Smart-Coord: Enhancing Healthcare IoT-based Security by Blockchain Coordinate Systems

Talal Saad Albalawi [1†],
tsalbalawi@imamu.edu.sa
College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU),
Riyadh 11432, Saudi Arabia [1]

Abstract
The Internet of Things (IoT) is set to transform patient care by enhancing data collection, analysis, and management through medical sensors and wearable devices. However, the convergence of IoT device vulnerabilities and the sensitivity of healthcare data raises significant data integrity and privacy concerns. In response, this research introduces the Smart-Coord system, a practical and affordable solution for securing healthcare IoT. Smart-Coord leverages blockchain technology and coordinate-based access management to fortify healthcare IoT. It employs IPFS for immutable data storage and intelligent Solidity Ethereum contracts for data integrity and confidentiality, creating a hierarchical, AES-CBC-secured data transmission protocol from IoT devices to blockchain repositories. Our technique uses a unique coordinate system to embed confidentiality and integrity regulations into a single access control model, dictating data access and transfer based on subject-object pairings in a coordinate plane. This dual enforcement technique governs and secures the flow of healthcare IoT information. With its implementation on the Matic network, the Smart-Coord system's computational efficiency and cost-effectiveness are unparalleled. Smart-Coord boasts significantly lower transaction costs and data operation processing times than other blockchain networks, making it a practical and affordable solution. Smart-Coord holds the promise of enhancing IoT-based healthcare system security by managing sensitive health data in a scalable, efficient, and secure manner. The Smart-Coord framework heralds a new era in healthcare IoT adoption, expertly managing data integrity, confidentiality, and accessibility to ensure a secure, reliable digital environment for patient data management.

Keywords:
Healthcare, Internet of Things, Integrity, Confidentiality, Access control, Internet of things, Security, Blockchain.

1. Introduction

The Internet of Things (IoT) is a key part of the technology revolution that aims to improve life [1]. The IoT is essential for tackling numerous practical difficulties, making it necessary for survival in today's world. Its broad application in healthcare, automotive, agriculture, and education affects daily life and user behavior [2]. IoT device heterogeneity and operational differences present major security issues. Early adopters expect changes in professional and domestic realms, including assisted living, healthcare, and learning. The Internet of Things (IoT) has complicated challenges that require meticulous preparation to gain general adoption [3]. The novel technology with networking components addresses current issues within processing and energy constraints [4].Smart devices collaborate to achieve the Internet of Things (IoT). It improves technological processing and communication. These infrastructures rely heavily on their ability to repair and modify themselves to withstand predicted and unforeseen changes in their environments. In a contemporary setting, privacy and security are crucial to network building. Despite its potential, the Internet of Things (IoT) is vulnerable to targeted cyberattacks such as data breaches, ransomware attacks, and denial-of-service attacks [7]. Open IoT designs and standards are essential for seamless integration and interoperability. These frameworks should let services work together and across devices. Creating a single, open, and uniform framework is tough. This requires separating application logic and hardware infrastructure, as well as device self-configuration, unique identity, and network scalability to handle rising workloads. Reputable cloud services are essential for addressing these security issues. However, this technique may compromise security, privacy, data manipulation, and service accessibility [9–12]. The cloud provider may manipulate data due to its centralized control, requiring trust in cloud data and service management. Blockchain technology ensures that all network nodes have the same blockchain state, making it more secure. Reduces data tampering by unauthorized parties [13]. Bitcoin and other cryptocurrencies utilize this technology to prevent transaction modifications, decentralize network control, and maintain information confidentiality within a chain of interconnected blocks. Blockchain technology can alter education, healthcare, and finance by building a decentralized system backed by distributed consensus, asymmetric cryptography, and cryptographic hash functions. The combination of IoT and blockchain is needed to protect IoT devices [15] from network attacks, stressing security in this technology. This merger reassesses access control measures to protect data. It might create a single system that incorporates both features to ensure data accuracy and quality as technology advances.

The following are the main contributions to this article:

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.4

1) The Smart-Coord model allows respect for confidentiality and integrity to control access simultaneously. The main contribution of this paper is to provide a combined Smart-Coord model that handles them simultaneously.
2) To test and evaluate the Smart-Coord system, the Internet of Things (IoT) scenario described for healthcare involves interacting technology and IoT protocols.
3) The healthcare-IoT information should be confidential and secured; it should be transferred through the application layer, which controls the management of the collected data, and the community of applications or end users should receive the processed information.
4) To implement confidentiality and integrity of data, a coordinate system with encrypting and decryption algorithms is developed in a smart healthcare environment.
5) State-of-the-art comparisons were also performed with the proposed Smart-Coord system. Overall, the Smart-Coord system achieved the best results.

The structure of this research paper unfolds as follows: Section 2 delineates the existing body of knowledge concerning IoT integration in healthcare. Section 3 elucidates the formulated methodology, followed by a concise presentation of the findings in Section 4. Subsequently, Section 5 undertakes a critical discourse on the proposed methodology, culminating in a conclusive synthesis in Section 6.

