IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155147

Real -Time Medicine Tracking and Distribution Coordination System

Ms. A. Nisha, ME.[1], Guruprasath M[2], Nagoor Meeran T[3]

Assistant Professor, CSE & Dhanalakshmi Srinivasan College of Engineering & Technology, India[1]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[2]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[3]

Abstract: The project not only addresses privacy and security needs but also the issue of trust in data sharing practices. By providing a privacy-preserving system that guarantees the confidentiality of individuals' information, the project aims at creating a secure and reliable environment for data sharing. Additionally, the proposed system will support the implementation of various use cases such as health care, banking, and e-commerce where data privacy and security are of paramount importance. The integration of various advanced techniques like decision tree, random forest, or support vector machine for data sensitivity assessment and the selection of the most suitable cryptographic technique for the different types of data to be processed will be also feasible. This will help in providing the best possible solution in terms of data privacy and accessibility.Ultimately, the project is expected to make a strong contribution to the development of privacy-preserving technologies through its innovative approach and the development of the proposed Intelligent Privacy Preserving Data Encryption and Anonymization System. In the long run, the project's results might have a significant impact on the future of data protection technologies as more and more organizations migrate to cloud services and share information across borders.

Keywords: Data protection, encryption, anonymization, privacy-preserving, cloud computing, big data analytics, interconnected systems, decision making, automated systems, trust

1.INTRODUCTION

The digital era has given rise to a very rapid and very large data generation and storage which has transformed the way of working of organizations, governments, and individuals. It is worth mentioning that all these transitions have been made possible through the broad use of cloud computing, the Internet of Things (IoT), big data analysis, and artificial intelligence to name just a few, which have resulted in continuous collection, processing, and sharing of sensitive data over various systems. Though, this data-centric environment is a boon to innovation and efficiency, at the same time it is fraught with very serious concerns regarding data privacy, security, and unauthorized access. Protection of sensitive information from cyber threats, data breaches, and misuse has now become one of the topmost challenges confronted by the modern information systems industry.The conventional data protection paradigm mainly revolves around encryption as the primary method for securing data during the phases of storage and transmission. Encryption is the process through which data is kept a secret by converting readable information to an unreadable format through the use of cryptographic keys. But in most cases when, data is shared, analyzed or processed by third parties, encryption alone is not sufficient. Once decrypted, the sensitive information can be exposed, attacked from within or misused. Moreover, with the growing amount of computing power and the emerging cyber-attack techniques, static encryption models have difficulty in providing the flexibility and long-term security required.Besides encryption, data anonymization has emerged as the principal method for safeguarding individual privacy. The objective of the Anonymization techniques is to eliminate or obscure personally identifiable information (PII) from datasets in such a way that the individuals can neither be recognized directly nor indirectly. Data masking, generalization, suppression, and pseudonymization are the most commonly used methods in healthcare, finance, social media, and research applications. Nonetheless, the traditional anonymization techniques often come with the drawback of re-identification risk, and others.

2.LITERATURE REVIEW

Q. Li, Y. Tian, Y. Zhang, L. Shen and J. Guo., (2025) [1] suggests an effective access control system relying on CP-ABE encryption that however mainly covers access policy protection and not complete data privacy. Besides that, no intelligent or adaptable mechanisms are employed in the proposed method to modify encryption and anonymization according to either data sensitivity or user behavior. Furthermore, the system does not tackle the issue of applying anonymization techniques in order to avoid identity leakage in the course of data sharing and analytics. Apart from that, the inadequacy

DOI: 10.17148/IJARCCE.2026.155147

of scalability and real-time performance in large-scale cloud and heterogeneous mobile environments is still an uncharted territory in this field of research.

