I.J. Wireless and Microwave Technologies, 2026, 5, 145-157
Published Online on October 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.05.09

A Lattice-Enhanced Dynamic Threshold CRT-Based Secret Sharing for Mobile Agent Security in Decentralized Networks

Priyank Sirohi
Sir Chhotu Ram Institute of Engineering and Technology, C.C.S. University, Meerut, India
Email: priyanksirohi01@gmail.com
ORCID ID: https://orcid.org/0009-0005-4334-1926

Kakoli Banergee
Department of Computer Science and Engineering, JSS University, Noida, Uttar Pradesh, 201301, India
E-mail: kakoli.banerjee@jssaten.ac.in
ORCID ID: https://orcid.org/0000-0002-4306-2194

Bijendra Tyagi
Department of Computer Science and Engineering, JSS University, Noida, Uttar Pradesh, 201301, India
E-mail: bijendra.tyagi@jssaten.ac.in
ORCID ID: https://orcid.org/0000-0002-0732-9584

Anuradha Singh
Department of Information Technology, JSS University, Noida, Uttar Pradesh, 201301, India
E-mail: anuradha.singh@jssaten.ac.in
ORCID ID: https://orcid.org/0000-0008-4765-1341

Pradeep Kumar*
Department of Computer Science and Engineering, JSS University, Noida, Uttar Pradesh, 201301, India
E-mail: pradeep8984@jssaten.ac.in
ORCID ID: https://orcid.org/0000-0001-6177-8527
*Corresponding Author

Received: July 3, 2026; Revised: August 05, 2026; Accepted: September 22, 2026; Published: October 8, 2026

Abstract: A mobile agent is a small piece of program that migrates automatically among different platforms, on which it executes assigned tasks. Mobile agents migrate in malicious and unsecure networks. So, there will be chances of compromising mobile agent as well as host computer. So, during the mobile agent executing life cycle there will be chances of stealing of confidential information about host and agents. The application of mobile agents is increasing day by day in various domains such as distributed computing, cloud computing and Internet of Things. In this article, we propose a method based on lattice-based dynamic threshold Chinese Remainder Theorem for the security of mobile agents. The combination of dynamic threshold, lattice-based encryption-decryption and Chinese remainder theorem provides optimal security as compared to traditional approach. After the analysis of turnaround time of creation of share, distribution and recreation of secret is optimal as compared to traditional approach. Another comparison is also done on the basis of memory utilization, computational cost, communication overhead and scalability of proposed method. Proposed approaches provide effectiveness of security for mobile agents in a decentralized and malicious environment. The framework was implemented in Python and analyzed with 10 to 1000 mobile agents. With 1000 mobile agents, the framework gains a turnaround time of 12.4 ms, memory utilization of 18.7 MB, and CPU efficiency of 91.3%, demonstrating better scalability and computational cost compared with Shamir Secret Sharing, Integer CRT, Homomorphic Encryption, Vectorized Tree Parity Machine and Boneh Goh Nissim techniques. Performance evaluation based on computational cost, communication overhead and scalability further shows the effectiveness of the framework. These outcomes show that the proposed methods provide an efficient, scalable and post-quantum-secure method for securing mobile agents in cloud computing, Internet of Things (IoT), and other decentralized distributed computing environments.

Index Terms: Mobile agent, Threats on mobile Agents, Encryption and decryption based on lattice, Dynamic threshold,

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

Chinese remainder theorem CRT

1. Introduction

A mobile agent is a small piece of code that migrates automatically across various platforms to carry out assigned tasks for a host. Due to their intelligence, mobility and autonomy, mobile agents are useful for different real-time applications. They can do activities, collect data, analyze information, and communicate with distant resources with little assistance from humans.

Figure 1 shows the migration process of a mobile agent in a distributed environment. Initially the mobile agent is created at the home platform and where assigned some specific tasks with required execution parameters. The mobile agent then migrates through the network to one or more remote platforms for assigned task execution. At the hour of migration, the communication channel is vulnerable to various security threats such as eavesdropping, data tampering, impersonation and malicious attacks. After reaching the destination platform, the mobile agent executes the assigned task, collects the necessary output, and may continue migrating to other platforms if necessary. At the end the mobile agents return back to the home platform or forwards the processed information to another authorized platform. Execution model reduces network load and increases distributed processing efficiency. It also necessitates robust techniques for authentication, confidentiality, integrity and secure state synchronization throughout the migration process.

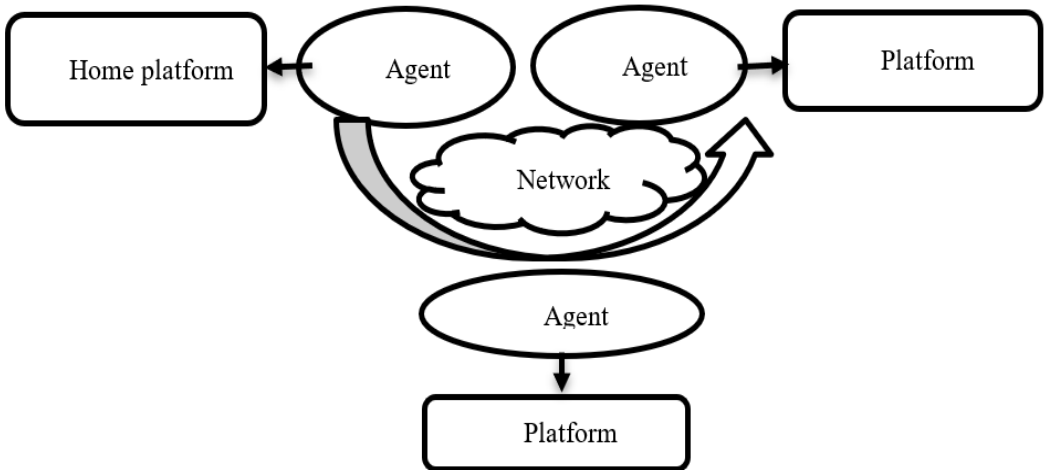


Fig. 1. Mobile Agent System

The use of mobile agents in contemporary distributed computing systems has completely changed the way activities are completed in a variety of dynamic environments. Because they may move between platforms to carry out autonomous activities, these agents are widely used in a variety of applications, such as cloud computing, e-commerce, Internet of Things (IoT) systems, and healthcare. Life cycle of mobile agent during the execution of assigned task is shown in figure 2.

