

A Secure and Efficient Mobile Agent Framework for Medical Data Protection Using Variable Threshold CRT and Lightweight Cryptography

Anuradha Singh

JSS Academy of Technical Education, Noida /Department of Computer Science and Engineering, Uttar Pradesh, 201301, India

E-mail: anuradha.singh@jssaten.ac.in

ORCID iD: <https://orcid.org/0009-0008-4765-1341>

Pradeep Kumar

JSS Academy of Technical Education, Noida /Department of Computer Science and Engineering, Uttar Pradesh, 201301, India

E-mail: pradeep8984@jssaten.ac.in

ORCID iD: <https://orcid.org/0000-0001-6177-8527>

*Corresponding author

Received: February 17, 2026; Revised: May 3, 2026; Accepted: August 20, 2026; Published: October 8, 2026

Abstract: Mobile agents are powerful advanced technology for distributing computing with intelligent and autonomous execution of assigned tasks. During the execution, a mobile agent utilizes a specific life cycle in a malicious environment. Collaboration of mobile agents for securing medical data like patient information, patient medical report etc. plays an important role. In the digital world, smart health care system is required. For secure accessing of patient information from one hospital to another hospital a framework is proposed based on the variable threshold Chinese remainder theorem with the present and pride lightweight cipher. The Chinese remainder theorem is used for secret sharing of key among hospitals. The VT-CRT approach 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 evaluated by the ability to securely and effectively transmit medical information. The lightweight PRIDE and PRESENT encryption methods provide efficient, low-latency encryption that is ideal for resource-constrained 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. Experimental results show that the proposed framework improves security while maintaining optimal speed, making it a reliable solution for safe patient information sharing in medical applications.

Index Terms: 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 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 health care 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 its patient data as an Electronic Health record on the 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. A total of 1.5 million pieces of medical equipment has 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 by the Protenus Breach Barometer. There are various users such as Doctors, medical students and medical insurance agents who want to access 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.

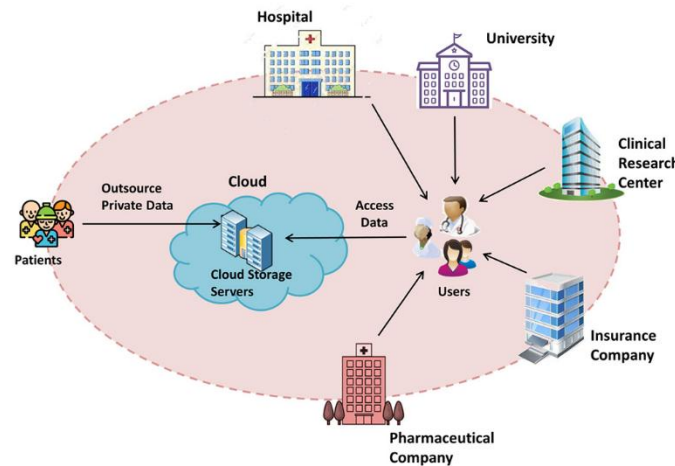


Fig. 1. Healthcare data sharing

Despite its obvious advantages, health information sharing among institutions has several obstacles that must be overcome in order 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 inadequate documents can all influence the accuracy of transmitted health information, potentially resulting in inaccurate diagnoses or improper treatments. To guarantee the accuracy of transmitted information about patients, institutions should use stringent data verification and validation methods.

Mobile agent technology has developed fast which is transforming data transfer and confidentiality in many sectors, mostly in healthcare[5]. Mobile agents are small program code entities that may migrate between network nodes to perform functions such as safe information retrieval, the process and communication shown in figure-2.

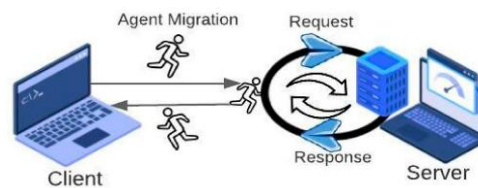


Fig. 2. Mobile agent for sharing of information

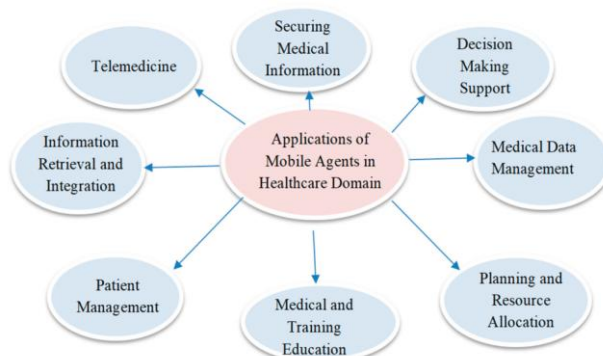


Fig. 3. Application of Mobile agent in health care Domain

Mobile agents provide secure information exchange for the medical field, easy communication among hospitals, cloud-based record and IOT enabled medical equipment. However, these benefits are linked with serious security

challenges, especially regarding maintaining confidentiality, integrity and efficiency in key distribution and data encryption. The increasing prevalence of cyber threats, eavesdropping assaults and illegal access makes it a necessity to develop robust cryptographic techniques for secure mobile agent transmission[6].

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

One difficult aspect of protecting mobile agents is efficiently distributing cryptographic keys and minimizing computing overhead. Traditional key-sharing mechanisms, such as Shamir's Secret Sharing and Threshold Cryptography frequently give 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 per the requirement of each transaction. Along with secure key sharing, encryption is important for securing medical data from illegal access and modification. Conventional encryption algorithms such as AES, DES, and Blowfish give high security assurances but frequently have large computational costs rendering them unsuitable for resource constrained medical equipment and real-time healthcare applications. To address this constraint, we 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].

Electronic Health Data

In order to ensure the security and privacy 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].