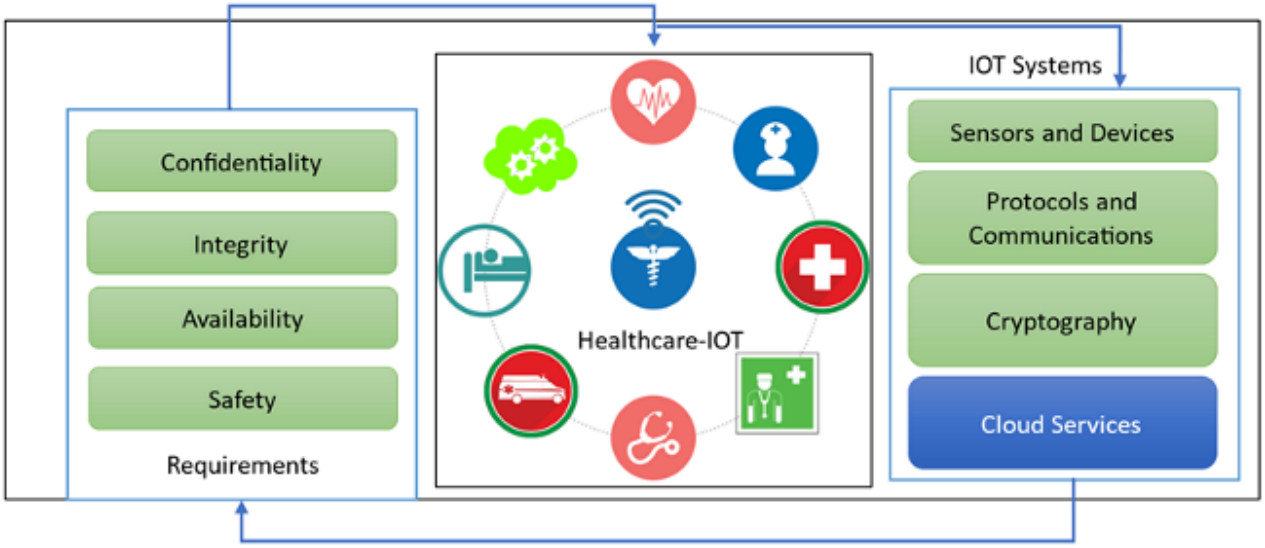

Figure 1. IoT applications have other needs besides safety, as shown here. When deciding on the communication and security protocols, they should be considered.

2. Background

In today's interconnected era, the Internet of Things (IoT) stands as a revolutionary framework, encapsulating a myriad of devices endowed with network connectivity to facilitate seamless data production and exchange [9–12]. This innovative network is portrayed in Figure 1 and prominently pervades various sectors, including smart homes, healthcare, urban planning, agriculture, and education, leveraging sensors and other IoT instruments to actualize its applications. The Internet of Things (IoT) impacts healthcare by integrating technology and protocol. The perceptual, network, and application layers show this integration. The perception layer has sensors to monitor temperature, heart rate, and oxygen levels, and ECG reports are the main data-gathering interface [13]. Devices on local networks with limited coverage can synchronize and exchange information using this layer. Gateways deliver the captured data to the network layer, which securely transfers it to storage servers. The application layer manages data and sends it to apps or end-users [14–16]. Access control mechanisms in data governance are classified as required and discretionary [17]. Within a security policy, these paradigms might work independently or together. The Mandatory Access Control (MAC) system secures people and things differently. The operating system control access enforces security policies.

The DAC allows the object owner to establish access privileges, creating a customized access control scheme.

Supplementing these are role-based access control (RBAC) systems, offering a versatile framework that accommodates either DAC or MAC structures, tailored to suit specific applications. RBAC centralizes rights allocation to roles rather than individuals, a strategy executed by administrators to prevent privilege misuse and facilitate systematic access control by grounding permissions on roles rather than individual identities.

Within the broader spectrum of access control, two predominant models focus on safeguarding confidentiality and integrity, namely the Bell-LaPadula and Biba models. D. Elliott Bell and Leonard J. La Padula created the former in 1973 to improve system confidentiality by combining MAC and DAC. It regulates access through security clearances [18]. Two principles underpin this paradigm: the simple-security property, which rules read access based on security levels, and the star property, which governs write access. The Biba integrity model regulates information flow based on integrity levels. This paradigm secures data transport, preventing low-integrity actors from corrupting information. The simple integrity and integrity star policies underpin the Biba model.

3. Literature Review

In recent years, the technological landscape has seen significant advancements in architecture and techniques for secure access to data on the Internet of Things (IoT) ecosystem. Key among these are initiatives utilizing blockchain technology to enhance the security and privacy of data sharing across diverse networks, as underscored in various scholarly works.

The integration of blockchain technology in mobile health systems, denoted as mHealth, is an exemplary development in this sphere. Reference [18] delineates a system where every device within a network is assigned a unique identity, facilitating secure and transparent data exchanges. Current IoT paradigms often rely on singular password systems for authentication and authorization, which are susceptible to security breaches.

In [19], a creative way to fix this vulnerability is shown. A nuanced authentication method is used, and each part of the system is treated as a separate node connected by network technologies. Also, the study in [20] emphasizes the use of blockchain platforms for the safe management and analysis of healthcare data. These platforms use advanced cryptographic methods to prevent cyberattacks and make IoT transactions more secure.

A notable trend in the IoT space is the emergence of the Internet of Medical Things (IoMT), which necessitates extensive infrastructure to manage the vast quantum of generated medical data. The research cited in [21] says that blockchain data structures should replace centralized data storage repositories in IoMT systems. This would improve security and privacy. This approach involves the decentralized storage of substantial data, with hash references maintained on the blockchain.

In works [22] and [23], promising steps forward in healthcare infrastructure are shown. These works suggest reliable medical care engineering and secure exam mechanisms for clinical sensors within the IoT healthcare framework. These advancements integrate sophisticated verification strategies and smart contract applications based on the Ethereum protocol, enhancing security multifold.

Moreover, the utilization of blockchain technology transcends healthcare, finding applications in various industries including finance, smart homes, and automation, providing reliability and efficiency as outlined in [24]. However, these innovations are not without challenges, primarily concerning the security and privacy of patient data in intelligent healthcare systems. Future trajectories in this domain seem to converge towards a harmonious integration of blockchain and IoT, potentially revolutionizing data privacy and accessibility in healthcare ([25], [26], [27]).