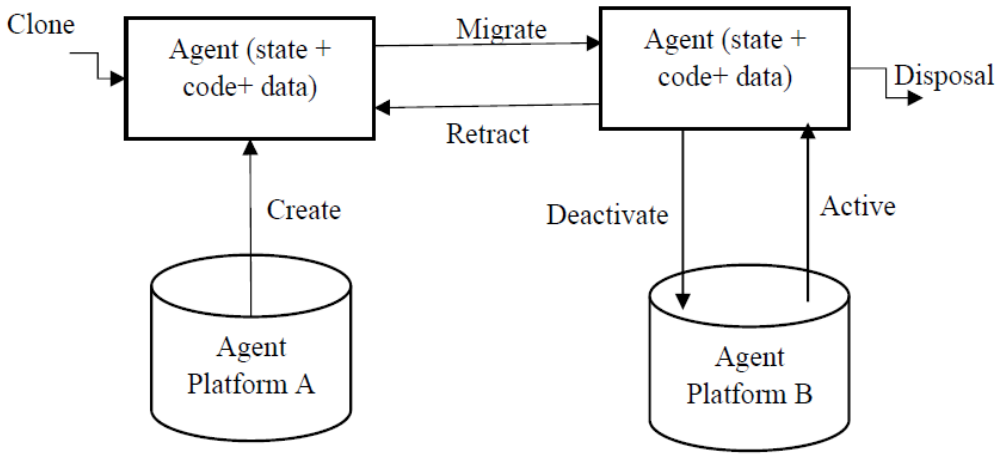


Fig. 2. life cycle of mobile Agent during execution

1.1. Advantage of mobile agent for real life application

- **Low Network Load:** A mobile agent does not carry large data; it only carries small activity output and some short result after the execution of task on assigned platform or server. Because of this characteristic mobile agent network have low latency and network congestion.
- **High Flexibility and Efficiency**: Using mobile agents in real time systems makes it easy to manage the resources of different places with high efficiency and flexibility.
- **Improved Fault Tolerance:** Mobile agents migrate to various platforms for the execution of assigned task within the network. If one system fails there is no impact on the execution of task.
- **Load Balancing and Decentralization**: Mobile agents use decentralized computing and load balancing in an efficient manner in malicious environments. Mobile agent uses job distribution to different platform for fast execution of assigned task.
- **Less Response Time:** Using mobile agent technology reduces the execution time of assigned tasks.
- **Autonomy and Adaptability**: Autonomy and adaptability are the main characteristics of mobile agents. A mobile agent executes the task without the need of centralized control for real time application.

1.2. Challenges and Considerations

Mobile agent in real time application faces the different issues like security of mobile agent during migration, Coordination of mobile agents for execution of task, optimized recourse allocation, and scalability of system.

- **Security of mobile Agents:** Mobile agents are moving automatically for executing task. Security of mobile agent is prime concern during performing task. Security includes authentication, access control, integrity of mobile agents, and security of data of mobile agent by malicious agents and platform.
- **Mobile Agents Coordination**: The coordination and synchronization of mobile agents for large task execution is prime concern. So, there is requirement of advance algorithm for coordination of mobile agents for consistency of data, and to avoid disputes transaction.
- **Resource Allocation for mobile agents**: For mobile agent operation, the resources of a platform play an important role in the execution of tasks. To avoid the overload efficient resource allocation is required for real time application.

The major concern of this paper is security of mobile agent during the transmission of agents. To provide security for the mobile agent system, we propose a method based on lattice-based variable threshold Chinese Remainder Theorem. Proposed method is focusing on concerns about mobile agent data integrity, confidentiality, and authenticity when mobile agent migrates over different networks. In conventional security mechanism it is difficult to provide dynamically change threshold parameter and control all agents in decentralized way. Mobile agent's technology plays a major role for improving real time distributed application, fault tolerance, efficiency and responsiveness. They lower latency and enhance system performance by completing activities nearer the data source. To fully realize their promise in real-time computing systems, however, we must solve important issues like security and coordination.

Despite significant advances in mobile agent security, traditional secret key sharing and cryptographic techniques still exhibit many issues when deployed in dynamic and decentralized environments. Conventional Shamir's Secret Key Sharing and CRT-based techniques employ fixed thresholds, making them unsuitable for environments where the security requirements and number of participating mobile agents change dynamically. Moreover, most traditional techniques focus on secure secret key recreation without providing fast method for adaptive threshold adjustment or secure state synchronization among migrating mobile agents. Although lattice-based cryptography gives strong post-quantum security, current lattice-based secret key sharing techniques rarely synchronized dynamic threshold with CRT-based reconstruction for mobile agent applications like IOT, E-commerce etc. Consequently, there is requirement of lightweight, scalable and post-quantum-secure framework that synchronized dynamic threshold update, fast secret key reconstruction and secure mobile agent migration while maintaining low computational and communication cost.

The main contributions of this paper are proposed a secure mobile agent framework by synchronized lattice-based cryptography with variable threshold Chinese Remainder Theorem (CRT) secret key sharing to improve confidentiality, integrity, authentication and post-quantum security in malicious environments. Suggested framework is evaluated with respect to traditional methods and demonstrates improved computational cost, scalability and security. Paper is organized as follows: Section 2 shows the reviews of previous related work, Section 3 demonstrates the proposed framework, Section 4 discusses the implementation and experimental outcomes and Section 5 concludes the paper with future scope.

2. Related works

Previous research work and development in lattice-based cryptography, secret sharing strategies, and mobile agent security are described in the related work section.

Chen J et al. [1] summarized and studied the lattice-based threshold secret sharing key technique. The paper is a

review of lattice-based threshold secret key sharing schemes and classifies techniques as per their various functions and compares and analyzes them. Further article also deeply studies the application research of TSS techniques in various area, including blockchain, threshold federated learning and cryptography techniques. At present lattice-based secret key sharing is still fast-growing technique and a more usable technique. Optimization of this research is future scope.

Pradeep [2] proposed model focuses on securing mobile agents and addresses key challenges in mobile agent security. It leverages two polynomial-based authentication systems to enhance security. The model uses the Blowfish algorithm for encoding patient information, as it offers an efficient alternative to other encryption methods. Blowfish, a symmetric encryption algorithm, requires a secret key for both encryption and decryption, which is generated and authenticated through the polynomial-based systems. The choice of Blowfish over DES and AES is based on its optimal performance in terms of speed and security. When compared with other symmetric key cryptosystems, the proposed model's key generation and key recreation processes were found to significantly outperform those of the CRT and Euler methods.