Ding et al., (2024) [2] proposal of a privacy-preserving data processing system that uses homomorphic encryption and attribute-based access control comes with the drawback of incurring high computational overhead which limits its applicability to environments with real-time and limited resources. While the model focuses mainly on secure data processing, it does not include data anonymization as an additional measure to reduce privacy leakage risks. Furthermore, the access control policies are fixed and do not exhibit any intelligent adaptation to the varying user scenarios and threat levels. The capacity of the proposed method to handle large-scale cloud and big data deployments has not been looked into comprehensively in relation to its scalability the work of Aminuddin Mohd Kamal et al., (2025) [3] who proposed a privacy-preserving keyword search framework with secure search as its principal aspect, but not end-to-end data privacy management. Furthermore, themethod does not incorporate smart mechanisms that are capable of adjusting the access control or encryption policies depending on the user's actions or the sensitivity of the data. Moreover, the use of data masking methods is not included in the proposal, which may leave room for possible identity inference during the analysis of the outsourced data. The proposed scheme's performance impact and scalability concerning large-scale, multiperson cloud environments still need to be explored further.

While Bakas et al., (2020) [4] present an access control solution for symmetrically encrypted data in insecure cloud settings, the method depends mostly on fixed access rules without any smart flexibility to changing user situations. The approach centers around secure storage and access but does not utilize any data anonymization methods to further increase privacy protection. Also, the reliance on trusted execution environments like SGX poses issues about complexity and scalability of the deployment. The framework's ability and efficiency to cater large-scale, multi-tenant cloud data sharing scenario has not been thoroughly assessed yet.

Even though Morales-Sandoval et al., (2020) [5] suggest an attribute-based encryption scheme for safe storage, sharing, and retrieving cloud data, the system is essentially dependent on unmodifiable access policies that do not adapt to changing user roles and threats. Their work deals with encryption and searchable access but fails to deal with data anonymization so as to avoid the inference of identities during sharing and retrieval. Furthermore, the use of asymmetric pairing may cause a slowdown, which might be a drawback in large-scale cloud environments. The framework's integration of smart privacy-preserving measures has not yet been realized.

The authors, Aminuddin Mohd Kamal et al., (2025) [6] come up with a solid privacy-preserving keyword search system that integrates secret sharing and searchable encryption. However, the system is primarily focused on conducting secure searches and not on complete protection of data privacy. The method does not have any smart or adaptive capabilities that could automatically modulate access control and encryption according to the level of data sensitivity or user's activity. Moreover, the deployment of data anonymization techniques is not considered which can lead to users being vulnerable to inference and linkage attacks during the process of data outsourcing. The performance in terms of scalability and computation for the system in large-scale, real-time cloud environments is still an open research question.

Tao et al., (2023) [7] suggest a lattice-based matchmaking identity-based encryption scheme with post-quantum security for IoT environments, but the model is mainly concerned with secure key matching and not comprehensive data privacy preservation. The method does not employ data anonymization techniques to ensure anonymity for devices or users while sharing data. Moreover, the scheme lacks the ability to smartly adapt to access control in heterogeneous and large-scale IoT networks. More studies are needed to assess the performance and scalability of the solution under the true nature of IoT constraints and vast deployments of devices.

Y.You., (2025) [8] However, while You puts forward a blockchain-based scheme as a solution for secure sharing and encryption control of e-commerce data, the spotlight is mainly on decentralized access control, not on intelligent privacy preservation. The framework does not incorporate any adaptive mechanisms that would enable it to at any time change encryption and access policies, depending on both data sensitivity and user behavior. Moreover, data anonymization techniques that are necessary for the prevention of exposing user identities and transaction patterns are not part of this system. The issue of computational overhead and scalability difficulties associated with blockchain-based systems for the large-scale e-commerce arena is still not fully tackled.

Iwamura and Kamal., (2025) [9] have developed a user authentication process that is both secure and totally safe, using secret sharing and information-theoretic security as the basis. The writers, nevertheless, concentrate on authentication and ignore the broader topic of data privacy. The authors' technique does not allow for any kind of data encryption or anonymization to be used in the case of authentication and thus keeps the sensitive user data exposed. Also, the system

DOI: 10.17148/IJARCCE.2026.155147

is fixed; it lacks any intelligent or adaptive functions to modify itself in line with the changing threat models and user behavior. Another question that has to be researched is the proposed authentication scheme's compatibility with scalable cloud or data-sharing environments.