4. Proposed Methodology

In the proposed study, a robust and secure methodology for managing data acquired from various medical sensors and wearable IoT devices is delineated. This data, comprehensively compiled from patients' files available on the Kaggle website, is transmitted to and stored securely in a blockchain storage system known as the Interplanetary File System (IPFS). This approach entails a hierarchical and secure data flow mechanism, efficiently structured into distinct layers as depicted in Figure 2.

Sensors and medical equipment collect data for diagnostic and therapeutic processes at the start of this organized design. These devices directly collect data from patients. The second level, a service layer that facilitates data transmission, receives the data after that. This layer's services collect data from the primary layer and transport it to the next layer, ensuring smooth data transfer. A health gateway connects IoT devices to the network. The IoT platform receives medical sensor data. Data assimilation and processing depend on the third tier. Verifying results before storing them in the IPFS blockchain repository is its major task. The layer includes an application that lets

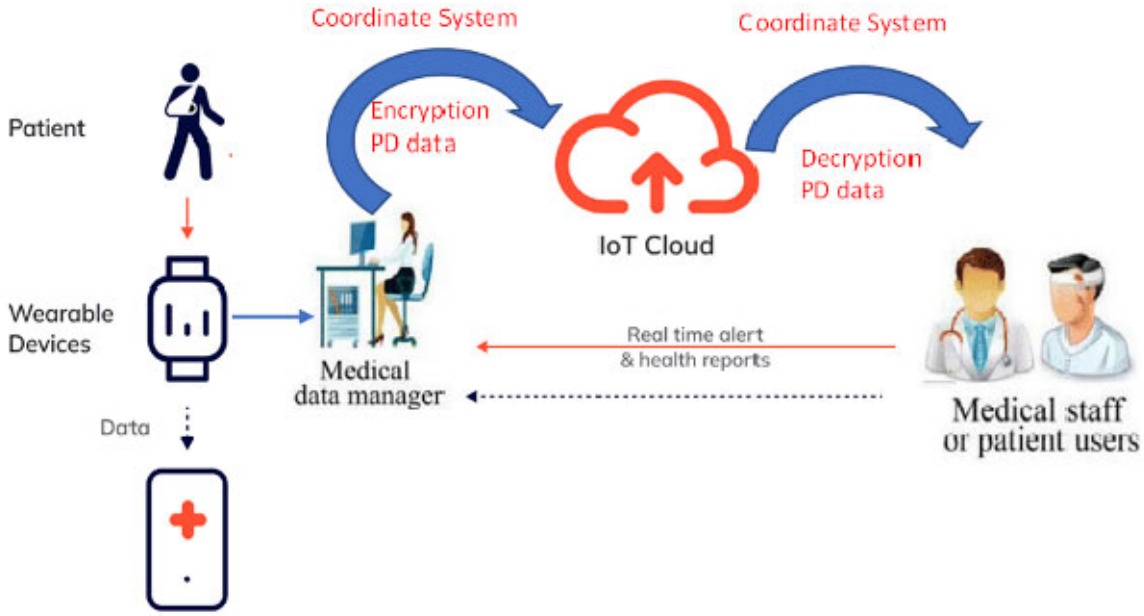

Figure 2. A systematic flow diagram of the proposed Smart-Coord Model.

authorized individuals access patient data via blockchain. We use RSA encryption for secure data retrieval. Primary users include doctors and nurses, and secondary users include health insurance companies and researchers. Each access attempt requires user authentication, improving data security. In this complex network, strong internet security protects communications and devices. These protocols use symmetric and asymmetric encryption to prevent security breaches. It also uses peer-to-peer file storage systems like IPFS, which use distributed hash tables, block exchanges, and other processes to protect and efficiently store data. Blockchain storage stores JSON data files encrypted with the powerful round-based AES-CBC cryptographic technique. Data confidentiality and integrity are ensured. This advanced healthcare-IoT system securely and anonymously transmits data through its application layer and handles it efficiently. Smart healthcare environments use advanced encryption and decryption to protect and manage data. This solution meets the needs of the needs of the digital healthcare industry.

4.1. Framework of Smart-Coord System

This section introduces the new Smart-Coord structure, which combines confidentiality and integrity policies. The framework is based on the relative location of a subject-object in a coordinate system. The following text describes the entire model and each policy's complex access control procedures. The integrity component of the architecture, shown in Figure 3(a), allows subjects with higher integrity levels to access objects above them on the coordinate plane. However, they can write things below, showing lower integrity. This means information is transferred from a higher integrity level to a lower one while enabling access to objects in the same integrity tier. This technique believes that information quality varies, with greater levels being better. Figure 3(b) shows that people can access items to their left on the coordinate plane, indicating less confidentiality. Meanwhile, they can write to objects on their right, representing a higher level of confidentiality. Here, the information flow transitions from lower to higher levels, adhering to the guidelines established in the BLP model. This maintains stringent control over access, safeguarding confidentiality at each level.

In Figure 4, the model synthesizes both confidentiality and integrity protocols to showcase the permissible information flow that complies with both policies concurrently. The graph demarcates specific zones within the coordinate plane where access aligns with the dual enforcement of integrity and confidentiality rules.