Ivan Damgård [3] noted that by adding a trapdoor feature to the commitment, it is possible to achieve safe two-round n-out-of-n distributed signing and multi-signature in the simple public key framework in addition to resolving the slight problem with aborts. A secondary contribution of this research is the creation of appropriate trapdoor commitment from lattices.

Joon Sik Kim [4] suggested a dynamic TKEM with a transparent setup, allowing for a flexible selection of both receiver and thresholds without need of trusted third parties in the setup stage. furthermore, our construction does need of pairing operations, that is less efficient compared to exponentiation. Demonstrate the selective chosen-ciphertext security of our construction under the decisional Diffie-Hellman assumption, zero-knowledge and soundness of a non-interactive zero-knowledge (NIZK) proof system. Proposed technique satisfies decapsulation consistency when the underlying NIZK system is sound. Proposed proof-of-concept implementation shows the practicality and efficiency of these techniques, further improving the area of threshold cryptography.

Guyue Li [5] Suggested techniques can guarantee key confidentiality even in the face of adversaries with infinite computing power. By redesigning a multi-user application edge forwarding techniques, the fundamental techniques that were developed for a single-user scenario are expanded into a multi-user scenario. Furthermore, different enhancement tactics are investigated to decrease the time delay and increase the secret key generation rate in a secure manner in order to make CR-QKD more practical. In a metropolitan area network two distant loT devices that are about fifteen kilometers apart trade secret keys in order to showcase a CR-QKD prototype. CR-QKD enables a secret key rate of 424 bits per second with a retransmission rate of 2.1 percent, according to experimental findings.

Niraj Singhal [6] Proposed a multilevel authentication framework for mobile agents and platforms using Lagrange interpolation and Fast Fourier Transformation to enhance security across multiple levels. By incorporating multiple security layers, the system creates confusion for malicious mobile agents, offering robust key protection through a threshold-based value and a strong key management scheme. This approach ensures that only the authorized number of users can access the mobile agents. The validation of mobile agents across different platforms is a critical security aspect. The proposed framework strengthens key security at multiple levels, one for authentication and another for task execution. Experimental results demonstrate that our scheme requires less computational time compared to the CRT-based algorithm, providing multilevel security and being approximately 10% faster than the single-level authentication based on CRT.

Pallavi bagga [7] Suggested a thorough analysis of the typical threats to mobile agents and their platforms, as well as the shortcomings of the current defenses, with three primary contributions: It starts by introducing researchers to different security goals and criteria. Second, it examines several prevention and detection strategies meant to lessen security issues in mobile agent systems. Thirdly, it talks about the security issues that will arise in this field in the future. In conclusion, researchers that are interested in resolving security concerns in mobile agent-based systems may find this survey to be a useful resource.

Longlong Li [8] Proposed a (k,n) threshold Secret Image Sharing (CRTSIS) technique based on the Chinese Remainder Theorem that is both lossless and practical. The suggested method overcomes the difficulties in using Asmuth and Bloom's technique with image data. Based on the locations of the secret pixels, the Least Significant Bit (LSB) matching approach is utilized to embed the LSBs into random integers. The secret is the high seven bits of grayscale pixels. The scheme’s usage of moduli larger than 255 and a screening procedure to exclude erroneous pixels are two of its main innovations. Consequently, the size of the shares and the secret space are equal.

K. meng [9] A proactive secret sharing plan requires shareholders to update their shares on a regular basis without changing the secret. Improved protection for long-lived secrets is achieved by ensuring that an opponent can only recover the secret by capturing at least t shares within a specified period, rather than at any time. There is currently no Chinese Remainder Theorem (CRT)-based PSS scheme that has been suggested, despite the fact that most extant PSS schemes are based on linear secret sharing (SS). In addition to introducing a CRT-based PSS scheme for the integer ring, this study examines the reasons why conventional CRT-based SS schemes are inappropriate for PSS scheme design. The isomorphism of CRT is also used to build efficient share refreshing in an ideal PSS scheme based on CRT for polynomial rings.

Dinesh Pande[10] Introduced a single secret picture sharing method that uses the Boolean XOR operation, a modified Shamir's scheme, and the Chinese Remainder Theorem (CRT). The technique makes use of inverse CRT for share generation and reconstruction, Boolean XOR operation, and a modified version of Shamir's Secret Sharing system. The

shares that were highly randomized and those that were evenly distributed were separated using histogram analysis. The outcomes of the study demonstrate that the secret has been fully recovered.

Jinrui Chen[11] The Chinese Remainder Theorem (CRT) is the basis for a Secret Image Sharing (SIS) technique that generates tiny shadow images. Approximately 1/k of the original hidden image is decreased in size to create these shadow images. Auxiliary encryption is not required by using random bits in the binary representations of the random factors in the CRT. Additionally, the technique can take advantage of all the benefits of CRT, such as a (k,n) threshold, lossless recovery, and low computational complexity, by carefully adjusting the random variables. Experiments and analyses confirm that the suggested plan works.

Kareem Shehata et al. [12] suggested the first effective verifiable WSS method that is compatible with the most recent CRT-based WSS and can withstand malevolent sellers [9]. Our approach presents new privacy-preserving methods for demonstrating relationships between committed values, which may be of independent interest, and employs Bulletproofs for effective verification. Ethereum evaluations reveal improvements in communication complexity of up to 100 × over the existing design and 20 × over unweighted VSS technique.

Yung-Hsiang[13] Suggested a weighted threshold secret sharing method and shows that it is asymptotically perfect using the (CRT). As all CRT-based secret sharing schemes rely on special sequences of pair wise coprime integers as parameters, this paper introduces the first algorithm for generating these integers. The correctness of the algorithm is proven using the prime number theorem. Experimental results validate the effectiveness and efficiency of our algorithm, as well as the space efficiency of our scheme when utilizing the integer sequences generated by it. Our scheme, along with the parameter generation algorithm, can be applied to various applications, including threshold cryptosystems.

Xingxing Jia[14] Presented a productive Collaborative Secret Sharing (CSS) system created especially for group collaboration participants with multiple privileges. In order to prevent information leaking, the CSS scheme is built by rearranging multi-privilege participants inside each participant set and then splitting them up into several separate secret sharing schemes, each with multi-privilege shares. The plan, which is based on the Chinese Remainder Theorem, guarantees that each multi-privilege member keeps only one share and offers a simpler recovery process. The scheme is shown to offer asymptotically perfect security. According to experimental findings, the scheme is effective for teamwork and provides computational benefits over current approaches found in the literature.

