Mobile Agent Security Using Multilevel Secret Sharing with Changeable Threshold Based on Chinese Remainder Theorem

Mohammad Asim* and Anil Kumar Sagar

Department of Computer Science and Engineering, Sharda University Greater Noida, India
E-mail: er.mohdasim@gmail.com; aksagar22@gmail.com
**Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

Abstract

A novel computational technique known as mobile agent technology, just a little piece of code travels from one place to another. This code can migrate to another computer on the network that has agent functionality enabled and carry out the assigned task there. It is necessary to shield these agents from several risks and weaknesses both during their execution and travel in order to ensure their security. Based on the Chinese remainder theorem, the suggested approach involves multilevel secret sharing with a threshold that may be changed to secure mobile agents. One important aspect of this technique is that shareholders are arranged in a hierarchical or multilayer framework, with each owner requiring only one hidden private share because it will enable us to have smaller share sizes, making the process of transferring them easier and the complexity of recovery lower. This is a sample input file. Comparing it with the output it generates can show you how to produce a simple document of your own.

Keywords: Mobile agents, secret share, threshold cryptography, modular arithmetic, chinese remainder theorem.

Journal of Mobile Multimedia, Vol. 21_3&4, 521–534.
doi: 10.13052/jmm1550-4646.213411

1 Introduction

Internet Mobile agents represent a unique paradigm in computing where software entities, termed agents, possess the ability to move autonomously across distributed and heterogeneous environments, executing tasks on behalf of users or applications. Unlike traditional programs that remain static on a single machine, mobile agents can migrate from one system to another, carrying their code, data, and state with them. The concept of mobile agents emerged from the need for efficient and flexible solutions in distributed computing, enabling decentralized and autonomous execution of tasks. These agents act as independent entities, capable of initiating actions, making decisions, and interacting with other agents or resources in the network.

1.1 Issue of Mobile Agents

The correspondence medium is intrinsically unreliable and the various agents and agent frameworks might have clashing destinations. In this situation, an assortment of assaults can be imagined. Unapproved clients might listen in network traffic and notice agents in real life, or more awful a functioning active intruder might alter the code, information or condition of an agent on the way Agents might assault the agent stage (have) supporting their execution to acquire unapproved access [1] to assets. Note that a portion of these issues is ordinary in traditional conveyed (client/server) frameworks and are settled by cryptographic methods.

2 Literature Review

A literature survey on mobile agent security would involve an extensive review and analysis of existing research, publications, and studies concerning

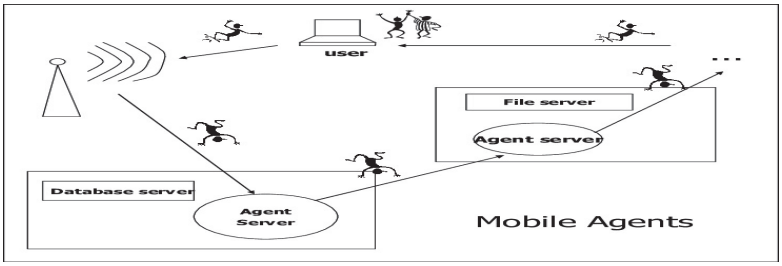

Figure 1 Mobile agent model.

the security aspects of mobile agents. Here's a structured approach to conduct such a survey:

Shamir and Blakley [2] Threshold secret sharing (SS) was presented, an A(t, n) threshold SS consist of following these stages: share generation(formation of the secret) and secret reconstruction(forming the actual text back from the pieces of secret). The vendor or the dealer is accountable for partitioning a secret allowing it to be 's' into 'n' shares and dispersing each offer to the relating shareholder safely during the share generation stage. In the secret reconstruction phase, 't' or more than 't' shareholders are permitted to recuperate the secret 's' by pooling shares together while not as much as 't' shareholders can't acquire 's'.