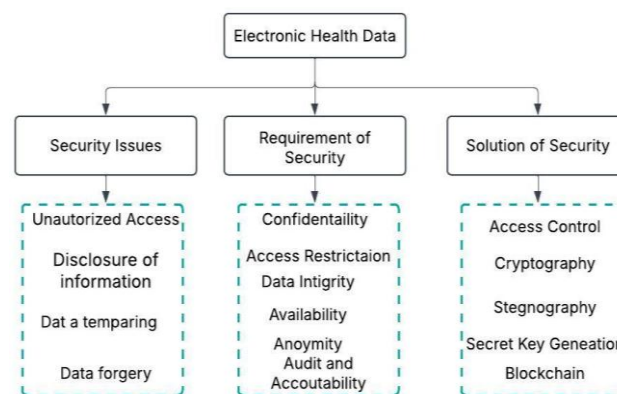


Fig. 4. A Hierarchy of the security and privacy for electronic health record

The goal 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 structure of paper is as follows: Section 2 discusses 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 future scope.

2. Related Works

This section 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.

Liehuang Zhu et al.[12] identified critical challenges in healthcare IoT (HIoT) systems and proposed a secure and efficient medical data-sharing scheme called ESDS to ensure privacy preservation, authenticity verification and high efficiency. To accomplish, they developed an aggregate signcryption mechanism with local verifiability. Security analysis confirms that ESDS upholds availability, confidentiality and unforgeability that meet the security requirements for medical data sharing in HIOT environments. Additionally, they perform both theoretical and experimental evaluations of its efficiency. The findings show that ESDS is practical and feasible offering minimized computational and communication overhead while enabling efficient verification due to its locality property.

Kukatlapalli Pradeep Kumar *et al.* [13] Proposed system increases the security of sensitive medical files stored in the cloud by implementing end-to-end encryption using AES client-side encryption algorithm. File access is permitted based on predefined rules ensuring that only an authorized candidate can retrieve specific files. For example, staff in emergency departments can only retrieve designated data and are restricted from viewing or downloading to unauthorized person. When a user downloads a file, they must request a key to open it. If the user is authenticated, the file owner securely shares the key through the ECDH key exchange technique. Only users who enter the right 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. Also, the key remains undiscoverable during transmission, further strengthening the security.

LIMING FANG *et al.*[1] Proposed a new data sharing framework with a data access control method. In this system medical officers submit applications and patient information is processed within the hospital. The data is stored on semi trusted servers, enabling selective sharing of electronic medical data among different medical centres and clinical officers. The Method addresses security concerns when granting access to patient's medical data. To ensure accountability, both patients and medical officers are required to add digital watermarks linked to their identities when uploading data that allows traceability in case of data modification or leakage. Comprehensive analytical and experimental outcomes demonstrate the security and efficiency of the proposed technique. Reetu Gupta *et al.*[14] Proposed the SP MAACS technique which is a totally secure and privacy preserving multi authority access control system for sharing healthcare data in the cloud. It enables data owners to share their information with users across both open and restricted domains that enhance the system's scalability and flexibility. The use of a partially hidden access policy protects the security of both users and data owners. Implementation outcomes indicate that the technique not only preserves security and ensures adaptive security under the standard model but also optimizes decryption costs which improve overall efficiency.

Jihyeon Oh *et al.*[15] Proposed a secure and privacy preserving data sharing technique that balances information confidentiality and privacy. By using key aggregate encryption and private set intersection techniques, the scheme enables secure data sharing while preventing the exposure of sensitive information. To assess its robustness against potential attacks, informal and formal security analyses are performed including Burrow Abadi Needham logic and Scyther. Also, the execution time of cryptographic operations is evaluated using a Multi Precision integer and rational arithmetic cryptographic library, comparing this approach with existing schemes in terms of security, computational cost and time complexity. The results confirm that the proposed scheme offers strong security and efficiency, contributing to the field by ensuring privacy protection and secure, flexible medical data sharing. James Scheibner *et al.*[16] Combined two advanced privacy enhancing technologies first, homomorphic encryption and second, secure multiparty computation into a unified framework called multiparty homomorphic encryption. This approach performs better over using either technique individually. They also discussed that multiparty homomorphic encryption meets the legal requirements for medical data sharing under the European Union's General Data Protection Regulation (GDPR), which serves as a global standard for data protection. Specifically, data processed and shared through this method can be classified as anonymized which can reduce 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.

Huseyin Bodur *et al.*[17] In the proposed scheme, medical data is categorized into sensitive and non-sensitive patient information. Three consensus mechanisms Proof of Work (PoW), Proof of Stake (PoS) and Proof of Authority (PoA) are implemented and assessed based on their performance. The analysis shows that PoW outperforms PoA and PoS by approximately 21 percent and 9 percent respectively, in block size efficiency for non-sensitive data. Similarly for sensitive data, PoW demonstrates around 23 percent and 32 percent better memory usage compared to PoA and PoS, respectively. Security analysis confirms that the method offers robust security against attacks such as man in the middle, impersonation and modification attacks that guarantee strong security features. Gianluca Lax *et al.*[18] Proposed a new solution for securely sharing health records and ensuring that access is granted only to authorized entities while preventing the linkage between a patient's identity and their Electronic 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, our proposal is built entirely on a public block chain. This key advantage allows for global accessibility, enabling any party to utilize the solution without restrictive registration requirements.

3. Proposed Framework

This section explains about the system model, various algorithms utilized for secure framework, and the security model based on Variable threshold Chinese remainder theorem and pride–Present Cipher is proposed to ensure the fast and secure storage and sharing of medical information about patient. For the secure information transmission of patient data from one hospital to another hospital or from a cloud-based database to other authorizers, a mobile agent secure framework is utilized. This is a collaborative approach of mobile agent for secure symmetric key transmission for encryption and encryption of patient information.

3.1. Framework

- Data Owner: Data owner like patient data, patient reports, patient identity etc. are encrypted using appropriate pride or Present algorithm in step1. In the second step, the encrypted data is uploaded on the cloud Servers. Access policy of data is hidden.
- CRT Based secret key sharing: For the secret key distribution, the Chinese remainder theorem is utilized.
- Cloud Service Provider: The CSP basically serves as a service provider in place of the cloud, mirroring its job. The data owners employ its data storage service, and users submit requests to retrieve the relevant data. Furthermore, the CSP is assumed to be interested about getting information while remaining genuine.
- Mobile agents: Mobile agents play a very important role for the security of patient data, and every agent carries

secret share with respective modulo.

