Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 6, pp. 2503–2519
DOI : 10.47974/JDMSC-2756

An efficient and secure mobile agent based model for medical health care data protection

Anuradha Singh *
Department of Information Technology
JSS Academy of Technical Education
Noida 201301
Uttar Pradesh
India

Pradeep Kumar †
Ajay Kumar §
Department of Computer Science & Engineering
JSS Academy of Technical Education
Noida 201301
Uttar Pradesh
India

Nishant Gupta ‡
Department of Computer Science & Engineering
ITS Engineering College
Greater Noida 201310
Uttar Pradesh
India

R. N. Ravikumar @
Department of Computer Engineering
Marwadi University
Rajkot 360003
Gujarat
India

* *E-mail:* anuradha.singh@jssaten.ac.in (Corresponding Author)
† *E-mail:* pradeep8984@gmail.com
§ *E-mail:* ajaykrverma@jssaten.ac.in
‡ *E-mail:* nishantlira@gmail.com
@ *E-mail:* rnravikumar.cse@gmail.com

Dharm Raj [#]
Department of Computer Science & Engineering
Sharda University
Greater Noida 201310
Uttar Pradesh
India

Abstract

Mobile agents are powerful advanced technology for distributing computing with intelligent and autonomous execution of assigned tasks. During the execution, mobile agent utilizes a specific life cycle in malicious environment. Collaboration of mobile agents for securing medical data like patient data, patient medical report etc. play important role. In the digital world, smart health care system is required. For secure transfer of patient information from one hospital to another hospital a framework is proposed based on variable threshold Chinese remainder theorem with present and pride lightweight cipher. Chinese remainder theorem is used for secret sharing of key among hospitals. The VT-CRT technique dynamically modifies the threshold in response to system variables, improving adaptability and security while minimizing computing cost. Present and pride are used for encryption and decryption of electronic medical records. This is the collaborative approach of mobile agents for creation and recreation of secret keys among hospitals for authentication. The effectiveness of the healthcare system is determined by the ability to share medical information safely and effectively. The lightweight PRIDE and PRESENT encryption methods provide efficient and low-latency encryption that is ideal for limited resources medical devices. The framework is compared to popular cryptographic systems like AES, DES, and Blowfish in terms of time complexity, communication cost, flexibility, and memory usage. Investigational findings show that the proposed framework enhances security while maintaining optimal speed, making it a reliable solution for safe patient's information sharing in medical applications.

Subject Classification: *94A60, 68M14, 68M10.*

Keywords: *Mobile agents, Variable threshold CRT, Lightweight encryption and decryption, PRIDE cipher, Present cipher, Key sharing, Secure medical data.*

1. Introduction

In the current era the population of every country is increasing in an exponential way. Every country has limited resources to handle the medical issue of a person [1]. Health care is an important issue because of rapidly increasing diseases and patients. Every patient has medical history. In emergency cases, hospitals can utilize the data of patients for fast treatment. There are many diseases, like sugar, heart related diseases, asthma etc. Instead of wasting time to do tests again and again by any hospital there is a requirement

[#] *E-mail:* **dharmraj4u@gmail.com**

of centralized data for every patient. So, every hospital can utilize this data for fast and reliable treatment of patients. The modern medical industry is adopting advanced technology for providing efficient healthcare facilities. Hospitals can frequently collect patients documents and evaluate information about patients to ensure suitable treatment for all situations. By using electronic health care record (EHR) hospitals can treat patients in all emergencies. Every hospital maintains their patient data Electronic Health record on cloud. Every hospital can access this data 24/7 for all emergencies [2]. Allowing hospitals to share critical information about patients, such as medical history, diagnostic findings, and treatment plans, enables healthcare practitioners to make educated decisions, decreasing medical intervention delays and increasing patient outcomes. Sharing data about patients is not secure [3]. So, the security of patient data is a prime concern in advanced technology. Total 1.5 million medical equipment have been hacked in the past ten years as a result of software flaws in their wireless networks and cloud-based services.41.4 million Records of patients were hacked in 2019, reported to the Protenus Breach Barometer. There are many users like doctors, medical students; medical insurance agents, etc want to get this data for their use [4]. Hospitals, Universities, clinical research centre, insurance company and pharmaceutical company utilize patient data as per their requirement shown in Figure 1.

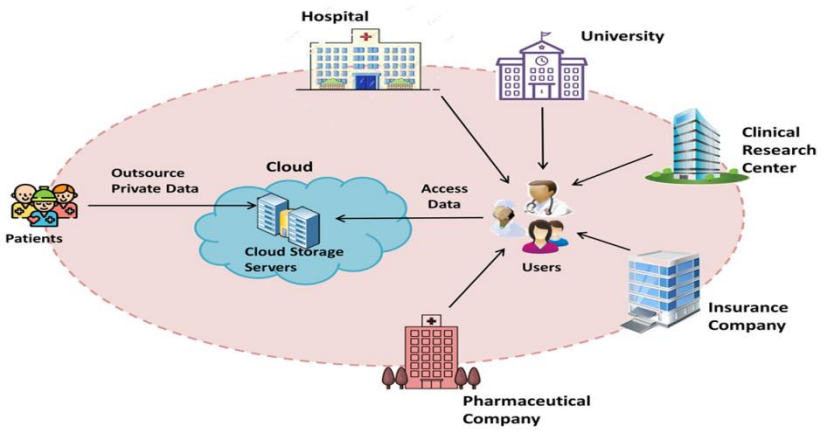

Figure 1
Healthcare data sharing

Although it's obvious advantages, health information sharing among institutions has several barriers that should be overcome to assure privacy, confidentiality, and efficiency. One of the most pressing concerns is the safety and confidentiality of data as private patient data is exposed to cyber-attacks unauthorized use and compromises. Challenges about data authenticity and integrity occur when medical information is shared between institutions. Insufficient recording methods, mistakes during data input and insufficient

documents can all affect the accuracy of transmitted health information, potentially resulting in inaccurate diagnoses or improper treatments. To make sure the accuracy of transmitted information about patients, the institutions should adopt rigorous data verification and validation methods.