Lein harn [15] A novel secret key sharing method based on a bivariate polynomial, shares that were first created by a dealer can be used to both reconstruct the secret and keep the shares hidden while doing so over a network. Without requiring any changes, we further extend this technique in this work to become a Threshold Changeable Secret Sharing (TCSS) scheme. The suggested TCSS is non-interactive and dealer-free. Three possible uses for the shares created by our method are (a) to rebuild the secret, (b) to safeguard the confidentiality of shares while they are being rebuilt over a network, and (c) to enable the threshold changeable property.

Ramakant Kumar [16], In order to avoid players having to hold their secret keys, a lattice-based threshold secret sharing method is suggested, in which participants choose their shares and safely transmit them to the dealer. Each participant has a single share in the multi-use, multi-stage, verifiable scheme. Due to the single-share structure, even if the shareholder sets are different, participants can own one share that represents several secrets. This feature makes it possible to manage participant shares with a great deal of storage efficiency.

Boxue Huang [17]The Ring Learning with Errors (RLWE) problem served as the foundation for the proposed lattice-based Cipher text Policy Attribute-Based Encryption (CP-ABE) scheme, which is more effective than systems based on the conventional Learning with Errors (LWE) problem. To enable effective user revocation and dynamic management of user groups, this system adds indirect revocation and a binary tree-based data structure. Additionally, it permits several authorities to collaborate in setting system parameters and managing key distribution in order to improve the scheme's effectiveness and facilitate file exchange across firms. Additionally, the method offers Decryption Key Exposure Resistance (DKER) by re-randomizing users' private and update keys. Based on a traditional security architecture and a series of security implementation, the architecture is safe from chosen-plaintext attacks. Output of proposed scheme show it is better than traditional one.

Chen-Da Liu-Zhang et al. [18] suggested a secure technique that needs no trust to generate shared random variables in distributed networks. The protocol greatly reduces communication load while preserving security against malevolent adversaries by requiring every participant to communicate just once in a serial order. Through cryptographic method that allow for dishonest or flawed user, it guarantees correctness, unpredictability and robustness. The proposed technique works well for blockchain consensus, secure multiparty computation, threshold cryptography and other decentralized applications that need effective distributed randomness creation.

Although previous studies have significantly advanced mobile agent security, threshold secret sharing and lattice-based cryptography several research gaps remain. Conventional Shamir’s Secret Sharing and CRT-based techniques give reliable secret key recreation but are based on fixed thresholds, making them unsuitable for highly dynamic distributed environments. Threshold-changeable techniques improve flexibility but having high computational cost and communication overhead at the time of threshold updates. Traditional lattice-based techniques give strong post-quantum security; however, most are designed for general cryptographic applications and do not specifically address secure mobile agent migration with dynamic threshold management. Similarly, trust-based and authentication-oriented frameworks improve platform reliability but employ less efficient techniques for secret key reconstruction and quantum-resistant

security. Therefore, there is a requirement for a modified framework that synchronized adaptive threshold adjustment, CRT-based secret key reconstruction, lattice-based post-quantum security and fast mobile agent migration while maintaining low computational and communication cost. The proposed framework is designed to overcome these limitations.

3. Proposed solution

The aim of this research is to allow only authentic flow of data among mobile agents in malicious environments. Goal is to provide secure transmission maintaining integrity of data. To solve problem of authentication various algorithms of security in mobile agent vary on basis of evaluation criteria they apply. The primary goal of this research is to determine criteria that allow transmission of only authentic data. The suggested authentication model generates a synchronized key which assures authenticity of data received by a mobile agent. To solve problem of data integrity another objective underlying this research is to maintain the integrity of data while transmission. Security Framework of mobile agent based on Lattice based dynamic threshold secret sharing and Chinese Remainder Theorem (CRT). Figure 3 showing the proposed framework based dynamic threshold secret sharing and Chinese Remainder Theorem (CRT).

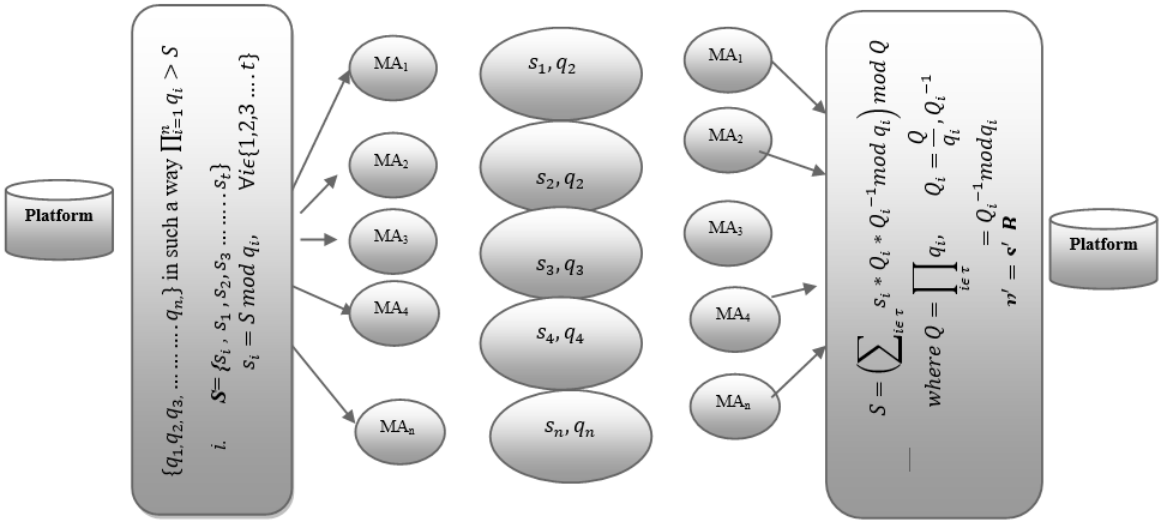


Fig. 3. Security frame work based on Lattice based dynamic threshold secret sharing and Chinese Remainder Theorem (CRT)

Proposed approach focuses on the major issues like data integrity, security, and authentication in decentralized distributed system. Framework is designed for the secure migration of mobile agents in cloud environment. Dynamically changing the threshold values improve the security of mobile agents. Proposed framework works on the basis of four algorithms, initialization, secret creation, secret reconstruction and dynamic adjust of threshold for different transactions. Algorithm 1 explains the initialization for secret sharing parameters on how to choose n different prime number $\{q_1,q_2,q_3, \dots \dots \dots q_n,\}$ and also fix the threshold values. Matrix L and B choose this step. Algorithm 2 is designed for secret creation, in which one secret is divided into multiple shares S= $\{ s_i , s_1 , s_2, s_3 \dots \dots . s_t\}$ $s_i = S \, mod \, q_i$, $\forall i \epsilon \{1,2,3 \dots . t\}$. and Lattice based encoding also done this step. Algorithm 3 discusses secret reconstruction and lattice verification. Algorithm 4 explains how to dynamically change the threshold for various transactions.