Lein Harn et al. [3] proposed another threshold secret sharing scheme in which all shareholders have different responsibility; while in a classical threshold SS, all holders have the only responsibility. In the multilevel threshold secret scheme, when there are essentially ti shareholders place with levels more than or similar, to a level Li, than that part of shareholders can recreate a secret.

Brickell [4] given optimal MTSS but, this concept given by him is not good enough because the dealer is necessary to figure rapidly to make certain outlandish frameworks.

Boudotet et al. [5] The CRT are well known techniques tools utilized for planning a SSs. Mignotte's and Asmuth's schemes are traditional (t, n) threshold SSs and Kaya called that both schemes together can't check a ruined trader from distributing conflicting shares to the shareholders. They also given a CRT-based VSS in which utilizes the reach verification method proposed. protection of all their VSS have support with the RSA presumption.

Jianjie Zhao et al. [6] presents a VMSS (confirmable collective secret sharing) build on YCH strategy and an ungovernable of a distinct logarithm. The paper focuses on multi or collective secrets sharing (MSS) and its secure reconstruction. In the VMSS they increased the verification algorithm and computational quality. Each participant/share can use their own secret shadow therefore the organization doesn't need a protection passage and the prize of the organization can be go-down. This method used in the empirical terms.

Om Prakash Verma et al. [7] In this paper in order to achieve more security and reliability and to dodge dishonest by any of the owners, the has to demonstrable secret sharing (VSS) has emerged. In this respect, a cross breed targeted for VSS strategic is proposes. In this scheme multiple secrets are shared among owners, where owners are also separated into dissimilar layers.

Hence it prevents typical untruthful strategic of dripping secret information in the different legal share.

Pallavi bagga et al. [8] the paper comprises of a precise methodology where it brings up every one of the common assaults on the portable agents and the agent stages, it is recorded down in the space of MAS security, the current restorative measures and their checks, calls attention to various security necessity and a portion of the examinations focus around cryptographic framework and exemplification to guarantee secretiveness and hashing strategies to certify system. In the end it addresses the future security challenges.

Pradeep et al. [9] suggested model, which is predicated on two authentication systems with polynomials. Here, a patient's information was encoded by the authors using the blowfish algorithm. Blowfish employs symmetric cryptography, wherein documents must be encrypted and decrypted using a secret key that is generated and verified through the use of two polynomial-based processes.

Samet et al. [10] suggested security framework was successful in identifying the simulated attacks and eliminating the malicious agents. This fact is meant to demonstrate the practical use of the security framework and the suggested security approach to safe mobile agent networks.

3 The Problem Definition

In distributed computing the major concern is mobile agent security during the migration in a malicious Heterogeneous environment. Mobile agents encounter various security concerns, such as platform vulnerabilities, integrity attacks, data confidentiality breaches, and authentication problems. For instance, by inserting malicious code into vulnerable agent platforms, attackers might alter an agent's execution state, intercept private data during agent migration, or take advantage of these vulnerabilities. Both the integrity of the agent and the security of the systems it interacts with are jeopardized by these attacks.

A solution to these problems is Multilevel Secret Sharing with Changeable Threshold using the Chinese Remainder Theorem (CRT), which divides sensitive data among several platforms and makes sure it can only be reconstructed when enough reliable platforms work together. This approach for adaptive thresholds improves security by dynamically modifying the degree of protection needed at various points throughout the agent's migration.

4 Preliminaries

In this part, we present a few preliminaries that are the essentials in our plan together with an explanation of MTSS, the CRT (Chinese Remainder Theorem), Mignotte's and Asmuth's-Bloom plans in view of the CRT.

4.1 Secret Sharing Scheme (SSS)

A Secret Sharing Scheme (SSS) is a cryptographic method that involves dividing a secret into multiple parts or shares and distributing these shares among different entities or participants in such a way that only a predefined subset of shares can reconstruct the original secret.