- User: Medical staff and researchers send 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.

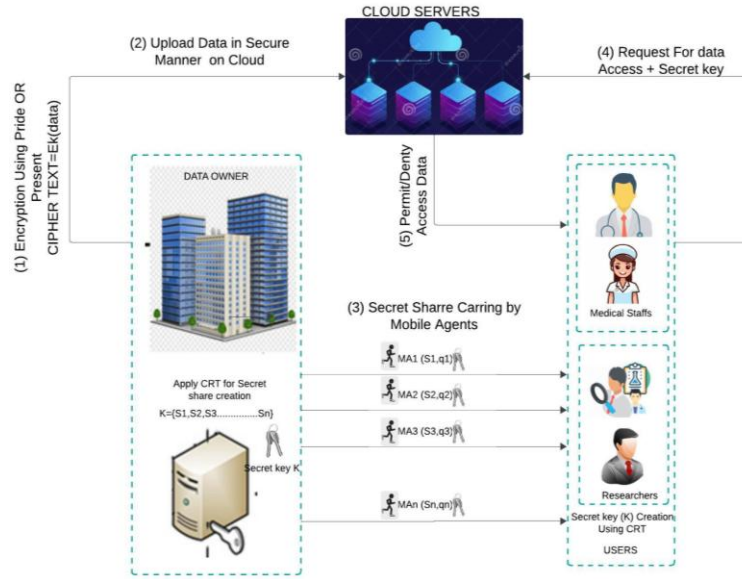


Fig. 5. Framework secure mobile agents of patient information

3.2. Algorithms

Secure medical information transfer in health care system utilizes six major 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.

- **Secret key Creation and Distribution:** The variable threshold Chinese remainder theorem is utilized for secret key sharing among mobile agents. The secret key is divided into different numbers of shares shown in equation 1.

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

These shares are dynamically assigned to mobile agents. For each transaction of information retrieval from one clinic to another, a dynamically variable threshold is used. 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.

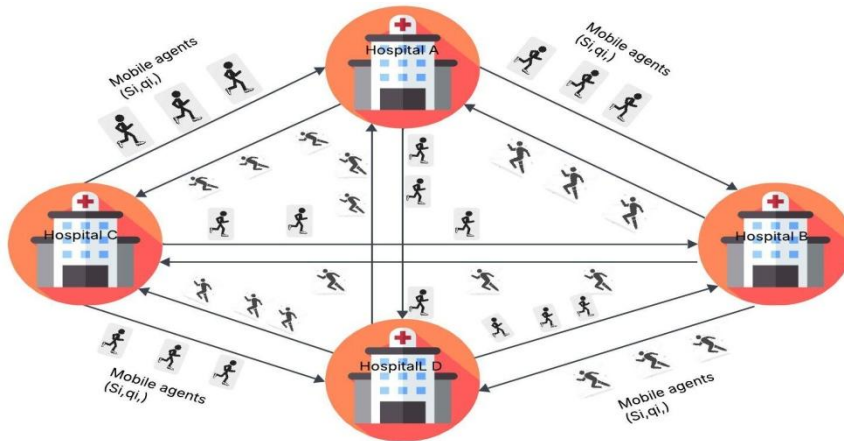


Fig. 6. Working of mobile agents to secure patient information

Algorithm1 Share Creation

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

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

- Choose n prime number $\{q_1, q_2, q_3, \dots, q_n\}$ in such a way $\prod_{i=1}^n q_i > S$
- $K = \{S_1, S_2, S_3, \dots, S_n\} / \text{Each share distributes to } n \text{ Mobile agents} /$
- $S_i = K \bmod q_i, \forall i \in \{1, 2, 3, \dots, n\}$

Algorithm 2 Reconstruction of key

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

Output: Secret key K

- Choose a subset of mobile agent who will participating reconstruction of secret share $\tau \subseteq \{1, 2, 3, 4, \dots, n\}$
- Using share of secret $\{s_i\}_{i \in \tau}$ and module $\{q_i\}_{i \in \tau}$ with CRT reconstruct secret

$$K = \left(\sum_{i \in \tau} s_i * Q_i * Q_i^{-1} \bmod q_i \right) \bmod Q$$

$$\text{where } Q = \prod_{i \in \tau} q_i, \quad Q_i = \frac{Q}{q_i}, \quad Q_i^{-1} = Q_i^{-1} \bmod q_i$$

Algorithm 3 Pride Encryption Algorithm

Input: Secret key Plain Text $X_0 = \{X_{63}, X_{62}, X_{61}, \dots, X_0\}$ and Key $K = K_0 \parallel K_1$

Output: Cipher Text computed

- $X_0 = P^{-1}(X_0) \oplus K_0$
- for $i = 1$ to 19 do
- for $i = 1$ to 15 do
- SubstitutionLayer $S(x_{3+4j}, x_{2+4j}, x_{1+4j}, x_{0+4j}) = (y_{3+4j}, y_{2+4j}, y_{1+4j}, y_{0+4j})$
- endfor
- PermutationLayer $(Y_{63}, Y_{62}, \dots, Y_0) = L(Y_{63}, Y_{62}, \dots, Y_0)$ Where L is the **bit-wise permutation function**.
- Key Mixing (XOR with Round Key)

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

- $(Y_{63}, Y_{62}, \dots, Y_0) = f_i(K_1) \oplus (Y_{63}, Y_{62}, \dots, Y_0)$
- $X_{i+1} = (Y_{63}, Y_{62}, \dots, Y_0)$
- endfor
- $X_{20} \leftarrow P(X_{20} \oplus K_2) / K_2 = \text{additional key derived from } K_1 \text{ and } P \text{ is Final Permutation.}$

Algorithm 4 Pride Decryption Algorithm

Input: Cipher Text $X_{20} = (X_{63}, X_{62}, X_{61}, \dots, X_0)$ and key $K = K_0 \parallel K_1$