Mobile agent technology has rapidly advanced, transforming data transfer and confidentiality in a variety of sectors, mainly in healthcare [5]. Mobile agents are small programs that can migrate between network nodes to perform functions such as safe information retrieval, the process and communication as shown in Figure 2.

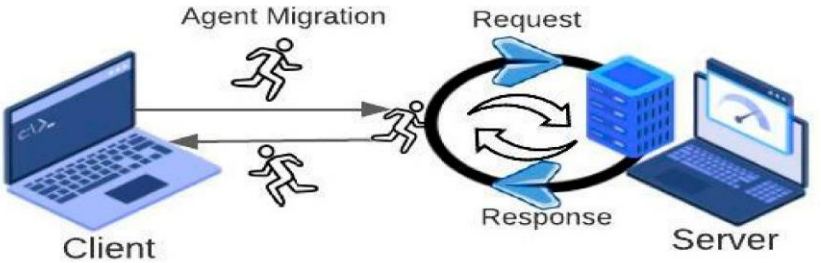

Figure 2
Mobile Agent for sharing of Information

Mobile agent provides secure exchange of information for the medical field, easy communication among hospitals, cloud-based record and IoT enabled medical equipment. But these benefits are linked with serious security challenges, especially regarding maintaining confidentiality, integrity and efficiency in key distribution and data encryption. The growing frequency of cyber-attacks, eavesdropping assaults, and illegal access necessitates the development of robust cryptographic techniques to secure mobile agent transmission [6].

Application of mobile agent in health care domain is shown in Figure 3.

One of the most challenging aspects of securing mobile agents is distributing cryptographic keys efficiently while minimizing computing overhead. Traditional key-sharing mechanisms such as Shamir's Secret Sharing and Threshold Cryptography, mostly exhibit inefficiency in dynamical multi-agent contexts. A variable Threshold Chinese Remainder (VTCRT) theorem for secret key sharing is proposed to address the problem [7]. Proposed technique adjusts the threshold value dynamically as the requirement arise during each transaction. Along with secure key sharing, encryption is important for securing medical data from illegal access and modification. Conventional encryption algorithms techniques such as AES, DES and Blowfish provide high security assurances but mostly have large computational costs rendering them unsuitable for limited resources medical equipment and applications for healthcare in real time. To address this constraint proposed the lightweight cryptographic approaches PRIDE and PRESENT ciphers into our system. Present or pride

Cipher provides low latency encryption with minimum resource usage, ensuring efficient, real-time data protection while maintaining security [8].

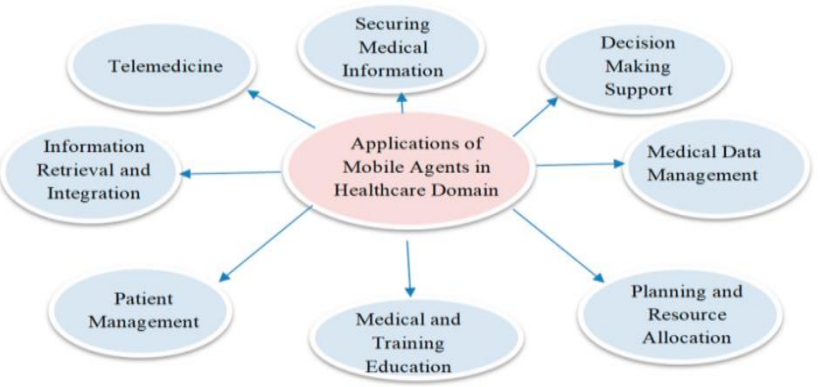

Figure 3
Application of Mobile agent in health care Domain

1.1 *Electronic Health data*

To ensure the safety and confidentiality of e-health data, this section outlines security concerns, needs, solutions, research trends, and unresolved issues. Figure 4 shows hierarchy for security issues, requirements of security, and solutions of security for electronic health data [9].

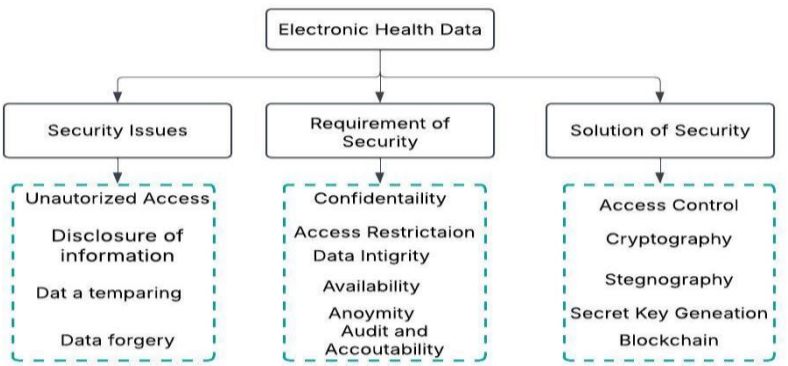

Figure 4
A Hierarchy of the safety and confidentiality for electronic health Record

The objective of this paper is to create an optimum security framework for mobile agents that balance security, efficiency, and scalability in medical data-sharing systems [10]. The paper is organised as follows: Section 2 discus about the existing literature survey of secure medical information transmission among different authorities. Section 3 explains proposed VT-CRT-based key-sharing

scheme and its integration with PRIDE and PRESENT ciphers [11]. Section 4 discusses experimental setup, performance analysis, and compares with traditional key sharing and encryption and decryption approach. Finally, Section 5 discusses the conclusion and the extent of the future.