Figure 5 further explains this by representing confidentiality on the horizontal axis and integrity on the vertical axis. The harmonization of information flow

directives for both domains yields the ensuing access guidelines:

1) Subjects can read objects situated above and to the left of their position, where the reading rules for both policies are concurrently satisfied.
2) Subjects are authorized to write to objects positioned below and to their right, complying with the combined writing rules.
3) Access is denied for objects found above and to the subject's right, as this would contravene either integrity (writing) or confidentiality (reading) protocols.
4) Similarly, access is restricted for objects located below and to the subject's left to prevent violations of integrity (reading) or confidentiality (writing).

Before presenting an example, algorithm 1 delineates the essential definitions underpinning this framework.

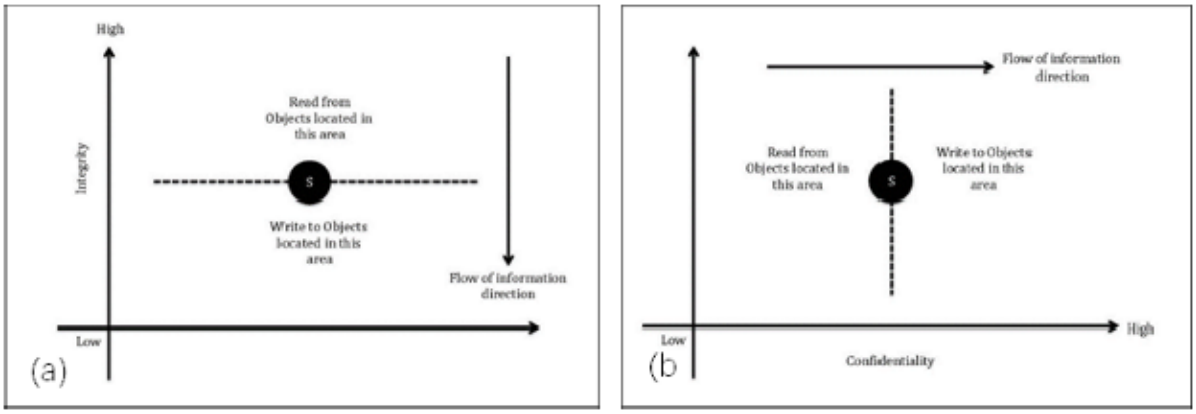

Figure 3. Integrity Access Control (a) and (b) Confidentiality Access Control.

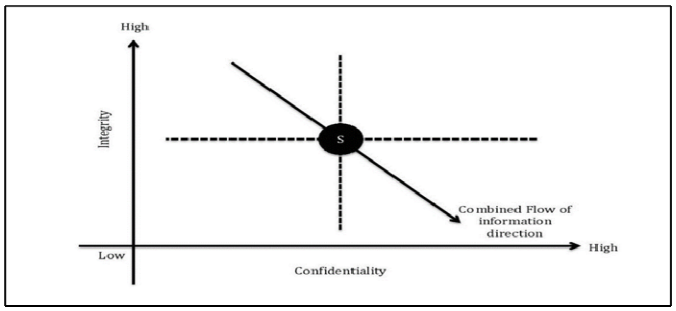

Figure 4. The direction of the flow in the combined model.

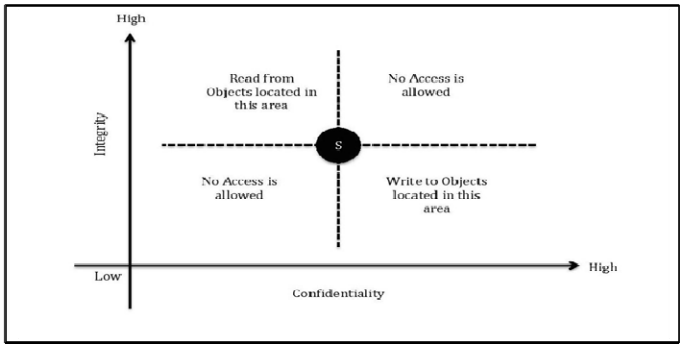

Figure 5. The combined model access rules.

Definition 1: A coordinate 2-D system consists of a pair **(*x*,*y*)** where both ***x*** and ***y*** are positive integers, ***X*** representing confidentiality level and ***Y*** representing integrity level.

Definition 2: A subject coordinate location $X_S \subseteq X$ and $Y_S \subseteq Y$.

Definition 3: An object coordinate location $X_O \subseteq X$ and $Y_O \subseteq Y$.

Definition 4: $\rightarrow$ is the flow of information from a subject to an object in a secure manner if permitted according to the rules and AC_s is the access request from a subject and LC_O is location of the object to be accessed.

Definition 5: Two access modes, ***R*** is access to read from an object and ***W*** is access to write too an object.

The previous rules are re-written in the following representation:

For each access request from a subject $AC_s(X_S, Y_S, Mode)$ to an object $LC_O(X_O, Y_O)$, the locations are compared according to the following:

- If the mode is ***R,*** then the following must hold, $(X_S \leq X_O) \cap (Y_S \leq Y_O)$ then it is said that the access request is granted and the information can flow from $LC_O(X_O, Y_O) \rightarrow AC_s(X_S, Y_S, R)$. **If the condition is not meet, then the access request is denied.**
- If the mode is ***W,*** then the following must hold, $(X_S \geq X_O) \cap (Y_S \geq Y_O)$ then it is said that the access request is granted and the information can flow from $AC_s\ (X_S, Y_S, W) \rightarrow LC_O(X_O, Y_O)$ **If the condition is not meet then the access request is denied.**
- All other locations on the plain are not allowed to have access to due to not meeting the above conditions.
-

4.2. Implementation of Smart-Coord System

In addressing the current challenges on the Internet of Things (IoT) healthcare sector, this study introduces a sophisticated solution grounded in blockchain technology. Utilizing the robust Ethereum Solidity programming language, we have devised smart contracts that act as a formidable barrier to potential network infringements, thereby ensuring both data integrity and confidentiality.