Output: Plain Text X_0

- Initial Transformation (INVERSE Permutation)

$$X_{20} \leftarrow P^{-1}(X_{20} \oplus K_2)$$

- for $i = 19$ to 0 do
- $f_i(K_1) = K_{10} \parallel g_i^{(0)} \parallel K_{11} \parallel K_{12} \parallel g_i^{(1)} \parallel K_{13} \parallel K_{14} \parallel g_i^{(2)} \parallel K_{15} \parallel K_{16} \parallel g_i^{(3)} \parallel K_{17}$
- $(Y_{63}, Y_{62}, \dots, Y_0) = X_{i+1} \oplus f_i(K_1)$
- $(Y_{63}, Y_{62}, \dots, Y_0) = L^{-1}(Y_{63}, Y_{62}, \dots, Y_0)$
- for $i = 1$ to 15 do
- $S^{-1}(x_{3+4j}, x_{2+4j}, x_{1+4j}, x_{0+4j}) = (y_{3+4j}, y_{2+4j}, y_{1+4j}, y_{0+4j})$
- $X_i = (Y_{63}, Y_{62}, \dots, Y_0)$
- $X_0 = P^{-1}(X_0) \oplus K_0$

Algorithm 5 Present Encryption Algorithms

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

80 bit or 128 bit

Output: Cipher Text computed 64 bit X_{31}

- $X_0 = P^{-1}(X_0) \oplus K_0$
- *for* $i = 1$ to 31 *do*
- *for* $j = 0$ to 15 *do*
- $S_{4j}, S_{4j+1}, S_{4j+2}, S_{4j+3} \leftarrow S(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3})$
- $\text{Permutation}(Y_{63}, Y_{62} \dots \dots Y_0) = P(X_i)$
- **Round key addition** $X_{i+1} = (Y_{63}, Y_{62} \dots \dots Y_0) \oplus K_i$
- $X_{31} = P(X_{31}) \oplus K_{31}$

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 $X_0 = \{X_{63}, X_{62}, X_{61} \dots \dots \dots X_0\}$

- $X_{31} = P^{-1}(X_{31}) \oplus K_{31}$
- *for* $i = 30$ to 0 *do*
- $\text{Inverse permutation}(Y_{63}, Y_{62} \dots \dots Y_0) = P(X_{i+1} \oplus K_i)$
- *Inverse S box layer*
- *for* $j = 0$ to 15 *do*
- $S_{4j}, S_{4j+1}, S_{4j+2}, S_{4j+3} \leftarrow S^{-1}(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3})$
- $X_i = (Y_{63}, Y_{62} \dots \dots Y_0)$
- $X_0 \leftarrow P(X_0) \oplus K_0$

Medical data security is crucial in healthcare systems where mobile agents provide data retrieval, storage, and communication between medical devices, cloud servers, and healthcare professionals like doctors, nurses, researchers 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.

Variable Threshold for session key K is defined as

$$t_k = t_{min} + (k \bmod (t_{max} - t_{min} + 1)) \quad (2)$$

Subject to $t_{min} \leq t_k \leq t_{max} \leq n$

Using equation 2, threshold value of key generation for each transaction of mobile agents rotates automatically.

The proposed framework integrates dynamic threshold value adaptation. Proposed framework formally proves correct key reconstruction under CRT, adopts a healthcare-oriented attack model, and presents normalized cryptographic comparisons to ensure fair and rigorous performance Analysis. The framework consists of three main components:

- Initialization: Key Generation & Distribution: VT-CRT ensures secure key sharing among authorized entities.
- Data Encryption & Decryption: Lightweight ciphers encrypt medical records before transmission. (PRIDE& PRESENT Ciphers)
- Mobile Agent Deployment: Secure migration of mobile agents between hospital servers and IoT-based medical devices. (Mobile agents migrate across healthcare nodes (hospitals, cloud servers, IoT medical devices))

3.3. Threat and Adversary Model

- System Model

Let

$$MA = \{MA_1, MA_2, \dots, MA_n\} \quad (3)$$

be a set of n mobile agents participating in secure medical data access. A secret session key $K_s \in \mathbb{Z}$ is shared using a Variable Threshold Chinese Remainder Theorem (VT-CRT) scheme with threshold t_s where:

$$2 \leq t_k \leq n$$

Each mobile agent MA_i holds a CRT share: $k_i = K_s \bmod m_i$
where m_i are pairwise coprime moduli:

$$\gcd(m_i, m_j) = 1, \forall i \neq j \quad (4)$$

- Adversary Model Network Adversary: A has full control over the communication Medium. Formally,

$$A = (\epsilon, I, M, R)$$

Where ϵ denotes eavesdropping, I interception, M message modification, and R replay capabilities.

- Mobile Agent Compromise: The adversary may compromise a subset:

$$C \subset \text{Mobile Agent } |C| \leq t_k - 1 \text{ and obtain } \{(k_i, m_i)\} \quad MA \in C$$

The adversary cannot compromise t_k or more agents in the same session.

Theorem 1: Correctness of VT-CRT Secret Key Reconstruction If at least t_s valid secret shares are available, then the secret key k_s can be uniquely and correctly reconstructed. If fewer than t_s shares are available reconstruction is computationally impossible.

Proof: let $S = \{(k_{i1}, m_{i1}), \dots, (k_{is}, m_{is})\}$ be any subset of t_s valid secret shares of mobile agents.

$$M = \prod_{j=1}^{t_s} m_{ij}, \quad M_{ij} = \frac{M}{m_{ij}} \quad (5)$$

Since the moduli are pair wise co prime there exist a unique modular inverse.

$$M_{ij}^{-1} \equiv M_{ij}^{-1} \bmod m_{ij} \quad (6)$$

Recreation of secret key of mobile agents

$$\widehat{K_s} = \sum_{j=1}^{t_s} k_{ij} * M_{ij} M_{ij}^{-1} \bmod M \quad (7)$$

Using Chinese remainder theorem satisfy

$$\widehat{K_s} \equiv K_s \bmod m_{ij} \text{ for all } j \quad (8)$$

Additionally

$$\prod_{j=1}^{t_s} m_{ij} > K_s$$

Solution is unique if

$$\widehat{K_s} = K_s$$

Secret key for mobile agents generated correctly.

Theorem 2: Threshold Resilience (Sub-Threshold Security) an adversary possessing fewer than t_s shares cannot reconstruct k_s with non-negligible probability.