The framework follows a sequential and synchronized workflow among four interconnected modules, initialization, secret creation, secret reconstruction and dynamic threshold setup. In the first initialization module (Algorithm 1) the system creates the global security parameters which include the set of pairwise coprime number, lattice basis matrix B, public system parameters and the starting threshold value t. These parameters are securely shared to all mobile agents and host platforms. In Algorithm 2 the initialized parameters are used to partition the secret key into multiple secret shares using the CRT technique, after that every secret share is encoded using lattice-based cryptography before being assigned to the respective mobile agents together with its agent identifier and transaction state. At the hour of migration, every mobile agent maintains a synchronized state containing the current threshold, share index, session identifier and integrity code. Algorithm 3 choose at least t valid shares, verifies their integrity through lattice-based verification and recreate the secret key using the CRT reconstruction module. At the end module 4, using algorithm 4 monitors the execution environment and dynamically updates the threshold value according to the current security needs. The modified threshold and synchronization state are securely broadcast to all active mobile agents without regenerating the original secret key, ensuring consistency, secure parameter passing and combined execution throughout the mobile agent migration lifecycle. Figure 4 explains the whole workflow of the proposed secret key sharing and reconstruction technique. Initially the secret key gives as input to the Share Generation Process, where the secret key is partitioned into “n” independent shares using

the proposed lattice-based dynamic threshold Chinese Remainder Theorem (CRT) secret key sharing algorithm. Every generated share (Share-1, Share-2, …, Share-n) is securely communicated to different mobile agents or platforms, ensuring that no individual secret share reveals any information about the original secret key. At the time of reconstruction phase only an authorized subset of shares satisfying the dynamic threshold requirement. These valid shares are authenticated by the lattice-based authentication techniques and then synchronized using the CRT reconstruction algorithm to gain the original secret key accurately. The dynamic threshold mechanism enables the minimum number of required shares to be adjusted according to the security level of the current transaction without regenerating the original secret key. Framework increases confidentiality, integrity, fault tolerance and resistance against attacks while providing efficient secret key recovery in decentralized mobile agent environment.

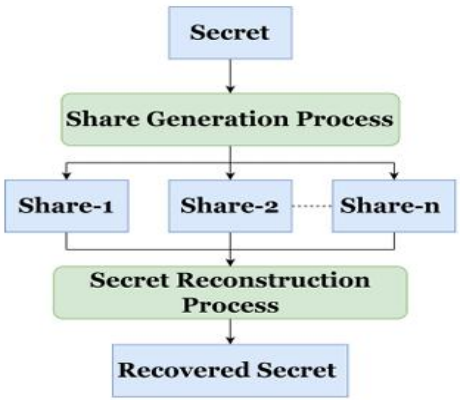


Fig. 4. General Architecture of Single secret share machine

Algorithm1: Initialization

In the initialization step fix the parameter and environment for secure secret sharing

i. Choose n different prime number $\{q_1,q_2,q_3, \dots \dots \dots . q_n,\}$ in such a way $\prod_{i=1}^{n} q_i > S$
ii. Threshold $t = minimum\ number\ of\ share\ required\ for\ construction\ of\ secret.$
iii. Select $L\ whose\ basis\ B\ derived\ from\ \{q_1,q_2,q_3, \dots \dots \dots . q_n,\}$ Lattice cryptography guarantees that it is computationally difficult to extract the secret without valid shares.

3.1. Lattice Basis Construction and Encoding:

Let q be a prime number and n shows the lattice dimension. A rank lattice basis matrix B,

$$\boldsymbol{B} = \left[b_{ij}\right]_{n*n} \in Z_q^{n*n}$$

where every value b_{ij} is chosen uniformly at random from Z_q. The security of the proposed framework is based on the Ring Learning with Errors (RLWE) assumption.

The original secret S is divided into n shares using the Chinese Remainder Theorem (CRT) shown in Eq. (1):

$$S_i = S\ mod\ q_i \ \ i = 1,2,3,4 \dots \dots . . n \tag{1}$$

Where $m_1, m_2, m_3 \dots \dots \dots \dots . . m_n$ are pairwise coprime integer satisfying shown in Eq. (2)

$$\gcd\left(q_i,q_j\right) = 1 \ \ i \neq j \tag{2}$$

Every share is encoded using lattice-based cryptography before transmission. The error vector is shown in Eq. (3)

$$e_i \sim D_\sigma \tag{3}$$

is sampled from a discrete Gaussian distribution with standard deviation σ. The encoded share is evaluated as shown in Eq. (4)

$$C_i = BS_i + e_i(mod\ n) \tag{4}$$

Where C_i represents the protected share transmitted to the corresponding mobile agent. The random error vector ensures semantic security, while the lattice basis matrix prevents unauthorized recovery of the secret share.

Algorithm2: Secret Share creation and lattice coding

Input: *Secret and lattice-based matrix B modulo q pairwise coprime number* $\{q_1, q_2, q \dots \dots \dots \dots q_n\}$
Output: Encoded shares $\{C_1, C_2, C_3 \dots \dots \dots \dots C_n\}$

i. Choose a secret $\boldsymbol{S}$ $such\ that\ \ 0 \leq S < \prod_{i=1}^{n} q_i$ *Secret only recovers under modulo arithmetic.*
ii. Create share of secret $\boldsymbol{S}$= $\{s_i\ ,\ s_1\ , s_2, s_3 \dots \dots \dots s_t\}$

$$s_i = S\ mod\ q_i, \qquad \forall i \epsilon \{1,2,3 \dots . t\}$$

Generate gaussian error vector

$$e_i \leftarrow D_\sigma$$

iii. Lattice encoding maps each share into a vector using the base matrix B

$$C_i = BS_i + e_i (mod\ n)$$

iv. Each mobile agent receives secretly share C_i

Algorithm 3: Secret Reconstruction

Secret can be recovered by using t or more than t shares
i. Choose a subset of mobile agents who will participate in the reconstruction of the secret share $\tau \subseteq \{1,2,3,4 \dots \dots n\}$
ii. Decode valid share $S_i = B^{-1}(C_i - e_i) mod\ q$
iii. Using share of secret $\{s_i\}_{i \epsilon\ \tau}$ *and module* $\{q_i\}_{i \epsilon\ \tau}$ *with CRT reconstruct secret*

$$S = \left(\sum\nolimits_{i \epsilon\ \tau} s_i * Q_i * {Q_i}^{-1} mod\ q_i \right) mod\ Q$$