2. Related works

This segment briefly discusses current advances in sharing information strategies in the cloud computing environment. Numerous previous studies included research on different issues of confidentiality and safety in medical care.

Zhu et al. [12] Identify critical challenges in healthcare IoT (HIoT) networks and suggest a safe and effective method for exchanging medical data, called ESDS, to ensure great efficiency, authenticity verification, and privacy protection. To accomplish this, developed an aggregate sign cryption mechanism in a locally verifiable manner. Security evaluation confirms that ESDS upholds accessibility, secrecy, and unforgeability, meeting the security requirements for exchanging medical data in HIoT environments. Additionally, performed both theoretical and experimental evaluations of its efficiency. The findings shows that ESDS is practical and feasible that offers reduced computational and communication overhead while enabling efficient verification due to its locality property. Kumar et al. [13] Proposed system which increases the security of sensitive Cloud-stored private medical records by implementing end-to-end encryption using the AES client-side encryption algorithm. Based on a predefined criteria file access is granted, ensuring that only authorized users can retrieve specific files. For example, only emergency departments have access to designated files and are restricted from viewing or downloading others. When a person downloads a file, they must ask for a key to open it. If the user is authenticated, the file owner securely gives the key through the ECDH key exchange method. Only users who enter the correct key can decrypt the file, guaranteeing both file and key security. Even if an attacker compromises on the server, they cannot access the file's contents. Additionally, the key is remains undiscoverable during transmission, further strengthening the security.

Fang et al. [1] introduced a novel data-sharing framework along with a method for controlling data access. In this system, doctors submit applications, and data of patient is processed within the hospital's centre for medical data. The data is stored on semi-trusted servers, enabling selective electronic health record sharing among various medical facilities and physicians. This approach addresses privacy concerns when granting access to patients' medical information. To ensure accountability, both patients and physicians are required to add digital watermarks linked to their identities when uploading data, allowing traceability in case of data modification or leakage. Comprehensive analytical and experimental results demonstrate the effectiveness and safety of the suggested plan. Gupta et al. [14] article presented the SP-MAACS plan, a fully secure and multi-authority access control system that is safe and protects

privacy for sharing healthcare data in the cloud. It enables data owners to exchange their information with users across both open and restricted domains and enhancing the system's scalability and flexibility. The use of a policy for partially concealed access safeguards the privacy of both users and data owners. Implementation results indicate that the scheme not only preserves privacy and ensures the conventional model of adaptive security but also optimizes decryption costs that improves overall efficiency.

Oh et al. [15] presented a safe and confidential data-sharing system that balances secrecy and data confidentiality. By utilizing methods for private set intersection and key aggregate encryption, the scheme enables secure data sharing while preventing the exposure of sensitive information. To assess its robustness against potential attacks, both formal and informal security studies are performed such as Scyther and Burrow Abadi Needham logic. Additionally, evaluated the execution time of cryptographic operations using a Mult Precision integer and rational arithmetic cryptographic library, comparing this approach with current systems in terms of time complexity, computational cost, and security. The results confirmed that the proposed scheme provide strong security and efficiency, contributing to the field by ensuring both privacy protection and secure, flexible sharing of medical data. Scheibner et al. [16] Integrated two sophisticated technologies that improve privacy, such as safe multiparty computation and homomorphic encryption into a unified framework called multiparty homomorphic encryption. This approach ensures mathematical privacy guarantees while offering a performance advantage over using either technique individually. Also argued that multiparty homomorphic encryption meets the criteria for sharing medical data under the General Data Protection Regulation (GDPR) of the European Union, which serves as a global standard to safeguard data. Data shared and processed through this method can be classified as anonymized, reducing the need for complex contractual agreements between institutions. By facilitating secure and privacy-preserving data sharing, the proposed approach can accelerate medical research and encourage healthcare and research institutions to adopt common data interoperability standards. Bodur and Yaseen [17] proposed scheme where medical data is categorized into sensitive and non-sensitive patient information. Proof of Work, Proof of Stake, and Proof of Authority are three consensus techniques that are used and evaluated based on their performance. The analysis discloses that PoW performs better than PoA and PoS by approximately 21% and 9%, respectively, in block size efficiency for non-sensitive data. For sensitive data, PoW shows around 23% and 32% better memory usage compared to PoA and PoS, respectively. Security analysis guarantees that the scheme provides robust protection against threats such as impersonation, man-in-the-middle and modification attacks that ensures strong security features. Lax, Nardone, and Russo [18] A new solution is proposed for securely sharing health records, ensuring that access is granted only to authorize entities while preventing the linkage between a patient's identity and their e-health records. This approach leverages a public block chain, which increases trust in the system and automates various operational phases.

