Multitiered Dynamic Threshold-Based Mobile Agents Secure Migration Using Lagrange Polynomial and Chinese Remainder Theorem

Niraj Singhal and Pradeep Kumar

Abstract A mobile agent is a software process that works repeatedly on the behalf of its owner. Mobile agents are an emerging computing area that replaces client–server computing model. Mobile agent processes different types of activities during its life cycle and executes code on another non-trusted host computer in a malicious heterogeneous environment. Because of the intelligence of mobile agents, they are being used in many applications like E-commerce, parallel computing, network management, etc. Providing protection for mobile agents is one of the prime issues in the broadening of mobile agent computing. Mobile agent technology faces security issues from mobile agents and platform sides. This article proposed a multilevel secure key management among mobile agents and platforms with a changeable threshold for different levels. The proposed approach is based on the Shamir secret share and Chinese remainder theorem. The novelty of this work is dynamical changing threshold value 't' provides higher security as compared to the traditional approach.

Keywords Mobile agent · Mignotte's sequence · Lagrange interpolation · Threshold value · Chinese Remainder Theorem (CRT)

1 Introduction

Mobile Agents are the composition of small programs and may keep on migrating as a unique independent unit from one platform to another. Mobile agents can execute on a remote platform and suspend its execution, migrate to another platform, and continue its execution on another platform. Because of the self-driven mobility of mobile agents through the distributed network, mobile agents may face malicious

N. Singhal (✉)
Shobhit Institute of Engineering & Technology (Deemed To-Be-University), Meerut, India
e-mail: niraj@shobhituniversity.ac.in

P. Kumar
JSS Academy of Technical Education, Uttar Pradesh, Noida, India

P. K. Mallick et al. (eds.), *Electronic Systems and Intelligent Computing*, Lecture Notes in Electrical Engineering 860, https://doi.org/10.1007/978-981-16-9488-2_52

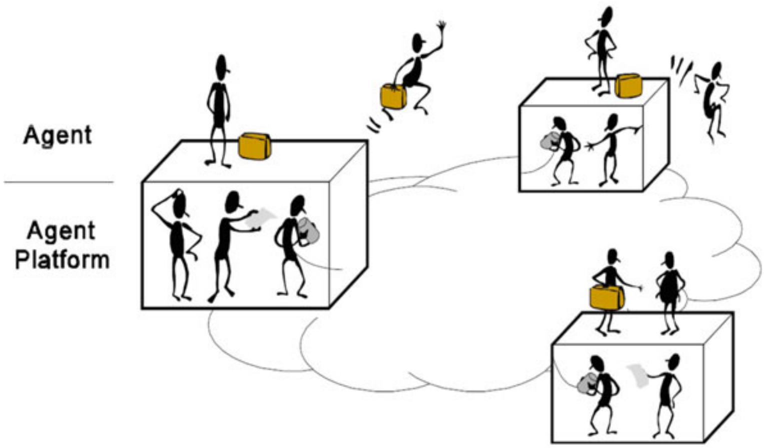

Fig. 1 Agent system model NIST

agents and platforms. Figure 1 shows the execution of mobile agents on other mobile hosts.

There are many applications in which distrusted information retrieval require mobile agent are using frequently. Mobile agent technology is useful in distributing computing because mobile agent takes less bandwidth and low latency and works automatically as compared to traditional computing.

Mobile agents migrate in a non-trusted heterogeneous environment from one hop to another hop automatically to perform the job assigned to them. Vulnerability to security can access important information by an unauthorized entity. Attacks on mobile agents are categorized into four main parts; the first Agent against platform, the second Platform against agent, the third Agent against agent, and the fourth other to both agent and platform.

The complete structure of the article is as follows. Sections 2 and 3 have been describing mainly about the agent-based frameworks and problem statement. In Sect. 4, the proposed approach has been given along with preliminaries. The performance evaluation of our approach along with implementation has been discussed in Sect. 5, and in Sect. 6, conclusions have been highlighted with future work.

2 Related Works

The major types of security risks include information disclosure, denial of service, and information corruption. These types of threats can be examined in greater depth as they pertain to the agent architecture in a variety of ways. Mobile agents simply provide more opportunities for exploitation and misuse, dramatically expanding the scope of threats.