4.2 The Chinese Remainder Theorem (CRT)

The Chinese Remainder Theorem (CRT) is a fundamental theorem in number theory and modular arithmetic. It provides a method for solving systems of simultaneous congruencies, allowing computations to be performed more efficiently. The theorem is named after the ancient Chinese mathematician Sun Tzu (or Sunzi), but it was independently discovered and formalized by multiple mathematicians across different cultures. Given a system of congruence of the form:

$$\begin{aligned} \mathrm{x} &\equiv \mathrm{a1}(\mathrm{modm1}) \\ \mathrm{x} &\equiv \mathrm{a2}(\mathrm{modm2}) \\ \mathrm{x} &\equiv \mathrm{an}(\mathrm{modmn}) \end{aligned}$$

Where m1,m2,...,mn are pairwise coprime (i.e., their greatest common divisor is 1), and a1,a2,...,an are integers. he CRT states that this system of congruences has a unique solution modulo

a. Compute M=m1$\times$m2$\times\cdots\times$mn.
b. Compute Mi=M/mi for each i.
c. Find yi for each i such that Mi$\times$yi$\equiv$1(modmi) using modular multiplicative inverses (often calculated using the extended Euclidean algorithm).
d. The solution x is given by x=a1$\times$M1$\times$y1+a2$\times$M2$\times$y2+$\cdots$+an$\times$Mn$\times$yn mod M.

5 Proposed Methodology

The following methods are part of the recommended strategy for protecting mobile agents employing Multilevel Secret Sharing with a Changeable

Threshold based on the Chinese Remainder Theorem (CRT):

i. Utilizing CRT, the secret key is divided into several shares, each of which is allocated to participants with varying levels of access (U1, U2, U3 . . . , Un);
ii. A dynamic threshold (t1, t2, t3. . . tn.) is assigned to each level, signifying the bare minimum of participants needed to reconstruct the secret.
iii. In order to reach their access level threshold for secret the reconstruction, participants work together during agent migration.
iv. Dynamically adjusting thresholds allows for flexible access control in response to changing security requirements.
v. The accuracy of the rebuilt secret is guaranteed by a public verification system that keeps it hidden. Adaptive thresholding and effective secret sharing are combined in this method to improve mobile agent security in heterogeneous situations.

In the context of mobile agent security, Figure 2 illustrates the Multilevel Secret Sharing with Changeable Threshold procedure utilizing the Chinese Remainder Theorem (CRT). There are two primary phases to it: Phases of Secret Creation and Secret Reconstruction on Two Platforms.

1. Platform 1's Secret Generation Phase:

Key/Secret: Platform1 is where the initial secret or key is generated. Using the Chinese Remainder Theorem (CRT), the secret is divided into several shares, S1, S2, S3,. . . , Sn.

The secret is divided among mobile agents A1, A2... An. Each share, S1, S2,. . . ,Sn, is assigned a piece of the secret.

Mobile Agents: These shares must be safely transferred to Platform 2 by agents A1, A2,..., An.

2. Platform 2's Secret Reconstruction Phase:

The agents A1, A2,. . . , An deliver their individual shares to Platform 2.

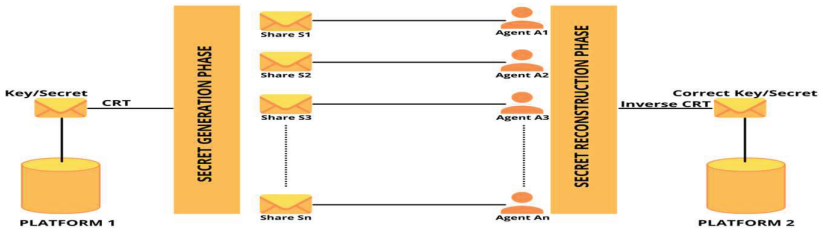

Figure 2 Proposed model based on CRT.

