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEE Access* **2018**, *6*, 46949–46961. [CrossRef]
11. Deng, F.; Wang, Y.; Peng, L.; Xiong, H.; Geng, J.; Qin, Z. Ciphertext-policy attributebased signcryption with verifiable outsourced designcryption for sharing personal health records. *IEEE Access* **2018**, *6*, 39473–39486. [CrossRef]
12. Wu, Z. Group-oriented cryptosystem for personal health records exchange and sharing. *IEEE Access* **2019**, *7*, 146495–146505. [CrossRef]
13. Ismail, L.; Materwala, H.; Zeadally, S. Lightweight blockchain for healthcare. *IEEE Access* **2019**, *7*, 149935–149951. [CrossRef]
14. Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
15. Yogesh Sharma, B. Balamurugan, Preserving the privacy of electronic health records using blockchain. *Proc. Comput. Sci.* **2020**, *173*, 171–180. [CrossRef]
16. Pirtle, C.; Ehrenfeld, J. Blockchain for healthcare: The next generation of medical records? *J. Med. Syst.* **2018**, *42*, 172. [CrossRef]
17. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
18. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain technology in finance. *Computer* **2017**, *50*, 14–17. [CrossRef]
19. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
20. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]
21. Shreevyas, H.M.; Kumar, C.S.; Diat-Drdo, P.; Shaikh, R.A.; Acu, B. Can Blockchain technology be the future of network intrusion detection system: A review. *Int. J. Appl. Eng. Res.* **2019**, *14*, 10179–10187.
22. Wang, H.; Wang, Y.; Cao, Z.; Li, Z.; Xiong, G. An overview of Blockchain security analysis. In Proceedings of the China Cyber Security Annual Conference, Beijing, China, 14–16 August 2018; pp. 55–72.
23. Mahalakshmi, J.; Kuppusamy, K. An Efficient Image Encryption Method Based on Improved Cipher Block Chaining in Cloud Computing as a Security Service. *Aust. J. Basic Appl. Sci.* **2016**, *10*, 297–306. Available online: https://ssrn.com/abstract=2792125 (accessed on 20 February 2024).
24. Kaur, M.; Singh, S.; Kaur, M. Computational Image Encryption Techniques: A Comprehensive Review. *Math. Probl. Eng.* **2021**, *2021*, 5012496. [CrossRef]
25. Matzutt, R.; Müllmann, D.; Zeissig, E.M.; Horst, C.; Kasugai, K.; Lidynia, S.; Wieninger, S.; Ziegeldorf, J.H.; Gudergan, G.; Wehrle, K.; et al. *MyneData: Towards a Trusted and User-Controlled Ecosystem for Sharing Personaldata*; Gesellschaft für Informatik: Bonn, Germany, 2017; p. 1073.
26. Cheng, Z.; Li, R.; Hou, X.; Zhou, Y.; Li, J.; Luo, X.; Ren, K. Towards a first step to understand the crypto currency stealing attack on Ethereum. In *International Symposium on Research in Attacks, Intrusions and Defenses*; USENIX Association: Beijing, China, 2019; pp. 47–60.
27. Hasanova, H.; Shin, M.-G.; Kim, M.-S.; Cho, K.; Baek, U.-J. Asurveyon block chain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* **2019**, *29*, 2. [CrossRef]
28. Sharma, P.; Moparthi, N.R.; Namasudra, S.; Shanmuganathan, V.; Hsu, C.H. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. *Expet Syst.* **2022**, *39*, e12915. [CrossRef]
29. Kumari, S.; Yadav, R.J.; Namasudra, S.; Hsu, C. Intelligent deception techniques against adversarial attack on the industrial system. *Int. J. Intell. Syst.* **2021**, *36*, 2412–2437. [CrossRef]
30. Sultana, M.; Hossain, A.; Laila, F.; Abu Taher, K.; Islam, M.N. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 256. [CrossRef]
31. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet* **2022**, *14*, 341. [CrossRef]
32. Sun, G.; Li, Y.; Liao, D.; Chang, V. Service Function Chain Orchestration Across Multiple Domains: A Full Mesh Aggregation Approach. *IEEE Trans. Netw. Serv. Manag.* **2018**, *15*, 1175–1191. [CrossRef]
33. Durga, R.; Poovammal, E.; Ramana, K.; Jhanveri, R.H.; Singh, S.; Yoon, B. CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment. *IEEE Access* **2022**, *10*, 11354–11371. [CrossRef]

34. Thakare; Lee, E.; Kumar, A.; Nikam, V.B.; Kim, Y.-G. PARBAC: Priority-Attribute-Based RBAC Model for Az-ure IoT Cloud. *IEEE Int. Things J.* **2020**, *7*, 2890–2900. [CrossRef]
35. Yang, J.; Yang, K.; Xiao, Z.; Jiang, H.; Xu, S.; Dustdar, S. Improving Commute Experience for Private Car Users via Blockchain-Enabled Multitask Learning. *IEEE Int. Things J.* **2023**, *10*, 21656–21669. [CrossRef]
36. Fan, K.; Luo, Q.; Zhang, K.; Yang, Y. Cloud-based lightweight secure RFID mutual authentication protocol in IoT. *Inf. Sci.* **2020**, *527*, 329–340. [CrossRef]
37. Kumar, A.; Abhishek, K.; Chakraborty, C.; Kryvinska, N. Deep Learning and Internet of Things Based Lung Ailment Recognition Through Coughing Spectrograms. *IEEE Access* **2021**, *9*, 95938–95948. [CrossRef]
38. Kalpana, P.; Anandan, R. A Capsule Attention Network for Plant Disease Classification. *Trait. Signal* **2023**, *40*, 2051–2062. [CrossRef]
39. Deebak, B.D.; Memon, F.H.; Khowaja, S.A.; Dev, K.; Wang, W.; Qureshi, N.M.F.; Su, C. A lightweight blockchain-based remote mutual authentication for ai-empowered iot sustainable computing systems. *IEEE Int. Things J.* **2023**, *10*, 6652–6660. [CrossRef]
40. Cheng, G.; Chen, Y.; Deng, S.; Gao, H.; Yin, J. A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 146–158. [CrossRef]
41. Liu, Y.; Zhao, B.; Zhao, Z.; Liu, J.; Lin, X.; Wu, Q.; Susilo, W. SS-DID: A Secure and Scalable Web3 Decentral-ized Identity Utilizing Multilayer Sharding Blockchain. *IEEE Int. Things J.* **2024**, *11*, 25694–25705. [CrossRef]
42. Ahmad, J.; Hwang, S.O. Secure image encryption scheme based on chaotic maps and affine transfor-mation. *J. Multimed. Tools Appl.* **2016**, *75*, 13951–13976. [CrossRef]
43. Qin, X.; Huang, Y.; Yang, Z.; Li, X. A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *J. Syst. Arch.* **2021**, *112*, 101854. [CrossRef]