Unlike existing solutions that primarily rely on private or consortium block chains where participating entities must be registered and known the proposal is built entirely on a public block chain. This key advantage allows for global accessibility and enabling any party to utilize the solution without restrictive registration requirements.

3. Proposed scheme (Framework, Security Model and Algorithms)

This section Explain about the system model, different algorithms utilized for secure framework, and the security model based on Variable threshed Chinese remainder theorem and pride–Present Cipher is proposed to ensure the fast and safe sharing and storage of medical information about patient. For the secure information transmission of patient one hospital to another hospital or cloud based database to another authorizers utilize mobile agent secure framework. This is a collaborative approach of mobile agent for secure symmetric key transmission for encryption and decryption of patient information as shown in Figure 5.

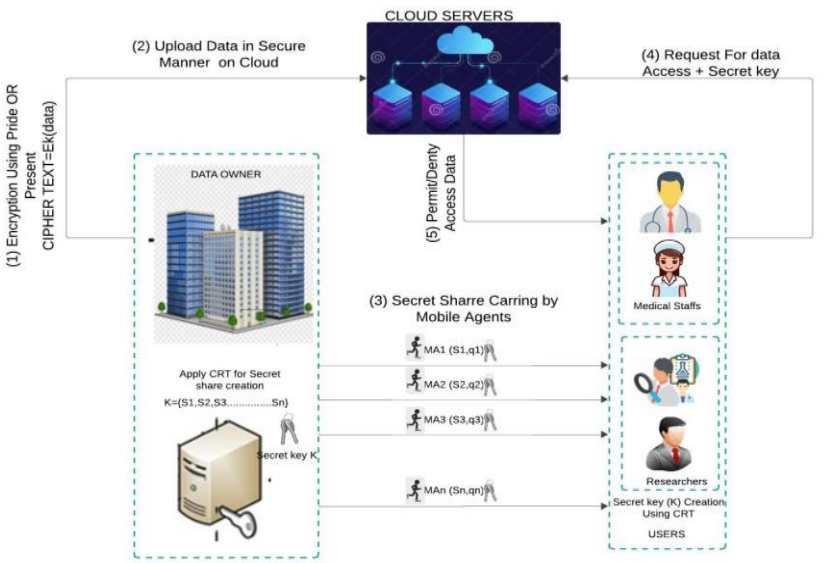

Figure 5
Framework Secure Mobile Agents of patient information

3.1. *Framework*

i. **Data Owner**: Data owner like patient data, patient reports, patient identity etc are encrypt using appropriate pride or Present algorithm in step1. In second step Encrypted data upload on the servers in the cloud. Data access policies are concealed.

ii. **CRT Based secret key sharing**: For the secret key distribution utilize Chinese remainder theorem.

iii. **Cloud Service Provider:** The CSP basically serves as a service supplier instead of the cloud, mirroring its job. The data owners use its data storage service, while users submit requests to retrieve the relevant data. Furthermore, the CSP is assumed to be interested about getting information while remaining genuine.

iv. **Mobile agents:** Mobile agents play very important role for the security of patient data every agent carrying secret share with respective modulo.

v. **User:** Medical staffs, Researcher sends the request to Cloud server for patient data access with secret keys generated by collaboration of mobile agent's shares. Collaboration of mobile agents depends on the threshold value.

3.2 *Algorithms*

Secure medical information transfer in health care system utilize major six algorithms Secret key Creation, Reconstruction of key, Pride Encryption Algorithm, Pride Decryption Algorithm, Present Encryption Algorithm and Present Decryption Algorithm. Proposed framework works in three main phases.

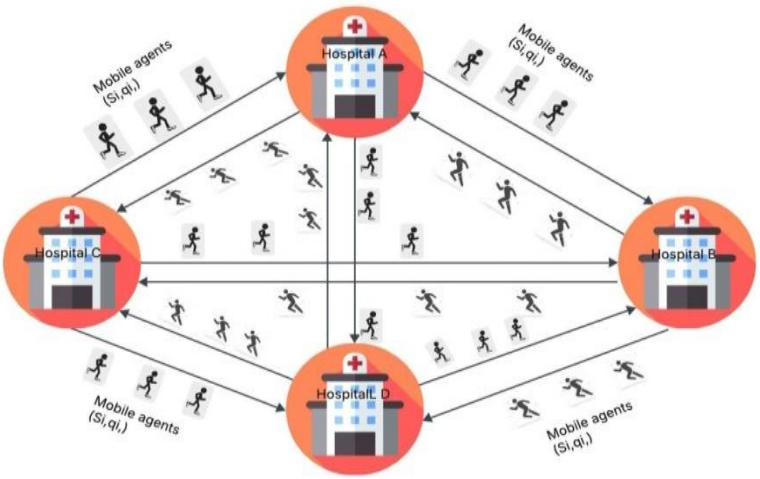

Figure 6
Working of mobile Agents to secure patient information

i. **Secret key Creation and Distribution:** Variable threshold Chinese remainder theorem utilize for secret key sharing among mobile agents. Secret key divided into different numbers of shares shown in equation 1.

$$K = \{S_1, S_2, S_3, S_4, S_5, S_6 \dots \dots \dots \dots \dots \dots S_n\} \quad (1)$$

These shares are dynamically assigned to mobile agents. For each transaction of information retrieval from one clinic to another clinic used dynamically variable threshold. Out of n shares there are t share is required to regenerate the secret key. Every mobile agent carries $\{S_i, q_i, C\}$ for i^{th} secure data transmission.$C = cipher\ Text$ is generated after encryption of data by using Present or Pride cipher. Working as a mobile agent for secure information transmission is shown in Figure 6.