Proof: Let the adversary $C = \{(k_{i1}, m_{i1}), \dots, (k_{ir}, m_{ir})\}$ $r < t_s$
System congruencies

$$K_s \equiv K_{ij} \pmod{m_{ij}} \text{ for all } j = 1, 2, \dots, r$$

The solution space contains infinitely many candidates

$$K_s = x + l * \prod_{j=1}^r m_{ij}, \quad l \in \mathbb{Z} \quad (9)$$

$$\text{Since } \prod_{j=1}^r m_{ij} < \prod_{j=1}^{t_s} m_{ij}$$

Adversary cannot determine the unique key K_s .

Theorem 3: Correctness under Dynamic Threshold Adaptation :Dynamic variation of the threshold does not affect correctness, provided CRT constraints are preserved.

Proof: Threshold for every transaction is defined

$$t_s = t_{min} + (s \bmod (t_{max} - t_{min} + 1)) \quad (10)$$

Subject to $2 \leq t_{min} \leq t_s \leq t_{max} \leq n$
For every transaction

$$\prod_{i=1}^{t_s} m_i > K_s \text{ and } \gcd(m_i, m_j) = 1 \quad (11)$$

Since CRT correctness depends only on the number of valid congruences and co-primality, not on how t_s is chosen, reconstruction correctness holds independently for each session.

The correctness and security of the proposed VT-CRT key-sharing scheme are formally proven using the Chinese Remainder Theorem, demonstrating unique reconstruction with at least t shares, information-theoretic resistance under sub-threshold compromise, and correctness preservation under dynamic threshold adaptation.

3.4. Formal Security Analysis Against Attacks

Let A be a probabilistic polynomial-time (PPT) adversary operating under the Dolev Yao network model, capable of intercepting, modifying, replaying, and injecting messages.

- Resistance to Man-in-the-Middle (MITM) Attack

Analysis: Each Mobile agent sends an encrypted secret share

$$C_i = \text{Enc}_{K_s}(k_i \parallel \text{nonce}_i) \quad (12)$$

Where $k_i = k_s \bmod m_i$ and nonces prevents reply.

Any modification by A results in decryption failure or inconsistency during CRT reconstruction.

$$\widehat{K_s} \equiv K_i \bmod m_i \quad (13)$$

Valid reconstruction secret key for mobile agent requires at least consistent shares, MITM manipulation is detected. t_s

- Resistance to Brute-Force Attack

Attack Model: An attempt by an attacker to guess the session key.

Analysis: The key space is $|K_s| = 2^k$ where $k \in \{80, 128\}$ depending on cipher selection

Brute-force success probability is:

$$\Pr[\text{Guess } k_s] = 2^{-k} \quad (14)$$

Moreover, sub-threshold knowledge yields:

$$K_s = x + l * \prod_{j=1}^r m_i, \quad r < t_s \quad (15)$$

Outcome is in exponential ambiguity.

- Resistance to Mobile Agent Cloning Attack: An adversary clones a mobile agent and attempts to impersonate it.

Analysis: Each mobile agent is bound to:

$$ID_i \parallel k_i \parallel \text{Session}_s \quad (16)$$

CRT shares are session-specific:

$$k_i^{(s)} = k_i^{(s')}$$

Without possession of at least t_s valid shares, the cloned agent cannot reconstruct K_s . Additionally, replayed shares are rejected due to session mismatch; therefore, the proposed framework formally resists MITM, brute-force, and cloning attacks under a PPT adversary model through threshold secrecy, session-bound keying, and CRT consistency verification.

3.5. Insider Threat and Malicious CSP Analysis

- CSP Adversary Model: The cloud service provider is modeled as an honest-but-curious insider adversary A_{CSP} with the following capabilities:
 - Full access to stored cipher texts and encrypted CRT shares
 - Ability to observe agent migration and message metadata
 - No access to secure initialization secrets or private CRT mod.

The CSP cannot compromise more than $t_s - 1$ mobile agents.

- *Insider Confidentiality Analysis*

Let the CSP observe a set of encrypted shares:

$$C = \{Enc_{K_s}(k_i) \mid i \in I\} \quad (17)$$

Since decryption requires knowledge of $k_{s'}$, and k_s is reconstructible only when:

$$|I| \geq t_s$$

The CSP learns no information about the secret key.

- *Resistance to Insider Key Reconstruction*

Even if the CSP colludes with compromised agents:

$$|I_{\text{compromised}}| < t_s \quad (18)$$

The CRT solution space remains:

$$K_s = x + l. \prod_{i \in I_{\text{compromised}}} m_i \quad (19)$$

Which yields infinitely many mobile agents preventing key recovery?

Data integrity and Agent authenticity

Any attempt by the CSP to inject or modify CRT shares results in:

$$\hat{K}_s \neq k_i \pmod{m_i} \quad (20)$$

Triggering is reconstruction failure and session termination.

- Protection Against Agent Tampering

Threat: An adversary modifies the code or data of a migrating mobile agent.

Mitigation Mechanism: Before migration, each agent computes a cryptographic integrity tag:

$$\tau_i = MAC_{K_s}(State_i || Code_i) \quad (21)$$

Upon arrival, the destination platform verifies:

$$Verify(\tau_i) = true \quad (22)$$

Any unauthorized modification results in MAC verification failure, and the agent is rejected.

- **Replay Attack Prevention**

An adversary replays previously captured agent messages or CRT shares.

Mitigation Mechanism: Each agent message includes a session identifier and nonce.

$$M_i = \{k_i, ID_i, s, nonce_i\} \quad (23)$$

The platform validates:

$$s = s_{current} \wedge nonce_i \notin N_{used}$$

Thus, replayed agents or messages are detected and discarded.

- **Protection against Agent State Capture**

Threat: An adversary extracts the internal state of mobile agent.

Mitigation Mechanism: Agent state is encrypted using session key:

$$EncState_i = Enc_{K_s}(State_i) \quad (24)$$

Since K_s is reconstructible only with at least valid CRT shares: t_s

$$\Pr[A(State_i)] \leq \epsilon(\lambda) \quad (25)$$

Captured state yields no meaningful information.