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

iv. Lattice verification if $\boldsymbol{C'} = \boldsymbol{s'}.\boldsymbol{B}$ *then valid secret otherwise invalid secret.*

Algorithm 4: Dynamic adjustment of threshold

i. Threshold is dynamically adjustable to enhance the flexibility without regenerating secret
ii. Dynamically select $t'\ with\ modulo\ \{q'_1, q'_2, q'_3, q'_4 \dots \dots . q'_n\}$
iii. Recomputed shares $s'_i = S\ mod q'_i, \forall i \epsilon \{1,2,3 \dots . t'\}$ *also update lattice matrix* B'

This framework incorporates Dynamic Threshold Secret Sharing using the Chinese Remainder Theorem (CRT) to guarantee a high degree of security and flexibility while utilizing the resilience of lattice-based approaches. Dynamic threshold approaches address the diverse levels of danger involved with mobile agent migration by providing the flexibility to modify the threshold for secret reconstruction according to the security requirements of various contexts.

4. Implementation and Results

The proposed lattice-based variable threshold CRT secret sharing framework was implemented in Python 3.11 to analyze its effectiveness for securing mobile agent migration. Implementation used PyCryptodome for cryptographic primitives, SymPy for modular arithmetic and CRT operations, fpylll for lattice-based computations and NumPy for numerical execution. The implementation was executed in a simulated distributed environment having a trusted home platform and multiple platforms, with the number of mobile agents varying from 10 to 1000. Each mobile agent executed a specified computational task and communicated over the same simulated network conditions to ensure a fair analysis. Proposed framework was evaluated against Shamir Secret Sharing, Integer CRT, Homomorphic Encryption, Vectorized Tree Parity Machine (VTPM), and Boneh Goh Nissim (BGN) techniques under same implementation setup, security parameters and threshold configurations. Performance was analyzed using turnaround time, memory utilization, CPU

efficiency, communication overhead and scalability. To improve reproducibility all experiments were executed under the same hardware and software environment and each experiment was repeated multiple times to minimize the effect of random variations. The outcome represents the average performance obtained from the experiments.

In this system, the secret is split into multiple shares using CRT, and lattice-based methods are employed to securely encode the shares, offering resistance to quantum computing attacks. After the implementation, the proposed framework is analyzed for 'n' number of mobile agents. Number of mobiles varies from 10 to 1000 mobile agents. Proposed framework utilizes four different algorithm initialization, secret creation, secret reconstruction and Dynamic adjustment of threshold. During the analysis, the proposed framework is compared with similar techniques: Vectorized Tree Parity Machine, homomorphic encryption, Shamir Secret Sharing, Integer CRT, and Boneh-Goh-Nissim. Among all lattice-based is optimal approach in terms of turnaround time of secret creation, and regeneration with dynamic threshold. Comparison of all techniques is shown in Fig. 5.

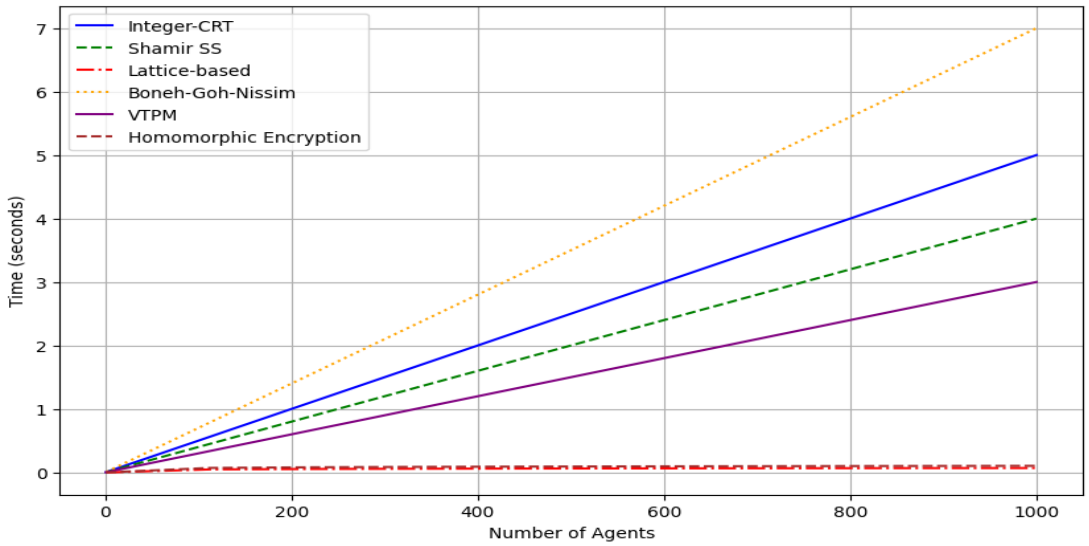


Fig. 5. Comparison of proposed framework with different similar techniques

Three other parameters are considered for comparison among all techniques with the proposed one. The three parameters are scalability, memory utilization and CPU efficiency. The comparison is shown in Fig. 6.