Algorithm 1 Share Creation

Input: Secret key K,$q_1, q_2, q_3, \ldots\ldots\ldots q_n,$

Output:$S_1, S_2, S_3 \ldots\ldots S_n$

i. Choose n prime number $\{q_1, q_2, q_3, \ldots\ldots\ldots q_n,\}$ in such a way $\prod_{i=1}^{n} \quad q_i > S$

ii. $K = \{S_1, S_2, S_3 \ldots\ldots S_n\}$/* *Each share distributes to n Mobile agents*/*

iii. $S_i = K mod q_i, \ \forall i \epsilon \{1,2,3 \ldots . t\}$

Algorithm 2 Reconstruction of key

Input: Secret key $S_1, S_2, S_3 \ldots\ldots S_n$ and threshold t

Output: $Secret\ key\ K$

i. Choose a subset of mobile agent who will participating reconstruction of secret share $\tau \subseteq \{1,2,3,4 \ldots\ldots n\}$

ii. Using share of secret $\{s_i\}_{i\epsilon\,\tau}$ and module $\{q_i\}_{i\epsilon\,\tau}$ with CRT reconstruct secret

$$K = \left(\sum_{i\epsilon\,\tau} \quad s_i * Q_i * {Q_i}^{-1} mod\ q_i\right) mod\ Q$$

$$where\ Q = \prod_{i\epsilon\,\tau} \quad q_i, \qquad Q_i = \frac{Q}{q_i}, {Q_i}^{-1} = {Q_i}^{-1} mod q_i$$

Algorithm 3 Pride Encryption Algorithm

Input: Secret key Plain Text $X_0 = \{X_{63}, X_{62}, X_{61} \ldots\ldots\ldots\ldots\ldots\ldots X_0\}$ and Key K=$K_0 IIK_1$

Output: $Cipher\ Text\ computed$

i. $X_0 = P^{-1}(X_0) \oplus K_0$

ii. $for i = 1\ to\ 19\ do$

iii. $for i = 1\ to\ 15\ do$

iv. $ubstitution\ Layer\ S(x_{3+4j}, x_{2+4j}, x_{1+4j}, x_{0+4j}) = S(y_{3+4j}, y_{2+4j}, y_{1+4j}, y_{0+4j})$

v. $endfor$

vi. $PermutationLayer(Y_{63}, Y_{62} \ldots\ldots\ldots\ldots Y_0) = L(Y_{63}, Y_{62} \ldots\ldots\ldots\ldots Y_0)$Where L is the **bit-wise permutation function**.

vii. Key Mixing (XOR with Round Key)

$$f_i(K_1) = K_{10}\text{II}g_i^{(0)}IIK_{11}IIK_{12}IIg_i^{(1)}\text{II}K_{13}IIK_{14}IIg_i^{(2)}$$
$$\text{II}K_{15}IIK_{16}IIg_i^{(3)}IIK_{17}$$

viii. $(Y_{63}, Y_{62} \dots \dots \dots \dots Y_0) = f_i(K_1) \oplus (Y_{63}, Y_{62} \dots \dots \dots \dots Y_0)$

ix. $X_{i+1} = (Y_{63}, Y_{62} \dots \dots \dots \dots Y_0)$

x. $endfor$

xi. $X_{20} \leftarrow P(X_{20} \oplus K_2)$ /*
$K_2 = additional\ key\ derived\ from\ K_1\ and\ P\ is\ Final\ Permutation.$

Algorithm 4 Pride Decryption Algorithm

Input: Cipher Text X_{20} =(X_{63} , $X_{62}, X_{61} \dots \dots \dots \dots \dots \dots X_0$) and key K=$K_0 IIK_1$

Output: $Plain\ Text\ X_0$

i. Initial Transformation (INVERSE Permutation)
$$X_{20} \leftarrow P^{-1}(X_{20}) \oplus K_2)$$

ii. $for\ i = 19\ to\ 0\ do$

iii. $f_i(K_1) = K_{10}IIg_i^{(0)}IIK_{11}IIK_{12}IIg_i^{(1)}IIK_{13}IIK_{14}IIg_i^{(2)}$
$IIK_{15}IIK_{16}IIg_i^{(3)}IIK_{17}$

iv. $(Y_{63}, Y_{62} \dots \dots \dots \dots Y_0) = X_{i+1} \oplus f_i(K_1)$

v. $(Y_{63}, Y_{62} \dots \dots \dots \dots Y_0) = L^{-1}(Y_{63}, Y_{62} \dots \dots \dots \dots Y_0)$

vi. $fori = 1\ to\ 15\ do$

vii. $S^{-1}(x_{3+4j}, x_{2+4j}, x_{1+4j}, x_{0+4j}) = (y_{3+4j}, y_{2+4j}, y_{1+4j}, y_{0+4j})$

viii. $X_i = (Y_{63}, Y_{62} \dots \dots \dots \dots Y_0)$

ix. $X_0 = P^{-1}(X_0) \oplus K_0$

Algorithm 5 Present Encryption Algorithms

Input: Plain Text $X_0 = \{X_{63}, X_{62}, X_{61} \dots \dots \dots \dots \dots \dots X_0\}$ and Key K=($K_{79}, K_{78}, \dots \dots . . K_0$)
$$80\ bit\ or\ 128\ bit$$