This framework uses cipher block chaining (AES-CBC) to encrypt the patient's data file before saving it in IPFS. The 'PD' file undergoes encryption to prevent unauthorized access. Upon storage, a unique hash value acknowledgment can verify it. This boosts data interchange trust. This decentralized strategy ensures that only authorized individuals can access vital data, eliminating the need for a central administrator. The PD is sent to IPFS storage using symmetric keys. Data transactions are safe and verifiable using a unique hash value. The blockchain stores the protected data file's hash value and the recipient's public key-encrypted symmetric key. This allows the recipient to decode the IPFS data file securely using their private key. This system also promotes new internet connections by utilizing blockchain smart contracts' immutability. Once signed, these contracts remain unmodifiable, thereby guaranteeing protocol compliance. Any production error-related modifications require manual data transmission, which hinders operations. Measuring blockchain performance indicators is difficult and necessitates careful consideration of network latency and block size. During the empirical phase, we tested the model on multiple blockchain networks to determine the gas required for setting up smart contracts, uploading encrypted data files and AES keys, and creating smart contracts. Figure 6 and Tables 1 and 2 indicate that Matic smart contracts are more efficient and cost-effective. In terms of gas and computation efficiency, this network outperformed others.

Finally, the implemented Smart-Coord system showcases exemplary performance in computational efficiency, offering a promising avenue for revolutionizing the security and integrity paradigms within the IoT-based healthcare sector.

5. EXPERIMENTAL RESULTS

In Figure 6, we elucidate the comparative analysis of transaction fees required for deploying smart contracts across different blockchain networks. This comparison is integral to understanding the cost-effectiveness of utilizing various blockchain networks within the Smart-Coord system. The statistic shows transaction costs on Kovan, Rinkeby, Binance, and Matic blockchains. Smart Value, which represents the cost of creating smart contracts on each network, is used to calculate fees.

Smart value 0.003000343 shows a low transaction cost on this test network. This score indicates the network's cost-effective smart contract implementation potential. The Rinkeby network, like the Kovan network, has a transaction cost of 0.003000343 Smart Value, making it an affordable smart contract alternative. With a smart value of 0.045080988, Binance has a much higher transaction cost. This increased price shows that implementing smart contracts on Binance may increase operating costs, reducing Smart-Coord's economic efficiency. Matic holds the lowest transaction cost with 0.001000456 smart value. The network's cost-efficiency may make it the most cost-effective smart contract deployment option in the proposed system.

Table 1. Comparison of three smart contacts.

Status	The transaction is successfully mined
Transaction Hash	0xf087759e0c8ab4e83e1ef1af98ffd5dd6ee94fdb99f6eb30659b4c44c20cd1ac
From	0x789b438da214e0c34b25164fdb8173f7937ba6da
To	Contract
Gas	0.000000003 Ether (3 Gwei)
Transaction Cost	0.000697965 Ether
Execution Cost	234,614
Hash	0xf073859e0c8ab4e83e1ef1af98ffd5dd6ee94fdb99f6eb30659b4c44c20cd1ac
Input	0xe56ba32c

Status	First contract value deployment	Second contract value deployment	Third contract value deployment
Transaction Hash	0x15634c8ac13876eacf17438b95baab7eb1cd504e310e267b6e480b5f73c4aa34	0xa46a5353dddd163a39afb8aeba88f033cad176be77b3886f93d758a214fa4528	0x7346f16ab5b91534987ba7c823658125175ee1c0c2990f63f4d7ebfbba2c33cb
From	0x871b438da214e0c34b25164fdb8173f7937ba6da	0x671b438da214e0c34b25164fdb8173f7937ba6da	0x671b438da214e0c34b25164fdb8173f7937ba6da
To	Smart Contract	Smart Contract	Smart Contract
Gas	0.000000004 Ether (3 Gwei)	0.000000003 Ether (3 Gwei)	0.000000003 Ether (3 Gwei)
Transaction Cost	0.0005566699 Ether	0.000699843 Ether	0.000699591 Ether
Execution Cost	235,495	235,543	235,459
Hash	x145634c8ac13876eacf17438b95baab7eb1cd504e310e267b6e480b5f73c4aa34	0xa46a5353dddd163a39afb8aeba88f033cad176be77b3886f93d758a214fa4528	0x7346f16ab5b91534987ba7c823658125175ee1c0c2990f63f4d7ebfbba2c33cb
Input	0xb788a82	0xb788a82	0xb788a82

Table 2. Gas of smart contracts

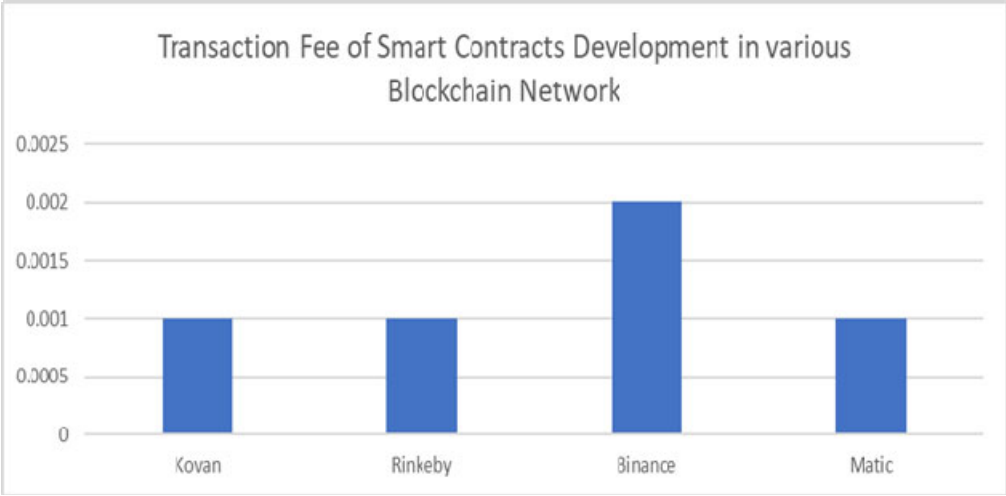

Figure 6. Comparisons of blockchain networks with transaction fees for smart deployment.