Reconstruction through Inverse CRT: On Platform 2, the original key or secret is reconstructed by combining the received shares using the Inverse CRT.

Correct Key/Secret: On Platform 2, the original key/secret is recovered once the shares have been merged.

As shown in the Figure 2 we are transferring a key from platform 1 to platform 2 and during the time of transferring when the key started to move from platform one it is encrypted and distributed into n number of unique shares which are relatively co-prime to each other and now these cipher text blocks are transferred from platform 1 to n different shareholders at platform 2 simultaneously. Numerically or in a mathematical way, if Ui, i = 1, 2,. . . , n, where U1 is the most elevated level (highest level) of parts and Um is the least (lowest level). share belonging to every subset, Ui, has a threshold, 'x'. Shares having a place with the subset, Ui, or any other part with cutting edge security's position than the part, Ui, may be utilized to recuperate the secrets, if the quantity of shares accessible is equivalent to or farther apart the thresholds, 'x'. The limit of a high-level position part is consistently lower to the thresholds of a ground-position part. In the secret rebuilding by share in the parts, Ui, and in any part of the cutting-edge security position, its requirements to full fill the resulting circumstances.

(1) The secrets can be recreated assuming the no. of share from the shareholders are greater than equal to x
(2) The secret can't be recreated once the no. of correct share from the shareholders are lesser than x. The planned model comprises of dual stages: a shared formation that is the generation phase or distribution of one secret into n number of secrets and secret reconstruction in which those n secrets or a part of it is combined to form the actual or initial secret. Hence bypassing a decryption mechanism our correct secret will be generated at the platform 2 end. Platform 1 and platform 2 can be basically two different machines within the same network or they can be two machines present in two different networks [11].

6 Implementation and Results

In Table 1 we have taken the value of the Reputation-based Model, Trust Scoring system, trust ranking system and multilevel security using CRT. The values of multilevel security using CRT have been derived from the GUI, as we just have to put some value and we can easily get response time

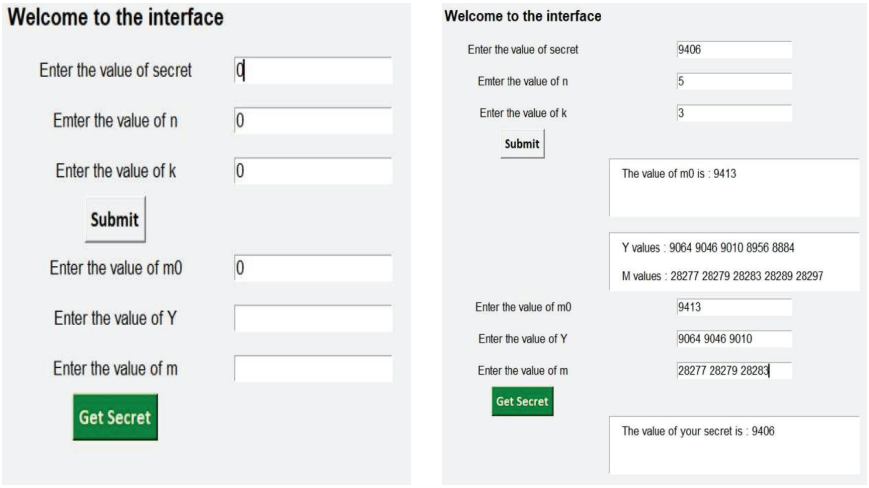

Figure 3 (a) GUI to Generate Secret Key. (b) Getting Secret key with help of GUI.