Output: $Cipher\ Text\ computed\ 64\ bit\ X_{31}$

i. $X_0 = P^{-1}(X_0) \oplus K_0$

ii. $fori = 1\ to\ 31\ do$

iii. $forj = 0\ to\ 15\ do$

iv. $S_{4j}, S_{4j+1}, S_{4j+2}, S_{4j+3} \leftarrow S(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3})$

v. Permutation $(Y_{63}, Y_{62} \dots \dots \dots \dots Y_0) = P(X_i)$

vi. **Round key addition** $X_{i+1} = (Y_{63}, Y_{62} \dots \dots \dots \dots Y_0) \oplus K_i$

vii. $X_{31} = P(X_{31}) \oplus K_{31}$

Algorithm 6 Present Decryption Algorithms

Input: $Cipher\ Text\ computed\ 64\ bit\ X_{31}$ and Key K= ($K_{79}, K_{78}, \dots \dots . . K_0$)
$$80\ bit\ or\ 128\ bit$$

Output: Plain Text $X_0 = \{X_{63}, X_{62}, X_{61} \dots \dots \dots \dots \dots \dots X_0\}$

i. $X_{31} = P^{-1}(X_{31}) \oplus K_{31}$
ii. $fori = 30\ to\ 0\ do$
iii. Inverse permutation $(Y_{63}, Y_{62} \ldots \ldots \ldots \ldots Y_0) = P(X_{i+1} \oplus K_i)$
iv. Inverse S box layer
v. $forj = 0\ to\ 15\ do$
vi. $S_{4j}, S_{4j+1}, S_{4j+2}, S_{4j+3} \leftarrow S^{-1}(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3})$
vii. $X_i = (Y_{63}, Y_{62} \ldots \ldots \ldots \ldots Y_0)$
viii. $X_0 \leftarrow P(X_0) \oplus K_0$

Medical data security is crucial in healthcare systems where mobile agents provide data retrieval, storage, and communication between medical devices cloud servers, and medical experts like doctors, nurse, researches etc. This paper proposes a Secure and fast Mobile Agent Framework based on Variable Threshold Chinese Remainder Theorem (VTCRT) for secure key sharing and Lightweight Cryptography for data encryption and integrity protection. The framework is optimized for computational efficiency, low communication overhead, and scalability in resource-constrained environments. The framework consists of three main components**:** First, Initialization of Key Generation & Distribution: VT-CRT ensures secure key sharing among authorized entities. Second, Data Encryption & Decryption using Lightweight ciphers encrypt medical records before transmission. Third, Mobile Agent Deployment of Secure migration between hospital servers and IoT-based medical devices. (Mobile agents migrate across healthcare nodes (hospitals, cloud servers, IoT medical devices)).

4. Implementation and Result Analysis

The implementation of proposed framework for Secure and Efficient Mobile Agent Framework for Medical Data Protection Using Variable Threshold CRT and Lightweight encryption and decryption is carried out in Python, integrating cryptographic method for secure mobile agent communication. The framework employs Variable Threshold Chinese Remainder Theorem (VTCRT) for dynamic key distribution and lightweight cryptographic algorithms (PRESENT, PRIDE and PRINCE) for efficient encryption and decryption. The mobile agent migration is simulated using a Python based agent system for ensuring secure data transmission between cloud servers and advance technology based medical devices. Performance metrics such as encryption time, decryption time, memory usage, scalability, and communication overhead are evaluated using matplotlib for visualization. Proposed framework aims on minimizing Time complexity while maintaining optimal security and efficiency for resource constrained environments. The Secure and Efficient Mobile Agent Framework for Medical Data security was evaluated based on encryption time, decryption time, memory usage, scalability and communication overhead shown in Figure 7. The lightweight cryptographic algorithms (PRESENT OR PRIDE) demonstrated superior efficiency compared

to AES, DES and Blowfish. The encryption time for PRIDE was 1.8 ms, outperforming PRESENT (2.3 ms) and AES (6.2 ms). Similarly, decryption time for PRIDE was 2.0 ms, significantly faster than AES (6.5 ms). Memory Utilization is minimum for PRIDE (10 KB), PRESENT (12 KB) as compared to AES (35 KB) demonstrating their suitability for resource constrained mobile agent's environment. Additionally, scalability and communication overhead were optimized with VTCRT ensuring adaptive Secret key Sharing, reducing the overhead by 30% compared to traditional Algorithms. The framework based on VTCRT and pride present cipher maintains High level security guarantees while increasing performance making it ideal for secure medical data transmission in advance technology-based healthcare systems. Lightweight encryption techniques such as PRIDE, PRESENT, and PRINCE ciphers are utilized for encrypting medical records to ensure low computational complexity while maintaining strong security guarantees.