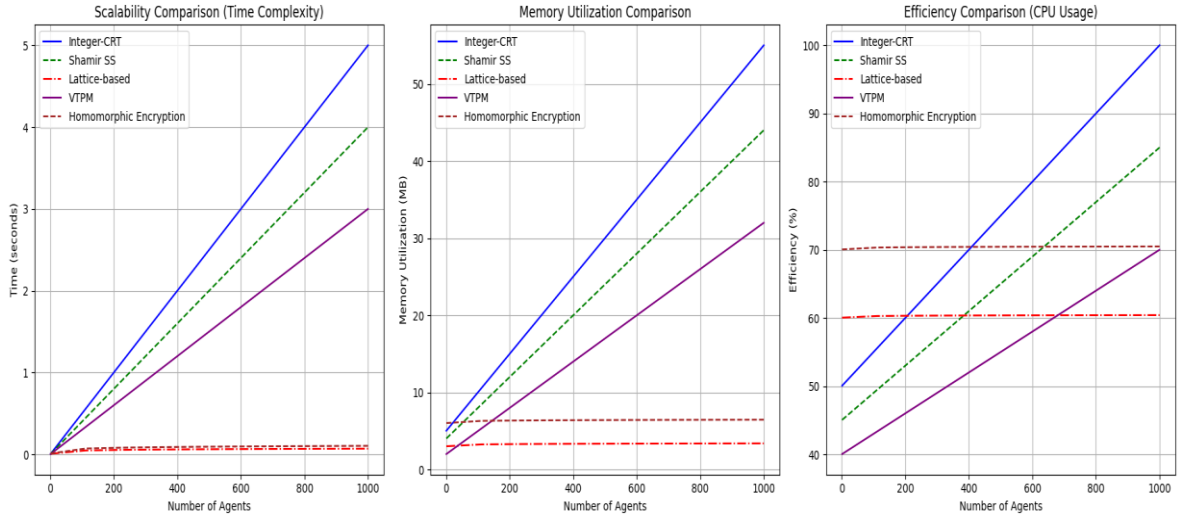


Fig. 6. Comparison on the basis of Scalability, Memory utilization and CPU efficiency.

The proposed framework is compared with existing secret sharing and cryptographic approaches under 1000 mobile agents. The proposed lattice-based dynamic threshold CRT framework gains the least turnaround time (0.10 second) and the best scalability (0.10 second execution time), showing that its execution time increases only marginally as the number of mobile agents increases. It also needs the least memory (3.5 MB) while maintaining a CPU efficiency of 60.5%, reflecting fast resource utilization. In the analysis, Integer CRT exhibits the highest execution time (5.0 s) and memory utilization (55 MB), followed by Shamir Secret Sharing and VTPM. Although Homomorphic Encryption shows

comparable execution time, it takes more memory than the proposed framework. Overall, outcome shows that integrating lattice-based cryptography with dynamic threshold CRT significantly improves scalability and computational efficiency while providing secure and post-quantum-resistant mobile agent migration.

5. Conclusion and future Scope

This paper proposes a lattice-based dynamic threshold CRT secret sharing framework to increase the security of mobile agent migration in decentralized and malicious networks. The proposed framework combines lattice-based cryptography with variable threshold secret key sharing to improve the confidentiality, integrity and authentication of mobile agents while maintaining fast secret key reconstruction. Experimental evaluation with 10 to 1000 mobile agents shows that the proposed framework gains a turnaround time of 0.10 second, memory utilization of 3.5 MB and CPU efficiency of 60.5% under 1000 mobile agents, outperforming Integer CRT, Shamir Secret Sharing, Vectorized Tree Parity Machine (VTPM), Homomorphic Encryption and Boneh Goh Nissim (BGN) techniques in terms of turnaround time, scalability and resource utilization under the specific conditions. Although these outcomes show the effectiveness of the proposed framework in a simulated environment, further investigation is needed to analyze communication overhead during frequent threshold variation, synchronization latency in large-scale distributed systems and resilience against malicious node collusion and network partitioning. Future work will focus on further optimizing the framework for resource-constrained environments and integrating it with other security mechanisms such as machine learning-based anomaly detection to enhance the system's robustness against emerging threats.

All the Declarations and Statements

Author Contributions Statement

Pradeep Kumar: Conceptualization, Methodology, Investigation, Formal Analysis, Supervision, and Writing Original Draft. Proposed the research concept, designed the lattice-enhanced dynamic threshold CRT-based framework, supervised the research, and prepared the initial manuscript.
Kakoli Banerjee: Data Curation, Software, Validation, and Investigation. Implemented the proposed framework, conducted experiments, managed data preparation, and validated the experimental results.
Bijendra Tyagi: Formal Analysis, Visualization, and Performance Evaluation. Performed comparative analysis, evaluated the proposed method using performance metrics, prepared figures and tables, and interpreted the experimental results.
Anuradha Singh: Methodology, Writing Review & Editing, and Literature Review. Contributed to the methodological development, reviewed the related literature, critically revised the manuscript, and improved its technical quality and presentation.
Priyank Sirohi: Project Administration, Resources, Writing Review & Editing, and Supervision. Assisted in project coordination, reviewed and edited the manuscript, verified the technical content, and supervised the overall progress of the research.

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

None

Data Availability Statement

This study used self-generated dataset.

Ethical Declarations

This study does not involve human participants, human data, human tissues, or animals. Therefore, ethical approval and informed consent were not required.

Acknowledgments

The authors sincerely thank the reviewers and editors for their constructive comments and valuable suggestions, which significantly improved the quality, clarity, and technical presentation of this manuscript. The authors also acknowledge the support provided by JSS University, Noida, for facilitating the research activities and computational resources used in this work.

Declaration of Generative AI in Scholarly Writing

Authors should disclose in their article how AI and AI-assisted technologies were used during the writing process.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Full Form
AI	Artificial Intelligence
BGN	Boneh–Goh–Nissim
CRT	Chinese Remainder Theorem
CPU	Central Processing Unit
DL	Deep Learning
HP	Home Platform
IoT	Internet of Things
MA	Mobile Agent
MB	Megabyte
NLP	Natural Language Processing
RLWE	Ring Learning with Errors
SOTA	State-of-the-Art
VTPM	Vectorized Tree Parity Machine
VSS	Verifiable Secret Sharing

Appendix A/B/C…, with appendix title

None

References

[1] Chen J, Deng H, Su H, Yuan M, Ren Y. Lattice-Based Threshold Secret Sharing Scheme and Its Applications: A Survey. *Electronics*. 2024; 13(2):287. https://doi.org/10.3390/electronics13020287.

[2] P. Kumar et al., “Verifiable, Secure Mobile Agent Migration in Healthcare Systems Using a Polynomial-Based Threshold Secret Sharing Scheme with a Blowfish Algorithm,” Sensors, vol. 22, no. 22, 2022, doi: 10.3390/s22228620.

[3] Damgård, I., Orlandi, C., Takahashi, A. *et al.* Two-Round *n*-out-of-*n* and Multi-Signatures and Trapdoor Commitment from Lattices. *J Cryptol* **35**, 14 (2022). https://doi.org/10.1007/s00145-022-09425-3

[4] J. S. Kim, K. Lee, J. Hwan Park and H. Kim, "Dynamic Threshold Key Encapsulation With Transparent Setup," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8433-8448, 2025, doi: 10.1109/TIFS.2025.3595667

[5] G. Li, H. Luo, J. Yu, A. Hu and J. Wang, "Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications," in *IEEE Wireless Communications*, vol. 31, no. 1, pp. 118-124, February 2024, doi: 10.1109/MWC.012.2200289.