Table 1 Comparison of response time among reputation-based model, trust scoring system, and trust scoring system and multilevel security model

		Response Time in Seconds			
S.No	No of Mobile Agents	Reputation-based Model	Trust Scoring System	Trust Ranking System	Multilevel Security Using CRT
1	5	0.47	0.35	0.17	0.22
2	10	0.94	0.69	0.35	0.31
3	15	1.37	1.06	0.52	0.47
4	20	1.95	1.42	0.72	0.81
5	25	2.29	1.84	0.94	0.85
6	30	2.86	2.16	1.3	0.99
7	35	3.45	2.49	1.3	1.25
8	40	3.85	2.86	1.5	2.12
9	45	4.37	3.26	1.8	2.14
10	50	4.78	3.53	1.75	2.28
11	55	5.24	3.88	1.94	2.39
12	60	5.98	4.35	2.19	2.48
13	65	6.25	4.65	2.36	2.74
14	70	6.67	5.03	2.7	2.76
15	75	7.1	5.33	2.64	2.94
16	80	7.68	5.75	2.87	3.19

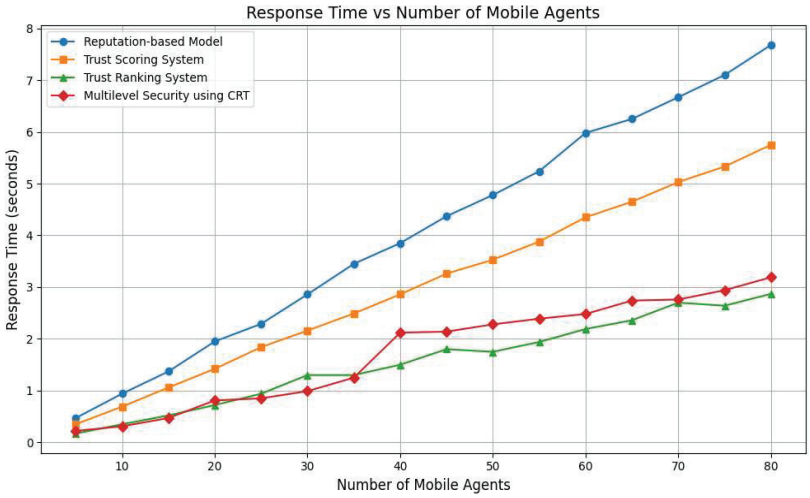

Figure 4 Number of mobile agent w.r.t response time graph of Multilevel security using CRT.

and we already know the value of the number of devices. And other values like Trust Scoring System are those values which are base values and from these values we get to know whether we stand somewhere near the ideal values or not. We have taken multiple data points as it allows us to better estimate the uncertainty in our calculations by checking how reproducible the measurements are. In order to get a better average value for the whole range we have gathered the data for different data values or for different numbers multiple times. The response time graph for the table 1 on the basis of various factors. Figure 4 graph shows how the reaction times for four security models – Multilevel Security utilizing CRT, Trust Scoring System, Trust Ranking System, and Reputation-based Model change as the number of mobile agents rises. The graph demonstrates that the Reputation-based Model has the worst reaction time, increasing from 0.47 seconds (5 agents) to 7.68 seconds (80 agents), and that it scales poorly as the number of mobile agents rises. The Trust Scoring System scales inefficiently and performs marginally better, taking 5.75 seconds at 80 agents. Multilevel Security employing CRT and the Trust Ranking System, on the other hand, provide significantly faster reaction times, with the Trust Ranking System continuing to perform better when there are more agents.

The CRT-based Multilevel Security is especially effective for small to medium-sized agent systems; however, after 35 agents, the reaction time