Shen et al., (2025) [10] have put forward a method of retrieving images in a secure and efficient way that uses additive secret sharing; however, this method is mainly designed for content-based image retrieval and not for general data privacy preservation. In the model, the images are not anonymized in the user identities or context mindfulness during image queries. Furthermore, the access control system does not have the necessary and smartly adaptable features to privacy levels adjustment according to the user's trust or sensitivity of the query. The overall performance of the method regarding large-scale multimedia datasets and real-time cloud settings in terms of scalability and computational overhead still needs to be investigated.

In the paper, Singamaneni et al., (2024) [11] present a quantum hash-based attribute-based encryption scheme, among other things, for the secure integrity and control of data in mobile edge computing. The method is based mostly on enforcing integrity and providing access to the data rather than offering complete privacy. Moreover, data anonymization methods that protect both the customer's sensitive identity and the user's behavior are not part of the model. Besides, the system is not capable of automatically adjusting privacy and encryption levels according to contextual risk or user behavior. The real-world, large-scale edge environments where quantum-assisted mechanisms have not been properly explored in terms of practical feasibility and scalability.

Even though the work of Farhadighalati et al., (2025) [12] is a very extensive systematic review of access control models and their challenges, the analysis is the main focus of the study and nothing similar to a implementation-oriented privacypreserving framework is suggested. The reviewing work points out adaptation problems but does not include any smart ways of implementing dynamic, real-time access control in data-centric systems. Moreover, the issue of combining access control with data encryption and anonymization techniques is not so much discussed. One of the most important points that can still be investigated is the practical evaluation of privacy-preserving access control models in large-scale cloud and big data environments.

Jastaniah et al., (2024) [13] suggest a configurable and privacy-preserving framework for processing wearables data based on homomorphic encryption and user-centric access control. However, the suggested solution mostly deals with secure computing rather than full data privacy management. The proposed solution does not consider data anonymization as an additional measure to protect the user's identity and sensitive information further. Besides, the access control system does not possess the required intelligence to alter privacy settings according to the circumstances, risk level, or user activity. The framework's scalability and performance need to be tested in extensive IoT and real-time wearable ecosystems which are still unanswered questions.

Even though Dheeba et al., (2025) [14] improve AES encryption with S-Box optimization to protect electrical drives from man-in-the-middle attacks, their method is restrictive to the device level communication security only. The authors do not consider data privacy that is enabled by anonymization or secure data sharing except for control signals. In addition, the encryption method is fixed and fails to intelligently adjust to developing threat situations. The potential of the suggested technique in massive, cloud-integrated, or data-centric environments has not been examined.

Razi et al., (2025) [15] do present a complete review of privacy-preserving technologies like encryption, anonymization, synthetic data, and differential privacy; however, their work remains mainly descriptive and does not provide a unified implementation framework. Moreover, the study does not suggest smart solutions for the dynamic selection or the combination of privacy methods depending on the data's level of sensitivity and the usage context. Interoperability and trade-off management between encryption and anonymization techniques are not also experimentally evaluated. It is still an open research challenge to practically validate adaptive, end-to-end privacy-preserving systems in real-world ecosystems.

It is a fact that Cilloni and others., (2024) [16] through their research, have shown that machine learning can uncover personal information even from datasets that have been anonymized, but the study has not suggested any strong ways of protection instead of exposing the flaws. The authors do not combine encryption with anonymization to offer multilayered privacy protection. Furthermore, the development of smart, flexible anonymization methods that can withstand inference and linkage attacks is not taken into account. The whole scenario of developing privacy-preserving systems that are practical and at the same time providing the right balance between data utility and resistance to AI-based reidentification is still an open research gap.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155147

3.BACKGROUND AND MOTIVATION

The pharmaceutical industry plays a vital role in maintaining public health and ensuring the safe delivery of medicines to patients. Proper medicine tracking and distribution management are essential to avoid medicine shortages, expired stock usage, and counterfeit medicine circulation. In many healthcare organizations, medicine management processes are still handled using manual registers, paper-based documentation, or traditional software systems with limited realtime monitoring capabilities. These methods often create operational inefficiencies and increase the possibility of human errors.