[6] P. Kumar, N. Singhal, D. Pandey, and A. Vatsa, “Secure Mobile Agent Migration Using Lagrange Interpolation and Fast Fourier Transformation,” Int. J. Comput. Netw. Inf. Secur., vol. 15, no. 4, pp. 72–83, 2023, doi: 10.5815/ijcnis.2023.04.07.

[7] P. Bagga and R. Hans, “Mobile Agents System Security,” ACM Comput. Surv., vol. 50, no. 5, pp. 1–45, 2017, doi: 10.1145/3095797.

[8] L. Li, Y. Lu, L. Liu, Y. Sun, and J. Wang, “Practical Secret Image Sharing Based on the Chinese Remainder Theorem,” Mathematics, vol. 10, no. 12, pp. 1–18, 2022, doi: 10.3390/math10121959.

[9] K. Meng, F. Miao, Y. Ning, W. Huang, Y. Xiong, and C. C. Chang, “A proactive secret sharing scheme based on Chinese remainder theorem,” Front. Comput. Sci., vol. 15, no. 2, 2021, doi: 10.1007/s11704-019-9123-z.

[10] D. Pande, A. S. Rawat, M. Deshmukh, and M. Singh, “Single Secret Sharing Scheme Using Chinese Remainder Theorem, Modified Shamir’s Scheme and XOR Operation,” Wirel. Pers. Commun., vol. 130, no. 2, pp. 957–985, 2023, doi: 10.1007/s11277-023-10315-5.

[11] J. Chen, K. Liu, X. Yan, L. Liu, X. Zhou, and L. Tan, “Chinese remainder theorem-based secret image sharing with small-sized shadow images,” Symmetry (Basel)., vol. 10, no. 8, 2018, doi: 10.3390/sym10080340.

[12] K. Shehata, H. Fangqi and S. A. Thyagarajan, "Verifiable Weighted Secret Sharing," *2025 Crypto Valley Conference (CVC)*, Rotkreuz, Switzerland, 2025, pp. 86-101, doi: 10.1109/CVC65719.2025.00017.

[13] Y. H. Liu and R. J. Chen, “An asymptotically perfect secret sharing scheme based on the Chinese Remainder Theorem,” Int. J. Comput. Math., vol. 94, no. 9, pp. 1890–1915, 2017, doi: 10.1080/00207160.2016.1274738.

[14] X. Jia, Y. Song, D. Wang, D. Nie, and J. Wu, “A collaborative secret sharing scheme based on the Chinese Remainder Theorem,” Math. Biosci. Eng., vol. 16, no. 3, pp. 1280–1299, 2019, doi: 10.3934/mbe.2019062.

[15] L. Harn, C. Hsu, and Z. Xia, “A novel threshold changeable secret sharing scheme,” Front. Comput. Sci., vol. 16, no. 1, pp. 1–7,

2022, doi: 10.1007/s11704-020-0300-x.
[16] R. Kumar and S. Padhye, "A Lattice-Based Single-Share Secret Sharing Scheme," SN Comput. Sci., vol. 4, no. 6, 2023, doi: 10.1007/s42979-023-02274-2.
[17] B. Huang, J. Gao, and X. Li, "Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing," J. Cloud Comput., vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00414-w.
[18] Liu-Zhang, CD., Masserova, E., Ribeiro, J., Soni, P., Thyagarajan, S.A. (2025). Efficient Distributed Randomness Generation from Minimal Assumptions Where PArties Speak Sequentially Once. In: Fehr, S., Fouque, PA. (eds) Advances in Cryptology – EUROCRYPT 2025. EUROCRYPT 2025. Lecture Notes in Computer Science, vol 15605. Springer, Cham. https://doi.org/10.1007/978-3-031-91092-0_7.

Authors' Profiles



Pradeep kumar is Ph.D. (Computer engineering 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.



Dr. Kakoli Banerjee is Associate Professor (Computer Science and Engineering Department), JSS Academy of Technical Education, Noida. She graduated from IET, Kanpur – B.Tech (CSE), did her Post Graduation from MNNIT, Allahabad – M.Tech (CSE) and Doctorate (Ph.D) from Shobhit University, Saharanpur. She has 22 years of experience in academics and in industry. She has published around 45 research papers in international journals of repute indexed in SCI, Scopus, ESCI, Google Scholar, and other eminent databases. Currently, she is working for a funded project, sanctioned by the Collaborative Research and Innovation Program (CRIP) under TEQIP- 3 by Dr. A. P. J. Abdul, Kalam Technical University Uttar Pradesh, Lucknow. She is a member of IEEE and other professional societies such as ISTE, CSI, etc. She has been a reviewer and guest editor of several reputed journals and books. She has also served in many conferences as session chair. She has two Granted Patent to my name and eight published. She has developed video content for Dr. A.P.J. Abdul Kalam Technical University, Lucknow and Swayam Prabha Chanel of Government of India for subjects like Operating System and Database Management System. She has published book - & quot; Industry 4.0: Research Trends, Challenges and Future of AI in Data Science & quot;, CRC Press, Taylor & Francis Group and & quot; Decision Analytics for Sustainable Development in Smart Society 5.0", Springer Nature.



Bijendra Tyagi is an Assistant Professor at JSS Academy of Technical Education, Noida. He received his B.Tech degree in Computer Science and Engineering from Uttar Pradesh Technical University in 2011, Master of Technology degree in Information Technology from Guru Gobind Singh Indraprastha University, Delhi in 2014. He has more than 10 years of academic and teaching experience. With a passion for Artificial intelligence, Machine Learning, Cloud computing and Security, he has contributed significantly to the field through various publications. In addition to research, he is actively involved in mentorship, aiming to inspire next generation of scientists.



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



Priyank Sirohi is a Ph.D. student of computer engineering and engineering at Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut, 250110. He obtained his M.Tech. in Computer Science and Engineering Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), with first class. He obtained his B.Tech degree in Information Technology engineering from RGEC Meerut *college of UPTU,* India in 2006 with first class. Presently he is working as Assistant Professor in the department of Information Technology at Sir Chhotu Ram Institute of Engineering & Technology, Chaudhary Charan Singh University, Meerut

How to cite this paper

Priyank Sirohi, Kakoli Banergee, Bijendra Tyagi, Anuradha Singh, Pradeep Kumar, "A Lattice-Enhanced Dynamic Threshold CRT-Based Secret Sharing for Mobile Agent Security in Decentralized Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.5, pp. 145-157, 2026. DOI:10.5815/ijwmt.2026.05.09