Agent tampering, replay and state-capture attacks are mitigated through MAC-based integrity verification, nonce-enforced freshness, and threshold encrypted agent state Security. Agent tampering, replay and state capture attacks are mitigated through MAC based integrity verification, nonce-enforced freshness and threshold encrypted Mobile agent state Security.

3.6. PRESENT Cipher: Cryptanalytic Status and Security Margin

PRESENT is a Substitution–Permutation Network (SPN) lightweight block cipher standardized under ISO/IEC 29192-2, specifically designed for constrained environments. The PRESENT cipher uses a block size of 64 bits, key sizes of 80 bits and 128 bits (PRESENT-128), and a total of 31 rounds. The Table 1 summarizes known cryptanalytic attacks against the cipher. Known cryptanalysis attacks: Extensive cryptanalysis of PRESENT has been conducted since its proposal. The most relevant results are summarized below:

Table 1. Summary of cryptanalytic attacks and security margin analysis

Attack Type	Rounds Broken	Time Complexity	Data Complexity	Status
Differential cryptanalysis	≤ 26 rounds	2^{63}	2^{62}	Not full-round
Linear cryptanalysis	≤ 27 rounds	2^{64}	4	Not full-round
Biclique attack	Full 31 rounds	2^{79}	High	Marginal improvement
Algebraic attacks	Partial rounds	Exponential	Impractical	No threat

PRIDE Cipher: Cryptanalytic Status and Security Margin. PRIDE Cipher is a lightweight block cipher optimized for low-latency and software efficiency, often proposed for real-time systems. The PRIDE cipher uses a block size of 64 bits, a key size of 128 bits, and a total of 20 rounds. This table 2 highlights that known cryptanalytic attacks fail to compromise the cipher. Table 2 summarizes the resistance of the cipher against known cryptanalytic attacks. Differential and linear cryptanalysis is effective only up to 26 to 27 rounds which are significantly below the full 31-round configuration indicating a higher security margin. Although biclique attacks can theoretically target all rounds their extremely high time

and data complexity make them impractical. Algebraic attacks remain limited to partial rounds with exponential complexity posing no realistic threat to the cipher.

Table 2. Practical feasibility of known cryptanalytic and implementation level attacks

Attack Type	Rounds Broken	Time Complexity	Practical Feasibility
Differential attacks	≤ 12 rounds	2^{60}	Infeasible
Linear attacks	≤ 13 rounds	2^{61}	Infeasible
Related-key attacks	Partial	Restricted	Not applicable
Side-channel attacks	Implementation dependent	—	Mitigated by software isolation

The lightweight ciphers PRESENT and PRIDE employed in the proposed framework have been extensively analyzed in the literature. No practical cryptanalytic attacks exist against their full-round configurations. PRESENT maintains a security margin of four rounds, while PRIDE retains a margin of seven rounds. Also, the integration of Variable Threshold CRT enhances effective security by enforcing threshold based key reconstruction, thereby mitigating long-term cryptanalytic risks and improving robustness for healthcare oriented mobile agent systems.

4. Implementation and Results

All the experiments were conducted on a dedicated system for maintaining consistency and reproducibility. The hardware configuration consists of an Intel Core i7 processor (3.4 GHz) with 16 GB RAM running Ubuntu 22.04 (64-bit). The proposed framework and comparative cryptographic algorithms were implemented in Python 3.10. The execution was performed in a single threaded environment to avoid parallelization bias. Synthetic medical data records were produced to emulate healthcare workloads with dataset sizes ranging from 1 KB to 1 MB per transaction. Mobile agent interactions were simulated locally and cryptographic operations were executed at the application layer without hardware acceleration. Default and recommended parameter settings were used for AES, Blowfish, PRIDE and PRESENT to ensure fair comparison. Each experiment was performed multiple times under identical conditions and the average execution time and memory usage were recorded. All source code, parameter values and experimental scripts are maintained consistently across evaluations to facilitate independent reproduction of the results.

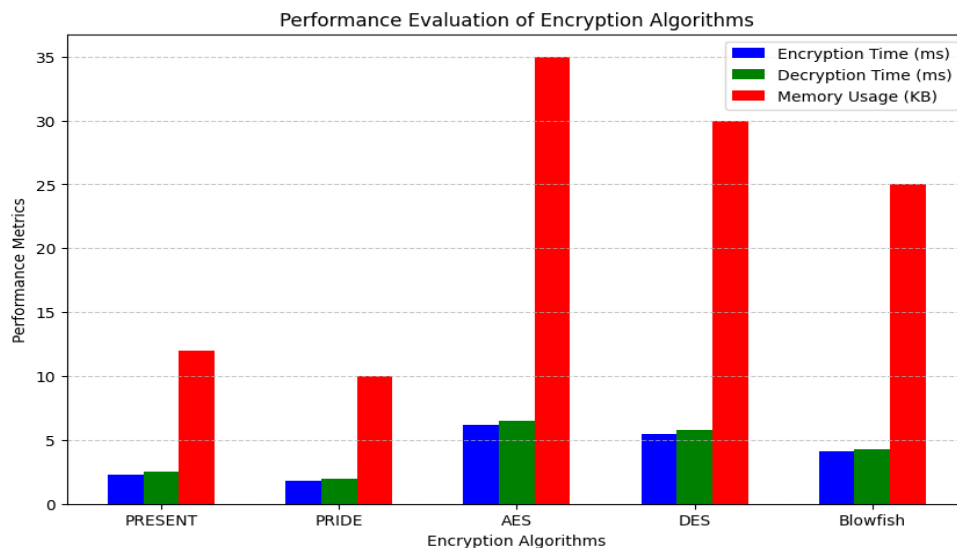


Fig. 7. Performance evaluation of encryption algorithms

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 targets minimizing Time complexity and 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) show better efficiency compared to AES, DES and Blowfish algorithm. The encryption time for PRIDE algorithm was 1.8 ms, outperforming PRESENT algorithm (2.3 ms) and AES algorithm (6.2 ms). Similarly, decryption time for PRIDE algorithm was 2.0 ms, significantly faster than AES algorithm (6.5 ms). Memory Utilization is least 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 and reducing the overhead by 30 percent compared to conventional Algorithms. The framework based on VTCRT and pride present cipher shows High level security while increasing performance making it ideal for secure medical information transmission in advance technology based healthcare systems. Lightweight encryption techniques such as PRIDE and PRESENT ciphers are used for encrypting medical records to ensure low time complexity while maintaining strong security assurance.