Figure 6 is essential for assessing the financial viability of adopting Smart-Coord across blockchain networks. It shows the Matic network's huge financial benefit, making IoT healthcare smart contract applications more cost-efficient and successful.

Developers must prioritize secrecy, integrity, and availability while building models. Confidentiality protocols restrict access to authorized users, protecting

system data. Ensuring communications are sent unchanged and received at their intended destination maintains integrity. Additionally, availability ensures users may get data without difficulty as needed.

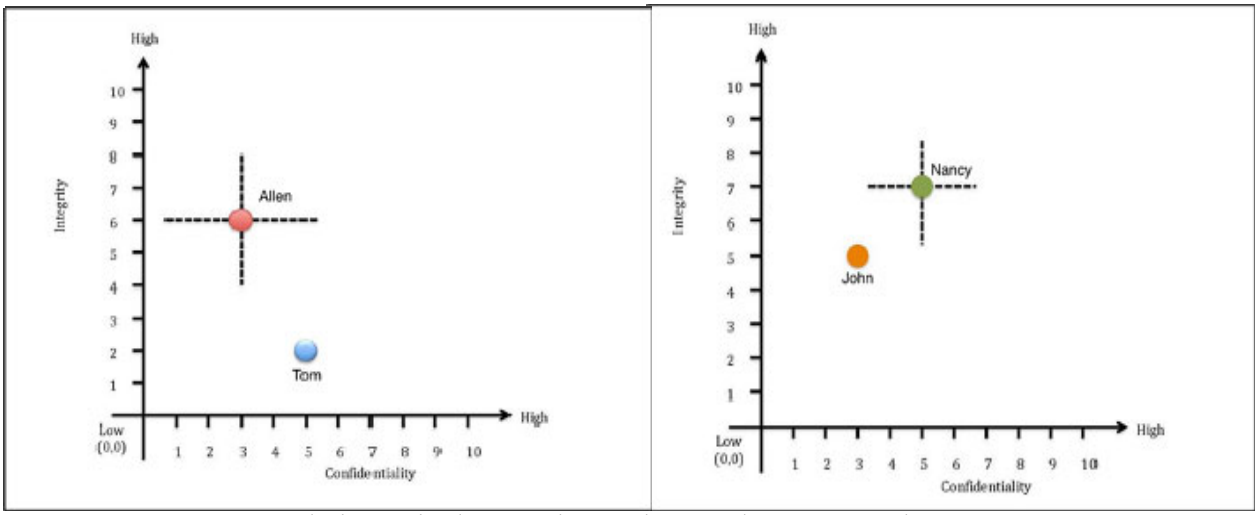

Figure 7. The interaction between the Development department employees

Table 3. Different roles and their respective integrity and confidentiality levels

Department	Role	Integrity level	Confidentiality level
Medical	Doctor	10	10
Development	Employee	2	5
Management	Medical Manager	10	10
Marketing	Secretary	7	5
Marketing	Employee	5	3
Management	Translator	8	4
Development	Secretary	6	3

Table 5. A comparative analysis of the proposed framework with state-of-the-art blockchain techniques

Scheme	Confidentiality	Data integrity	Data Availability	Data Security	Scalability
Zakzouk [28]	Yes	Yes	No	No	No
Vidhya [29]	Yes	Yes	Yes	Yes	No
Settipalli [30]	Yes	Yes	Yes	Yes	No
Smart-Coord	Yes	Yes	Yes	Yes	Yes