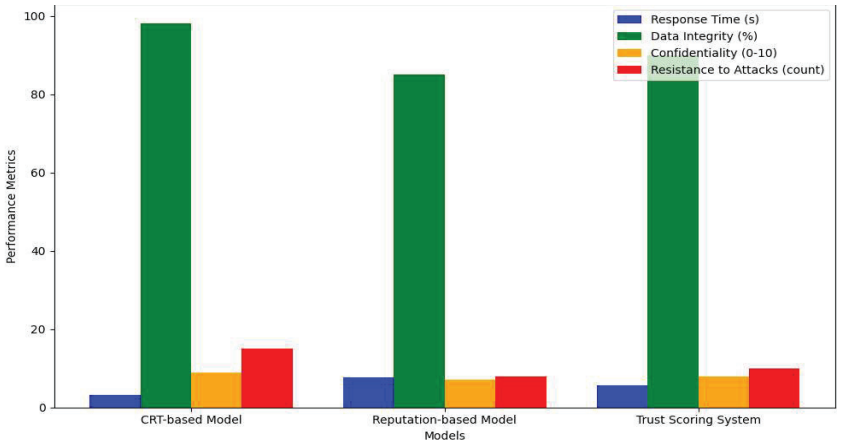

Figure 5 Comparison of mobile agent security model.

becomes more pronounced, reaching 3.19 seconds for 80 agents. The Trust Ranking System is the most scalable overall, but for smaller deployments, the CRT-based model manages to balance security and performance well.

Here also compare the proposed model with other parameter response time, data integrity confidentiality and resistance to attack. Figure 5 shows the comparison between the models' strengths and weaknesses in terms of several crucial mobile agent security criteria will be made evident through this graphical representation.

7 Conclusion and Future Scope

We proposed the Mobile Agent Security utilizing multi-level Secret Sharing with Changeable Threshold utilizing Chinese Remainder Theorem and an encoding technique that use in the Chinese Remainder Theorem and hash map to produce and allocate secret co-prime key to owners. The secret might get recuperated when adequate number of shares is accessible. Shareholders are arranged in a multi-levelled or a ranking levelled system and furthermore, Threshold Changeable Secret Sharing is being applied as it will assist us with having more modest share measures so transferring them will be a simple or easy task and lower recuperation intricacy or complexity the Multilevel Thresholds Secrets Sharing, any shares in the more raised level i.e., the one belonging to a high close of subset can be shares at the ground-close of subset to reclaim the secret at one exceptional part of our

planned multi-leveled changeable threshold-based secret sharing are those shareholders keep just single secret shares. This proposed secret sharing plan can be utilized in any environment. The assessment of mobile agent security through the use of Multilevel Secret Sharing with Changeable Threshold, which is grounded in the Chinese Remainder Theorem (CRT), indicates a notable improvement in response time while dealing with different quantities of mobile agents. According to performance statistics, the suggested CRT method's response time varies from 0.22 to 3.19 seconds as the number of mobile agents rises from 5 to 80, showing a comparatively steady increase in efficiency. When compared to other models, the multilevel security method consistently performs better. For example, the Reputation-based Model, Trust Scoring System, and Trust Ranking System have reaction times of 0.47 to 7.68 seconds, 0.35 to 5.75 seconds, and 0.17 to 2.87 seconds, respectively. Interestingly, the CRT-based approach keeps response time growth rates lower, indicating that it is more scalable and effective for secure mobile agent operations, guaranteeing improved data confidentiality and integrity while supporting growing loads in dispersed systems. This study emphasizes how well CRT and Multilevel Secret Sharing work together to maximize mobile agent security in dynamic settings. Future research on mobile agent security will focus on creating adaptive security mechanisms that use machine learning to detect and respond to threats in real time, integrating blockchain technology to improve data integrity and trust, and creating interoperability standards for various security solutions. Furthermore, attention must be paid to developing quantum-resistant cryptographic protocols, designing user-centric frameworks that provide users more control over their data, and developing privacy-preserving methods for sensitive applications. Last but not least, continued work to improve security algorithm performance will guarantee that improved security measures do not impair the effectiveness of mobile agent operations in dynamic and diverse contexts.

References

[1] S. S. Srivastava and G. C. Nandi, "Self-reliant mobile code: A new direction of agent security," J. Netw. Comput. Appl., vol. 37, no. 1, pp. 62–75, 2014, doi: 10.1016/j.jnca.2013.01.004.