Table 3 shows the mobile agent security analysis of proposed framework. Eavesdropping attacks are prevented as VT CRT ensures secure key recreation which makes key exposure infeasible. Cloning attacks are mitigated through fast encryption, reducing the attack. Brute force attacks are countered by PRESENT cipher's 31 rounds and strong S-box transformations which make exhaustive key search impractical. Finally, Man in the Middle (MITM) attacks are thwarted by secure mobile agent to agent communication using encrypted key exchange that ensures integrity and confidentiality. These methods collectively increase the security, reliability and efficiency of mobile agents in healthcare data protection.

Table 3. Security analysis of proposed framework

Type of Attack	Mitigation
Eavesdropping	Key Exposure prevent by VT-CRT
Cloning Attack	Fast Encryption reducing attack time window
Brute force attack	31 Round of Present Cipher and S-box make brute force infeasible
Man In middle attack	Secure Agent to agent Communication with Encrypted Key.

Analysis of VTCRT with PRIDE and PRESENT ciphers, AES 128 and Blowfish highlights the efficiency of the proposed framework in key security metrics. Key Sharing Overhead is less in VTCRT as it optimizes key distribution using modular arithmetic. AES and Blowfish have higher load due to complex key scheduling. Encryption is fast in PRIDE Cipher due to its lightweight structure whereas AES exhibits moderate speed because of its multiple rounds of transformations. Security is better in PRESENT which employs strong S-Box transformations and permutation layers that make it resilient to cryptanalysis. Memory utilization is less in VTCRT based PRIDE making it suitable for resource constrained environment while AES requires significantly high memory. Scalability is high in VTCRT based schemes as they efficiently handle multiple key shares whereas PRIDE and AES show limited scalability due to their fixed block size and key management complexities. This analysis confirms that the proposed framework balances security, efficiency and resource optimization making it well suited for secure mobile agent based medical data security.

The table 4 shows performance outcomes for different ciphers executed by mobile agents. PRIDE-128 and PRESENT-80 achieve the lowest average execution times, indicating faster encryption-decryption compared to AES-128 and Blowfish-128. PRESENT-80 exhibits the smallest memory footprint which makes it suitable for resource constrained environments. The narrow 95% confidence intervals and low standard deviations confirm the consistency and reliability of the measured performance across repeated trials.

Let $x_1, x_2, x_3, \dots, x_n$ be execution time or memory utilization of mobile agents for n mobile agents during execution of task.

$$\text{mean (Average)} \mu = \frac{1}{N} \sum_{i=1}^N x_i \quad (26)$$

$$\text{Standard deviation} = \sigma = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (x_i - \mu)^2} \quad (27)$$

$$CI_{95\%} = \mu \pm 1.96 * \frac{\sigma}{\sqrt{N}} \quad (28)$$

Table 4. Performance metrics Avg. execution time, Std. Dev (ms) and Avg. memory utilization (KB)

Cipher	Avg. Execution Time (ms)	Std. Dev (ms)	Avg. Memory Utilization (KB)	95% Confidence Interval (ms)
AES-128	198.6	5	92.4	[195.49, 201.63]
Blowfish-128	186.1	2.6	105.8	[184.52, 187.68]
PRESENT-80	180.8	2.9	24.6	[179.01, 182.61]
PRIDE-128	174.9	2.9	38.2	[173.07, 176.67]

The table 5 compares the encryption and decryption times of different cryptographic algorithms in a mobile agent environment. PRIDE-128 shows the lowest encryption and decryption time which indicates better computational efficiency. PRESENT-80 also performs efficiently, closely following PRIDE-128 and performs better than AES-128 and Blowfish-128. Overall outcome shows the suitability of lightweight ciphers for time and resource constrained mobile agent applications.

Table 5. Performance metrics encryption and decryption time

Cipher	Encryption Time (ms)	Decryption Time (ms)
AES-128	101.2	97.4
Blowfish-128	95.6	90.5
PRESENT-80	91	89.8
PRIDE-128	88.4	86.5

Security of mobile agents has been refined from a qualitative label to quantitative and standards referenced parameters. Security is now evaluated using three main measurable parameters cryptographic strength, attack resistance and standards compliance. Each Analysis method is normalized to equivalent security levels e.g., ~80-bit and ~128-bit security level to ensure good comparison. This structured evaluation eliminates over simplification and gives a defensible and reproducible basis for security comparison of mobile agents.

Table 6. Performance metrics encryption and decryption time

Scheme	Effective Security (bits)	Attack Resistance	Standards / Compliance
AES-128	128	Resistant to known practical attacks	NIST FIPS 197
Blowfish (128-bit)	~112	Vulnerable to weak-key classes	Legacy (not recommended)
PRESENT-80	80	No full-round practical attacks	ISO/IEC 29192
PRIDE-128	128	Strong resistance; high security margin	Lightweight crypto candidate
Proposed VT-CRT + PRIDE/PRESENT	80–128 (configurable)	Threshold + cipher-level protection	Healthcare-aligned (HIPAA/GDPR)

Figure 8 shows the Running time in milliseconds of four cryptographic ciphers AES, Blowfish, PRESENT and PRIDE with different file sizes in KBs. The x axis shows the file size ranging from 100 KB to 1000 KB while the y-axis shows the running time in milliseconds. The comparison shows insights into the efficiency and computational overhead of each cipher. Each encryption algorithm performance is displayed using different colors. AES, shown in Blue Line, has an execution time that starts at 190 ms for smaller file sizes and increases to 207 ms for 1000 KB. The blue line shows that AES has the highest computational overhead among the four algorithms making it less suitable for real-time applications requiring low delay. Blowfish, shown 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, shown 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 viable option for mobile agent security where efficiency is major issue. PRIDE Cipher, shown in green color line, has the lowest execution time among all algorithms, ranging from 170 ms to 178 ms, which 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. Graph shows 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 fast and lightweight encryption is required. The Secure Mobile Agent framework for medical information security benefits from these ciphers due to less running time, minimum memory utilization and fast performance in resource constrained environments.