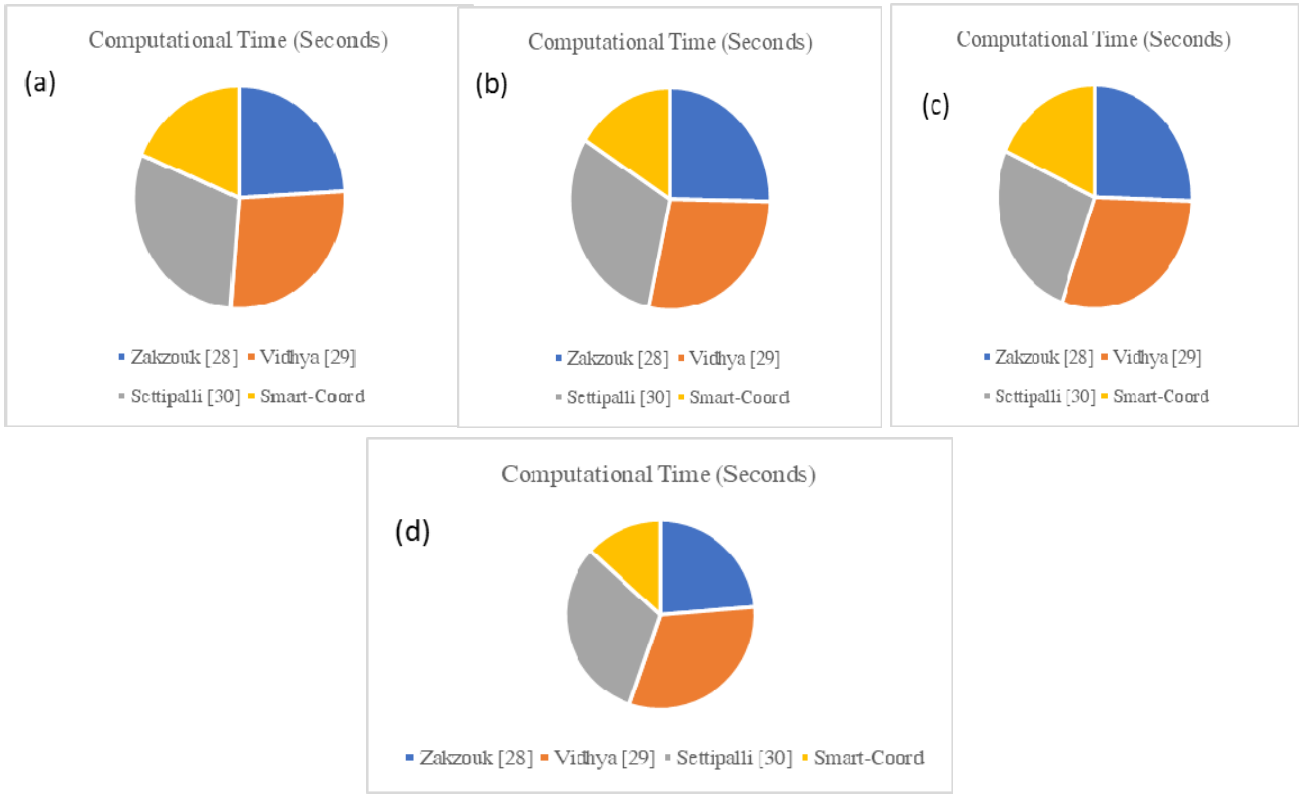

Figure 7. The computational time for different queries on patients' data file with encryption, where figure (a) shows the display of patient records, (b) insert patient records, (c) delete patient records, and (d) update the patient records.

To elucidate the functionality of the model, a hypothetical scenario is presented involving "Company A," a healthcare entity comprising several departments including medicine, research, accounting, and management. The model employs a role-based access control (RBAC) system, wherein integrity and confidentiality levels are ascertained

on a scale of 0 to 10, contingent upon individual job roles. Table 3 meticulously categorizes various roles alongside their respective integrity and confidentiality levels, offering a comprehensive overview of the security protocols in place.

Table 4 shows a clear link between employment and security by comparing Company A employees' honesty and confidentiality. This architecture enforces data security requirements, reduces breaches, and promotes operational security. Figure 7 of the research shows how workers use job and security clearance data. It aims to combine confidentiality and honesty with workers in their jobs. This strengthens data retrieval and employee interaction. This careful approach emphasizes data security, operational optimization, and a safe and collaborative workplace.

5.1. Comparative Evaluation

The Smart-Coord architecture outperforms current blockchain methods in data integrity, accessibility, security, secrecy, and scalability. Table 5 shows that Smart-Coord overcomes other systems' concerns, such as data security and scale, by providing a detailed comparison.

Specifically, the Smart-Coord system triumphs in all the evaluated categories—confidentiality, data integrity, availability, security, and scalability—as opposed to the schemes by Zakzouk [28], Vidhya [29], and Settipalli [30], which falter in one or more of these aspects. This robust performance signifies a breakthrough in blockchain technology, paving the way for a more secure and efficient data management system.

Further, the computational time analysis depicted in figure 7 accentuates the efficiency of the Smart-Coord system. It outperforms the referenced studies [28, 29, 30] across various operations such as select, insert, delete, and update actions on the data files. A nuanced breakdown of the computational times reveals that the Smart-Coord system markedly reduces the time required for these operations, thereby highlighting its computational supremacy. Smart-Coord's deletion time is 2.5 seconds, far

faster than other tests' 3.5 to 4.1 seconds. Figure 9 shows how long it takes to search patients' data files with encryption. Parts of the graphic divide the time required to display, insert, remove, and update patient records.

This advanced tool appropriately evaluates Smart-Coord's efficiency. The system's better computation time is crucial to blockchain system performance and efficacy. These results show Smart-Coord leads to blockchain. Data handling in healthcare and other industries is now secure and efficient due to enhanced security and computational performance.

6. Conclusions

IoT technologies in healthcare have transformational promise but severe security risks, especially for data integrity and privacy. This work introduces the innovative Smart-Coord system, which uses blockchain technology and a unique coordinate-based access control method to overcome these difficulties. IPFS for immutable data storage and intelligent Solidity Ethereum contracts for data integrity and confidentiality make the Smart-Coord framework a robust, secure, and scalable solution for managing sensitive healthcare data.

According to empirical evidence, the Smart-Coord solution not only improves IoT-based healthcare data management security and efficiency but also demonstrates significant scalability. With substantial increases in computational efficiency and cost-effectiveness across blockchain networks, particularly the Matic network, the Smart-Coord system proves its feasibility and scalability, providing reassurance about its economic viability. This makes it a promising and reassuring solution for the future of IoT healthcare ecosystem security.

The coordinate-based access control mechanism of Smart-Coord innovatively incorporates confidentiality and integrity policies, ensuring a comprehensive and balanced approach to managing and securing information flow. This paradigm effectively secures IoT-based healthcare systems by maintaining a careful balance of data privacy, accessibility, and integrity.

Finally, the Smart-Coord system advances IoT-based healthcare system security. Smart-Coord helps healthcare organizations implement and trust IoT technology by reducing data integrity and privacy threats. Successful deployment and shown security, efficiency, and cost-effectiveness merit future research and use of the Smart-Coord framework in real-world healthcare settings. The Smart-Coord system may be adapted to different IoT applications such as remote patient monitoring, medical device management, and healthcare supply chain tracking, and integrated with new technologies to improve its capabilities and usability.