One of the major challenges in the pharmaceutical supply chain is the inability to track medicine movement accurately from manufacturers to distributors, pharmacies, and hospitals. Without a proper tracking mechanism, medicines may be misplaced, delayed, or distributed incorrectly. Additionally, counterfeit medicines have become a serious global issue that threatens patient safety and reduces trust in healthcare services. Traditional barcode systems and manual verification methods are often insufficient to prevent fake medicine circulation because they can be easily duplicated or manipulated. Modern technologies such as QR codes, blockchain, smart contracts, and decentralized storage systems provide better solutions for secure medicine management. QR codes allow quick access to medicine information and enable real-time verification during distribution. Blockchain technology provides tamper-proof transaction storage, ensuring transparency and security throughout the supply chain. Smart contracts automate verification processes and reduce manual intervention, while decentralized storage systems like IPFS improve secure file management.

The QR Code Based Real-Time Medicine Tracking and Distribution Coordination System was developed to address these issues by creating a secure, transparent, and efficient medicine tracking platform using modern web technologies and real-time data synchronization.

The main motivation behind developing the QR Code Based Real-Time Medicine Tracking and Distribution Coordination System is to improve medicine safety, transparency, and efficiency within the pharmaceutical supply chain. Existing systems often suffer from poor tracking capabilities, delayed updates, inventory mismatches, and weak verification mechanisms. These problems may lead to medicine wastage, incorrect stock management, and circulation of counterfeit medicines.

Another important motivation is the growing need for real-time medicine monitoring. Healthcare organizations require systems that can provide instant updates regarding medicine location, stock availability, shipment status, and expiry information. Real-time tracking helps reduce operational delays and improves coordination between manufacturers, distributors, pharmacies, and hospitals.

The increase in counterfeit medicines worldwide also motivated the development of this project. Fake medicines can create serious health risks for patients and negatively affect healthcare systems. By integrating QR code verification and blockchain security, the proposed system helps verify medicine authenticity and prevents unauthorized modifications to transaction records.

The project is also motivated by the need to reduce manual paperwork and improve automation in pharmaceutical operations. Digital record management reduces human errors, improves data accuracy, and enhances overall operational efficiency.

Furthermore, advancements in technologies such as React.js, Node.js, blockchain, IPFS, and cloud computing encouraged the development of an intelligent medicine tracking platform capable of supporting secure and scalable healthcare solutions for real-world environments.

4. ANALYSIS AND DISCUSSION

The analysis and discussion of the QR Code Based Real-Time Medicine Tracking and Distribution Coordination System explain the overall performance, functionality, reliability, and effectiveness of the developed application. The system was designed to improve medicine tracking, verification, inventory management, and distribution coordination using QR code technology, blockchain integration, and real-time database synchronization.

During the implementation and testing phases, the application successfully performed all major functionalities including user authentication, medicine registration, QR code generation, shipment tracking, inventory updates, medicine

DOI: 10.17148/IJARCCE.2026.155147

verification, and report generation. Each module operated according to the specified project requirements without major system failures or data inconsistencies.

The QR code verification mechanism proved highly effective in tracking medicine movement throughout the supply chain. Every medicine batch received a unique QR code containing important information such as medicine name, batch number, manufacturing date, expiry date, and shipment details. When scanned, the system instantly retrieved medicine information and updated transaction records in real time. This process improved transparency and reduced the possibility of medicine duplication and counterfeit distribution.