[2] V. Attasena, J. Darmont, and N. Harbi, "Secret sharing for cloud data security: a survey," VLDB J., vol. 26, no. 5, pp. 657–681, 2017, doi: 10.1007/s00778-017-0470-9.

[3] L. Harn and M. Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem," Inf. Process. Lett., vol. 114, no. 9, pp. 504–509, 2014, doi: 10.1016/j.ipl.2014.04.006.
[4] K. Meng, F. Miao, W. Huang, and Y. Xiong, "Tightly coupled multi-group threshold secret sharing based on Chinese Remainder Theorem," Discret. Appl. Math., vol. 268, pp. 152–163, 2019, doi: 10.1016/j.dam.2019.05.011.
[5] W. Jansen and T. Karygiannis, "NIST Special Publication 800-19 – Mobile Agent Security Computer," Nist Spec. Publ., vol. 323, no. September, pp. 3–10, 1999.
[6] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," Comput. Stand. Interfaces, vol. 29, no. 1, pp. 138–141, 2007, doi: 10.1016/j.csi.2006.02.004.
[7] O. P. Verma, N. Jain, and S. K. Pal, "A Hybrid-Based Verifiable Secret Sharing Scheme Using Chinese Remainder Theorem," Arab. J. Sci. Eng., vol. 45, no. 4, pp. 2395–2406, 2020, doi: 10.1007/s13369-019-03992-7.
[8] P. Bagga and R. Hans, "Mobile Agents System Security," ACM Comput. Surv., vol. 50, no. 5, pp. 1–45, 2017, doi: 10.1145/3095797.
[9] Kumar P, Banerjee K, Singhal N, Kumar A, Rani S, Kumar R, Lavinia CA. Verifiable, Secure Mobile Agent Migration in Healthcare Systems Using a Polynomial-Based Threshold Secret Sharing Scheme with a Blowfish Algorithm. Sensors. 2022; 22(22):8620. https://doi.org/10.3390/s22228620.
[10] Samet, D., Ktata, F.B. and Ghedira, K. A security framework for mobile agent systems. Autom Softw Eng 31, 12 (2024). https://doi.org/10.1007/s10515-023-00408-7.
[11] Chattopadhyay, T., Prasad, G. Mobile Agent Security Against Malicious Hosts: A Survey. SN COMPUT. SCI. 3, 160 (2022). https://doi.org/10.1007/s42979-021-01004-w.
[12] Kumar, P., Singhal, N. "An Optimized Authentication Mechanism for Mobile Agents by Using Machine Learning" I. J. Computer Network and Information Security, 2023, 6, 30–39, Volume 15 (2023), Issue 6, doi: 10.5815/ijcnis.2023.06.03.
[13] Kumar, P., Singhal, N. "An Enhanced Method Utilizing Hopfield Neural Model for Mobile Agent Protection", Volume 13 (2023), Issue 5, doi: 10.5815/ijwmt.2023.05.03.

Biographies

Mohammad Asim is presently working as Assistant Professor in the Department of Computer Science and Engineering at Sharda University. He has vast experience in teaching and research. He did M.Tech. (CSE) and B.Tech. (CSE) from Dr. APJ Abdul Kalam Technical University Lucknow and pursuing Ph.D. in Computer Science and Engineering. He has authored many research papers in conferences and journals of repute, indexed in Scopus/UGC care etc and have filled some patents also. His area of interest includes Information Security, Cryptography, Blockchain Technology and Distributed Computing.

Anil Kumar Sagar is a Professor in the Department of Computer Science Engineering at Sharda University, India. He holds a Ph.D. from JNU, New Delhi, and completed his B.E. and M.Tech in Computer Science. With 20 years of teaching experience, he has guided 10 M.Tech students and is currently supervising 5 Ph.D. scholars. He is actively involved in editorial boards, review committees, and organizing several national and international conferences. He has published several research papers in reputed journals like Scopus and SCI.