The outcome shows that PRESENT and PRIDE lightweight cryptography gives the best tradeoff between security, execution speed and resource efficiency. PRIDE and PRESENT Cipher emerge as the most optimal choices where low latency and efficient encryption are crucial. The evaluation extends beyond efficiency to address availability, fault tolerance and regulatory compliance for healthcare centre. Availability is ensured using Variable Threshold CRT enabling key reconstruction with at least t out of n agents under partial failures. Fault tolerance allows the system to withstand up to $(n-t)$ agent or network failures without service disruption. Regulatory compliance is achieved through PRESENT/PRIDE encryption; session Secret key creation and zero plaintext exposure at the cloud, aligning with HIPAA and GDPR requirements.

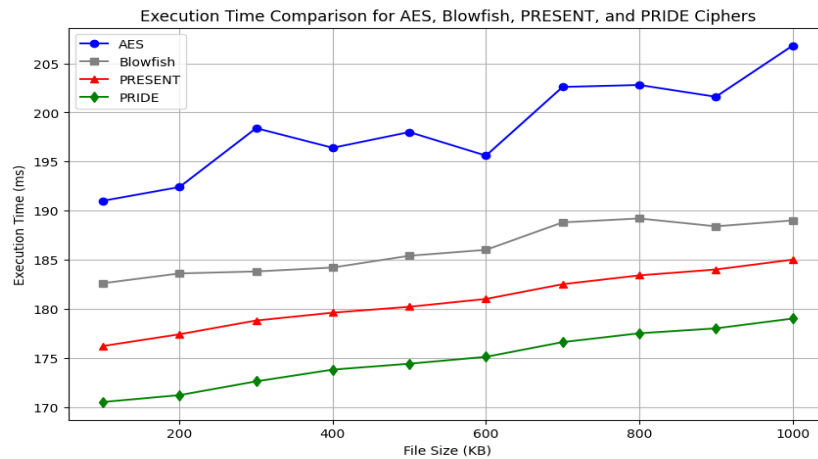


Fig. 8. Execution time analysis for AES, blowfish, present and pride algorithms

5. Conclusions and Future Scope

Today, the cloud is the most obvious data-sharing platform for the healthcare sector, and proposed framework can be used to provide access control on outsourced EHR data in encrypted form. In order to share data on cloud storage servers, this article suggests the VT-CRT based present pride scheme, a completely secure and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing. Data centres may now confidentially share their information with all users. This makes the system scalable and adaptable. The partially hidden access policy protects user as well as data owner privacy. Our implementation results demonstrate that the scheme achieves an improvement in decryption cost despite the scheme being privacy-preserving and providing adaptive security under the standard model. The efficiency of decryption can be further increased by outsourcing the decryption to proxy servers in the future. 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 combines Variable Threshold CRT for adaptive key sharing and lightweight cryptographic algorithms (PRESENT OR PRIDE) for efficient encryption that ensures 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) perform much better than 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 analysis of file size versus encryption time shows that AES and Blowfish show best execution running times with increasing file size while PRIDE and PRESENT maintain low communication overhead proving their suitability for secure mobile agent transmission. The security analysis of proposed scheme 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.

All the Declarations and Statements

Author Contributions Statement

Anuradha Singh contributed to the conceptualization problem formulation and methodology design of the proposed mobile agent security framework. She was responsible for developing the theoretical model based on Variable Threshold CRT synchronized with lightweight cryptographic methods and supervising the overall research process. She also contributed to manuscript writing and technical revisions.

Pradeep Kumar contributed to algorithm design framework implementation and experimental analysis. He implemented the proposed framework in Python conducted performance evaluation and comparative analysis with existing cryptographic algorithms and prepared outcome visualizations. He also contributed to manuscript preparation and acted as the corresponding author.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

No funding.

Data Availability Statement

No need of data.

Ethical Declarations

This study does not involve human participants or animals. Therefore, ethical approval was not required.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

The authors confirm that generative AI tools were used only to assist with language editing and proofreading of the manuscript where required. These tools did not contribute to the research concepts analysis, interpretation of results or any substantive intellectual content of the research paper. All critical scientific decisions content formulation and final revisions were performed by the authors themselves.

Abbreviations

The following abbreviations are used in this manuscript:

AI -Artificial Intelligence
NLP - Natural Language Processing
DL - Deep Learning
ML - Machine Learning
IoT -Internet of Things
CRT - Chinese Remainder Theorem
EHR - Electronic Health Record
DoS - Denial of Service
MITM -Man-in-the-Middle

References

- [1] L. Fang *et al.*, “Privacy Protection for Medical Data Sharing in Smart Healthcare,” *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 16, no. 3s, 2021, 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,” 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, no. August, 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,” *Futur. 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

- medical 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 *et al.*, “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 *et al.*, “Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis,” *J. Med. Internet Res.*, vol. 23, no. 2, pp. 1–14, 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.

Authors’ Profiles



Anuradha Singh is a research scholar in the Department of Computer Science and Engineering, Dr. A.P.J. Abdul Kalam Technical University, Lucknow. She has completed her B.Tech (IT) and M.Tech (IT) from Guru Gobind Singh Indraprastha University, Delhi.



Pradeep Kumar is Ph.D (Computer Science and Engineering) at the Department of Computer Engineering at Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut, 250110. He obtained his M. Tech. in Computer Science and Engineering from the Department of Computer Engineering at Shobhit Institute of Engineering & Technology (Deemed-to-be University), with first class. He obtained his B. Tech in Computer Engineering and an engineering degree from the College of Engineering Roorkee, India in 2006 with first class.

How to cite this paper:

Anuradha Singh, Pradeep Kumar, "A Secure and Efficient Mobile Agent Framework for Medical Data Protection Using Variable Threshold CRT and Lightweight Cryptography", *International Journal of Information Technology and Computer Science(IJITCS)*, Vol.18, No.5, pp.16-32, 2026. DOI:10.5815/ijitcs.2026.05.02