References

[1] HaddadPajouh, H., Dehghantanha, A., Parizi, R.M., Aledhari, M. and Karimipour, H., 2021. A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, p.100129.

[2] Kumari, P. and Jain, A.K., 2023. A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures. Computers & Security, p.103096.

[3] Khan, A.A., Laghari, A.A., Li, P., Dootio, M.A. and Karim, S., 2023. The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. Scientific Reports, 13(1), p.1656.

[4] Malik, A., Bhushan, B., Parihar, V., Karim, L. and Cengiz, K., 2023. Blockchain-Powered Smart E-Healthcare System: Benefits, Use Cases, and Future Research Directions. In Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities (pp. 203-228). Cham: Springer International Publishing.

[5] Zhao, Z., Li, X., Luan, B., Jiang, W., Gao, W. and Neelakandan, S., 2023. Secure Internet of Things (IoT) using a Novel Brooks Iyengar Quantum Byzantine Agreement-centered Blockchain Networking (BIQBA-BCN) Model in Smart Healthcare. Information Sciences.

[6] Guergov, S. and Radwan, N., 2021. Blockchain Convergence: Analysis of Issues Affecting IoT, AI and Blockchain. International Journal of Computations, Information and Manufacturing (IJCIM), 1(1).

[7] Bashir, A.K., Victor, N., Bhattacharya, S., Huynh-The, T., Chengoden, R., Yenduri, G., Maddikunta, P.K.R., Pham, Q.V., Gadekallu, T.R. and Liyanage, M., 2023. A Survey on Federated Learning for the Healthcare Metaverse: Concepts, Applications, Challenges, and Future Directions. arXiv preprint arXiv:2304.00524.

[8] Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D.H. and Soufiene, B.O., 2023. Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications. Sustainability, 15(6), p.5346.

[9] Sotenga, P.Z., Djouani, K. and Kurien, A.M., 2023. A virtual network model for gateway media access control virtualisation in large scale internet of things. Internet of Things, 21, p.100668.

[10] Ryalat, M., ElMoaqet, H. and AlFaouri, M., 2023. Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0. Applied Sciences, 13(4), p.2156.

[11] Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y. and Iranmanesh, M., 2023. The Internet of Things (IoT) in Healthcare: Taking Stock and Moving Forward. Internet of Things, p.100721.

[12] Djenouri, Y., Yazidi, A., Srivastava, G. and Lin, J.C.W., 2023. Blockchain: Applications, Challenges, and Opportunities in Consumer Electronics. IEEE Consumer Electronics Magazine.

[13] Blaszczyk, M., 2023. Smart Contracts, Lex Cryptographia, and Transnational Contract Theory. Lex Cryptographia, and Transnational Contract Theory (January 6, 2023).

[14] Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S., 2020. Survey on IoT security: Challenges and solution using

machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, p.100227.
[15] Franzoni, F., Salleras, X. and Daza, V., 2022. AToM: Active topology monitoring for the bitcoin peer-to-peer network. Peer-to-Peer Networking and Applications, pp.1-18.
[16] Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, pp.13938-13959.
[17] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S. and Yang, Y., 2020. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR), 53(1), pp.1-32.
[18] Alam, T., 2020. mHealth communication framework using blockchain and IoT technologies. International Journal of Scientific & Technology Research, 9(6).
[19] Snehi, M. and Bhandari, A., 2021. Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. Computer Science Review, 40, p.100371.
[20] Jayabalan, J. and Jeyanthi, N., 2022. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 164, pp.152-167.
[21] Anitha Kumari, K., Padmashani, R., Varsha, R. and Upadhayay, V., 2020. Securing Internet of Medical Things (IoMT) using private blockchain network. Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, pp.305-326.
[22] Kadhim, K.T., Alsahlany, A.M., Wadi, S.M. and Kadhum, H.T., 2020. An overview of patient's health status monitoring system based on internet of things (IoT). Wireless Personal Communications, 114(3), pp.2235-2262.
[23] Haque, A.B., Muniat, A., Ullah, P.R. and Mushsharat, S., 2021, February. An automated approach towards smart healthcare with blockchain and smart contracts. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 250-255). IEEE.
[24] Rogers, D., 2019. A visit to the oracle: reviewing the state of construction industry digitalisation. Construction Research and Innovation, 10(1), pp.11-14.
[25] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R., Jolfaei, A. and Islam, A.N., 2023. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing, 172, pp.69-83.
[26] Saxena, R., Arora, D., Nagar, V. and Mahapatra, S., 2023. Blockchain in Healthcare: A Review. Recent Advances in Blockchain Technology: Real-World Applications, pp.165-185.
[27] Peng, S., Bao, W., Liu, H., Xiao, X., Shang, J., Han, L., Wang, S., Xie, X. and Xu, Y., 2023. A peer-to-peer file storage and sharing system based on consortium blockchain. Future Generation Computer Systems, 141, pp.197-204.
[28] Zakzouk, A., El-Sayed, A. and Hemdan, E.E.D., 2023. A blockchain-based electronic medical records management framework in smart healthcare infrastructure. Multimedia Tools and Applications, pp.1-19.
[29] Vidhya, S. and Kalaivani, V., 2023. A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. Peer-to-Peer Networking and Applications, pp.1-14.
[30] Settipalli, L., Gangadharan, G.R. and Bellamkonda, S., 2023. An extended lightweight blockchain based collaborative healthcare system for fraud prevention. Cluster Computing, pp.1-11.