The integration of blockchain technology improved the security and reliability of medicine transaction management. Blockchain records remained tamper-proof and secure because each transaction was stored permanently within the distributed ledger. Smart contracts automated verification procedures and reduced manual intervention during medicine validation and transaction approval processes. This automation minimized operational delays and improved system efficiency.

Database analysis showed that the application handled medicine records, user data, inventory details, and transaction logs efficiently. Real-time synchronization between frontend and backend modules ensured accurate data updates across the entire system. The database also maintained consistency during multiple user operations and concurrent access conditions.

Performance testing demonstrated that the application responded quickly during login authentication, QR code scanning, dashboard loading, report generation, and medicine verification operations. Even when multiple users accessed the system simultaneously, the application maintained stable performance without major slowdowns or server failures.

Security analysis confirmed that the system successfully protected sensitive information using JWT authentication, password encryption, and role-based access control mechanisms. Unauthorized users could not access protected modules or modify transaction records without proper authentication permissions.

The discussion of results indicates that the proposed system significantly improves medicine supply chain transparency, inventory monitoring, and counterfeit medicine prevention compared to traditional tracking methods. The centralized dashboard and real-time monitoring features also improved communication and coordination among manufacturers, distributors, pharmacies, and administrators.

Although the system achieved its primary objectives successfully, certain improvements can be implemented in future versions. Features such as AI-based counterfeit detection, GPS-enabled shipment tracking, mobile application support, cloud deployment, and advanced analytics dashboards can further improve scalability, automation, and real-world usability.

Overall, the analysis confirms that the QR Code Based Real-Time Medicine Tracking and Distribution Coordination System is secure, reliable, efficient, and suitable for modern pharmaceutical supply chain management environments.

5. CONCLUSION

The QR Code Based Real-Time Medicine Tracking and Distribution Coordination System was successfully designed and developed to provide a secure, transparent, and efficient solution for medicine tracking and distribution management. The project effectively addressed the major problems found in traditional medicine management systems such as manual record maintenance, lack of real-time monitoring, inventory mismatches, and counterfeit medicine circulation.

The system successfully integrated QR code technology, blockchain security, smart contracts, and decentralized storage to improve medicine verification and transaction transparency throughout the pharmaceutical supply chain. Each medicine batch was assigned a unique QR code that enabled fast and accurate tracking during manufacturing, distribution, and pharmacy operations. Real-time updates helped improve inventory monitoring and reduced operational delays.

The implementation of blockchain technology provided tamper-proof transaction storage and secure record management, while smart contracts automated verification and validation processes. Role-based authentication and secure login mechanisms ensured proper access control and protected sensitive system data from unauthorized users. Testing and performance analysis confirmed that the application operated efficiently under different working conditions. All modules such as medicine registration, QR code generation, shipment tracking, medicine verification, report generation, and

DOI: 10.17148/IJARCCE.2026.155147

inventory management functioned correctly without major errors. The system also demonstrated stable performance during multiple user access conditions and maintained accurate database synchronization. The project achieved its main objectives of improving medicine transparency, reducing counterfeit medicine risks, minimizing manual workload, and enhancing communication between manufacturers, distributors, pharmacies, and administrators. The proposed solution demonstrates how modern web technologies and secure digital verification mechanisms can improve pharmaceutical supply chain management in real-world healthcare environments. In conclusion, the QR Code Based Real-Time Medicine Tracking and Distribution Coordination System provides a reliable, scalable, and secure platform for medicine monitoring and verification. The project has significant potential for future enhancements such as mobile application integration, AI-based counterfeit detection, GPS-enabled delivery tracking, cloud deployment, and advanced analytics, which can further improve system intelligence and operational efficiency in large-scale healthcare industries

REFERENCES

[1]. N. Nyi Myo, A. Boonkong, K. Khampitak and D. Hormdee, "A Two-Point Association Tracking System Incorporated With YOLOv11 for Real-Time Visual Tracking of Laparoscopic Surgical Instruments," *IEEE Access*, vol. 13, pp. 12225–12238, 2025.