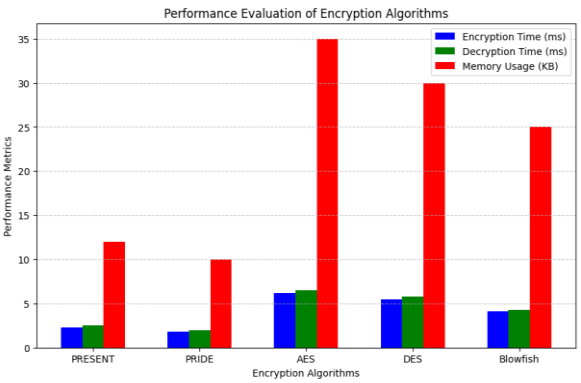

Figure 7
Performance Evaluation of Algorithms

Security analysis of proposed framework against eavesdropping attacks is prevented as VT CRT ensures secure key reconstruction, making key exposure infeasible. Cloning attacks are mitigated through fast encryption, reducing the attack time window. Brute force attacks are countered by PRESENT cipher's 31 rounds and strong S-box transformations, making exhaustive key search impractical. Lastly, Man in the Middle (MITM) attacks are obstructed by secure agent to agent communication using encrypted key exchange that ensures data integrity and confidentiality. These methods collectively improve the security, reliability, and efficiency of mobile agents in healthcare data protection. Figure 8 shows the execution time in milliseconds of four cryptographic ciphers AES, Blowfish, PRESENT and PRIDE over different file sizes in KBs. The x axis represents the file size ranging from 100 KB to 1000 KB and the y-axis shows the execution time in milliseconds. The comparison shows understanding into the efficiency and computational overhead of each cipher. Each encryption algorithm performance is represented using different colors. AES show in Blue

Line, execution time for AES starts at 190 ms for smaller file sizes and increases to 207 ms for 1000 KB. The blue line shows that AES has the very high computational overhead among the four algorithms making it less suitable for real-time applications requiring low delay. Blowfish show in Gray Line shows moderate performance starting at 182 ms and rising gradually to 189 ms. The gray line remains above PRESENT and PRIDE but below AES, reflecting its balanced encryption speed and security trade off. PRESENT Cipher show in red color represents the PRESENT cipher which starts at 176 ms and increases steadily to 185 ms. Present Cipher execution time is less than Blowfish and AES making it a better option for mobile agent security where efficiency is major issue. PRIDE Cipher show in green color line representing PRIDE lowest execution time among all algorithms ranging from 170 ms to 178 ms. Indicates that PRIDE is the most efficient encryption method in terms of speed making it ideal for real time data protection in mobile agents and IoT devices. In graph highlights the best efficiency of PRIDE and PRESENT cipher in handling encryption tasks for mobile agents. These ciphers are well suited for advance technology-based healthcare systems where quick, lightweight encryption is essential. The Secure Mobile Agent Framework for Medical Data Protection benefits from these ciphers due to less execution time, Minimum memory usage and fast performance in resource constrained environments.

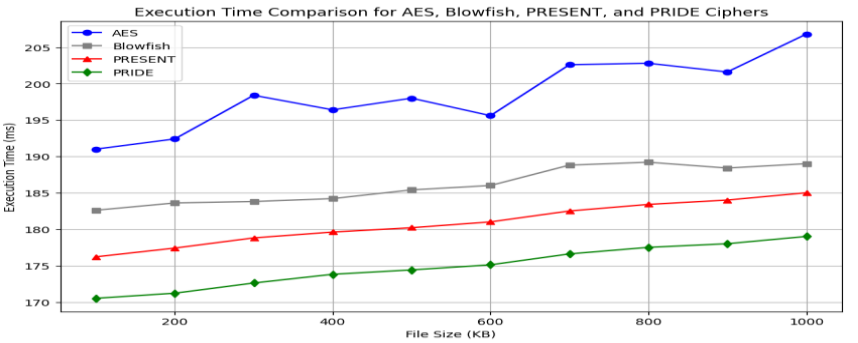

Figure 8

Execution Time Comparison for AES, blowfish, Present, and pride Cipher

The outcome shows that PRESENT and PRIDE lightweight cryptography gives the best trade-off between security, execution speed and resource efficiency. Requirements of mobile agents in medical environments, where low latency and efficient encryption are crucial, PRIDE and PRESENT Cipher emerge as the most optimal choices.

5. Conclusion and future scope

The most obvious platform for data sharing in the healthcare industry today is the cloud and proposed framework can be applied to an outsourced EHR information in encoded form to offer access control. This article explains

how to share data on cloud storage systems and proposed the VT-CRT based present pride Technique a multi-authority access control solution that is totally safe and protects privacy for cloud-based healthcare data distribution. Data owners can now freely distribute their data to all users. As a result, the system is flexible and scalable. Both users and data owners are protected by the partially disguised access policy. Our implementation outcomes show that even while the method preserves privacy and offers adaptive security under the conventional protocol, the framework improves decoding cost. In the future, decoding can be outsourced to proxy servers to increase its efficiency. Proposed framework presents a lightweight yet secure mobile agent framework for medical data protection using VT-CRT and PRESENT encryption. The approach ensures low latency, minimal resource utilization, and strong security guarantees in healthcare IoT environments. The proposed Secure and Efficient Mobile Agent Framework for Medical Data Protection integrates Variable Threshold CRT for adaptive key sharing and lightweight cryptographic algorithms (PRESENT OR PRIDE) for efficient encryption, ensuring data security in resource-constrained environments. Performance analysis demonstrates that PRIDE (1.8 ms encryption, 2.0 ms decryption and 10 KB memory) and PRESENT (2.3 ms encryption, 2.5 ms decryption and 12 KB memory) significantly outperform AES (6.2 ms encryption, 6.5 ms decryption and 35 KB memory) and Blowfish (4.1 ms encryption, 4.3 ms decryption and 25 KB memory) in execution time and memory efficiency. Comparative evaluations of file size versus Encryption time reveal that AES and Blowfish show higher execution times with increasing file size, while PRIDE and PRESENT maintain low computational overhead which proves their suitability for secure mobile agent migrations. The security analysis confirms strong confidentiality integrity, and authentication via HMAC based integrity validation and dynamic key reconstruction. Future work will explore quantum-resistant cryptographic techniques, homomorphic encryption for secure computations, and AI-driven adaptive security policies to enhance mobile agent security and privacy in real-time medical data processing. Future work also includes quantum-safe cryptographic integration and machine learning-based anomaly detection for enhanced agent security.