[2]. Y. Zhong, H. Xu and R. Yao, "An Innovative Research on Intelligent Nursing Medicine Delivery Trolley," in *2025 5th International Conference on Sensors and Information Technology*, Nanjing, China, 2025, pp. 603– 608.

[3]. W. Lin, J. Shi, H. Ma, L. Wang, J. Hu and C. Zhou, "Vision-Based Real-Time Tracking of Surgical Instruments in Robot-Assisted Laparoscopic Surgery," in *IECON 2023 - 49th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, 2023, pp. 1–6.

[4]. A. Boudagdigue, A. Benslimane, A. Kobbane and J. Liu, "Trust-Based Certificate Management for Industrial IoT Networks," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12867–12885, 2023.

[5]. D. Bradić, D. Delija, G. Sirovatka and M. Žagar, "Creating Own NFT Token Using ERC721 Standard and Solidity Programming Language," in *MIPRO 2022*, 2022, pp. 1053–1056.

[6]. Calderón, "Blockchain and NFTs as Secure and Reliable Tools for Academic Certificates Verification," in *IEEE CONCAPAN Conference*, 2023, pp. 1–6.

[7]. A. C. H. Chen, "Comments on L-ECQV: Lightweight ECQV Implicit Certificates for Authentication in IoT," *IEEE Access*, vol. 13, pp. 93883–93891, 2025.

[8]. M. Fartitchou, I. Lamaakal, K. E. Makkaoui, Z. E. Allali and Y. Maleh, "BlockMEDC: Blockchain Smart Contracts System for Securing Moroccan Higher Education Digital Certificates," *IEEE Access*, vol. 13, pp. 39152–39175, 2025.

[9]. C. Fioravanti, C. N. Hadjicostis and G. Oliva, "A Control-Theoretical Zero-Knowledge Proof Scheme for Networked Control Systems," *IEEE Open Journal of Control Systems*, vol. 3, pp. 416–428, 2024.

[10]. M. Hao, C. Shang, S. Wang, W. Jiang and J. Nie, "UAV-Assisted Zero Knowledge Model Proof for Generative AI," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 13441–13454, 2025.

[11]. H. Huang *et al.*, "BrokerChain: A Blockchain Sharding Protocol by Exploiting Broker Accounts," *IEEE Transactions on Networking*, vol. 33, no. 4, pp. 1930–1945, 2025.

[12]. IEEE, "Draft Standard for Application Technical Specification of Blockchain-Based E-Commerce Transaction Evidence Collecting," *IEEE P3802/D2.0*, pp. 1–20, 2021.

[13]. R. K. Kim, G. S. Lee, J. G. Park, H. Lee, S. I. Moon and J. W. Chang, "Optimal Scheduling of Integrated PVESS Systems," *IEEE Transactions on Sustainable Energy*, vol. 16, no. 2, pp. 1372–1387, 2025.

[14]. Li *et al.*, "Blockchain-Based Privacy-Preserving Mobile Edge Computing Framework," *IEEE Transactions on Green Communications and Networking*, vol. 9, no. 2, pp. 711–724, 2025.

[15]. T. Ma, T. Feng, Q. Li and J. Xiong, "Blockchain-Enabled Secure Distributed Data Aggregation," in *IEEE GLOBECOM 2022*, 2022, pp. 4383–4388.

[16]. H. Moon, H. Chung, J. Ryu, K. Hwang, H. Moon and W. Park, "Blockchain Knowledge and Intention to Use Blockchain Services," *IEEE Access*, vol. 13, pp. 74521–74530, 2025.

[17]. B. Naidu, R. Wanjari, R. Bhojwani, S. Suchak, R. Baser and N. K. Ray, "Blockchain-Based Medicine Tracking and Verification System for Pharmaceutical Supply Chains," in *International Conference on Smart Healthcare Systems*, 2023, pp. 112–118.