References

[1] L. Fang, C. Yin, J. Zhu, C. Ge, M. Tanveer, A. Jolfaei, and Z. Cao, "Privacy protection for medical data sharing in smart healthcare," *ACM Trans. Multimedia Comput. Commun. Appl.,* vol. 16, no. 3s, pp. 1–18 (Oct. 2020), doi: 10.1145/3408322.

[2] C. L. Chen, P. T. Huang, Y. Y. Deng, H. C. Chen, and Y. C. Wang, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Human-centric*

Comput. Inf. Sci., vol. 10, no. 1, pp. 1–31 (2020), doi: 10.1186/s13673-020-00221-1.

[3] H. Jin, Y. Luo, P. Li, and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," *IEEE Access,* vol. 7, pp. 61656–61669 (2019), doi: 10.1109/ACCESS.2019.2916503.

[4] D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare system," *J. Ambient Intell. Humaniz. Comput.,* vol. 14, no. 5, pp. 4853–4864 (2023), doi: 10.1007/s12652-022-04370-2.

[5] P. Kumar and D. Aggarwal, "Software Mobile Agent Migration : A Review," *Journal of Emerging Technologies and Innovative Research (JETIR),* vol. 6, no. 4, pp. 25–32 (2019).

[6] P. Kumar and A. K. Vatsa, "Novel Security Architecture and Mechanism for Identity based Information Retrieval System in MANET," vol. 1, no. 3, pp. 397–404 (2011).

[7] P. Kumar, N. Singhal, and S. Singh, "Anonymous scheme for secure mobile agent migration using Mignotte's sequence and back propagation artificial neural networks," *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.*, vol. 13, pp. 192–199 (2021).

[8] U. Upadhyay, P. Kumar, and D. Aggarwal, "Secure migration of mobile agent using AES & secret sharing approach," *Int. J. Emerg. Technol.,* vol. 10, no. 2, pp. 150–155 (2019).

[9] M. Gupta, M. Gupta, and M. Deshmukh, "Single secret image sharing scheme using neural cryptography," *Multimed. Tools Appl.,* vol. 79, no. 17–18, pp. 12183–12204 (2020), doi: 10.1007/s11042-019-08454-8.

[10] M. Alfalayleh and L. Brankovic, "An overview of security issues and techniques in mobile agents," *IFIP Adv. Inf. Commun. Technol.,* vol. 175, pp. 59–78 (2005), doi: 10.1007/0-387-24486-7_5.

[11] P. Bagga and R. Hans, "Mobile Agents System Security," *ACM Comput. Surv.,* vol. 50, no. 5, pp. 1–45 (2017), doi: 10.1145/3095797.

[12] L. Zhu, Y. Xie, Y. Zhou, Q. Fan, C. Zhang, and X. Liu, "Enabling efficient and secure health data sharing for Healthcare IoT systems," *Future Gener. Comput. Syst.,* vol. 149, pp. 304–316 (2023), doi: 10.1016/j.future.2023.07.031.

[13] K. Pradeep Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, and V. Jha Pillai, "Secure approach to sharing digitized medi-

cal data in a cloud environment," *Data Sci. Manag.*, vol. 7, no. 2, pp. 108–118 (2024), doi: 10.1016/j.dsm.2023.12.001.

[14] R. Gupta, P. Kanungo, N. Dagdee, G. Madhu, K. S. Sahoo, N. Z. Jhanjhi, M. Masud, N. S. Almalki, and M. A. AlZain, "Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing," *Sensors*, vol. 23, no. 5 (2023), doi: 10.3390/s23052617.

[15] J. Oh, S. Son, D. K. Kwon, M. Kim, Y. Park, and Y. Park, "Design of Secure and Privacy-Preserving Data Sharing Scheme Based on Key Aggregation and Private Set Intersection in Medical Information System," *Mathematics*, vol. 12, no. 11 (2024), doi: 10.3390/math12111717.

[16] J. Scheibner, J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Ienca, J. Fellay, E. Vayena, and J.-P. Hubaux, "Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis," *J. Med. Internet Res.*, vol. 23, no. 2, pp. 1–18 (Feb. 2021), doi: 10.2196/25120.

[17] H. Bodur and I. F. T. Al Yaseen, "An Improved blockchain-based secure medical record sharing scheme," *Cluster Comput.*, vol. 27, no. 6, pp. 7981–8000 (2024), doi: 10.1007/s10586-024-04414-6.

[18] G. Lax, R. Nardone, and A. Russo, "Enabling secure health information sharing among healthcare organizations by public blockchain," *Multimed. Tools Appl.*, vol. 83, no. 24, pp. 64795–64811 (2024), doi: 10.1007/s11042-024-18181-4.

Received November, 2025