Meng et al. [1] designed a tightly coupled multi-group secret sharing scheme to provide flexibility at the time of regeneration of secret keys. If sufficient number of participants collaborates recover the confidential key. Jia et al. [2] based on the Chinese remainder theorem proposed a novel threshold changeable secret share (TCSS) model (CRT). The TCSS technique uses a small share size and best time complexity as compared to other techniques. Yan et al. [3] designed using the Chinese remainder theorem, and the author created a lossless generic access structure for private picture sharing.

Li et al. [4] designed a multi-secret sharing decentralized technique based on multi-target MSP. Muhil et al. [5] presented a cloud security mechanism based on the Shamir secret sharing. Liu et al. [6] presented a model, for the security of packet and session key. Using quantum key distribution and otp algorithm provide unconditional data security. Takahashi et al. [7] The ramp technique was used to create a revolutionary secret sharing scheme. In this scheme, many participants can independently regenerate secret. Narad et al. [8] built a Shamir and artificial Neural Network with backpropagation-based group authentication secret sharing scheme. Many-to-many authentication is established by a given approach. Abdallah et al. [9] analyze the sharing techniques Shamir's sharing scheme, Rabin's IDA, and hybrid sharing. Basit et al. [10] Using polynomials and a one-way function, a Hierarchical Multistage Key Sharing Scheme was devised. Strong security is provided by a one-way function, a threshold value, and a hierarchical structure. Yuan et al. [11] On the basis of a one-way function, a variable threshold secret sharing technique was presented.

Phiri et al. [12] Based on Shamir's scheme, the Elgamal algorithm proposed a new (t, n) threshold secret key sharing mechanism called the Polynomial Based Linear Scheme (PBLS). Shehada et al. [13] For real-time applications, a new broadcast-based Secure Mobile Agent Protocol was proposed. Higher security is provided by the proposed mobile agent architecture, which employs a combination of private and public cryptography schemes. Fragkakis et al. [14] produced a comparison of mobile agent security among different protocols. On the basis of comparison, mobile agent security faces a lack of security trust and models. Adri et al. [15] proposed a trust score-based itinerary planning algorithm for decision-making for authentication of mobile agents and platforms. Trust ability is based on the coefficient of variance. Trust score is calculated by five parameters; persistence, competence, reputation, credibility, and integrity. Srivastava et al. [16] proposed an algorithm to provide self-protection of the mobile agent in such a way it can assure confidentiality and authentication at the time of execution in a malicious environment. Raji et al. [17] proposed a new algorithm to provide anonymity of both mobile agent owner and the itinerary. The proposed algorithm is more advantageous compared to the previous algorithm.

Chen et al. [18] Using Euler's theorem and modular arithmetic, we proposed a secret sharing mechanism for n users with a threshold value. The proposed secret sharing scheme has a linear time complexity.

3 Problem Statement

According to the research on protecting migrating agents, there are a variety of ways for providing security for migrating agents, but none of them currently provide an overall framework that incorporates compatible techniques into an effective security model. The old host security mindset prevails, and protection mechanisms inside the mobile agent paradigm continue to prioritize safeguarding the agent platform. However, the focus is gradually shifting toward developing solutions aimed at migrating (mobile) agent security, which is a considerably more complex problem.

Mobile agent-based framework uses the recourses of different hosts for the execution of code. Because mobile agents freely move in a heterogeneous environment, this is the main reason mobile agent opens for attack. So, there is a requirement to design such a framework that solves the security problem of the mobile agent as well as the platform.

The problem to design a mechanism is a challenging task because of the autonomy and mobility of mobile agent. A new scheme is proposed here for the security of mobile agent and platform based on multilevel key management and dynamic threshold value. The mobile agent and platform require a dynamic threshold value for different levels of authentication. A strategy based on the Lagrange polynomial and the Chinese remainder theorem is proposed for secure mobile agent migration. Multilevel secret keys for the execution and authentication of mobile agent migration have been generated. At the first level, the Secret is divided into 'n' partial shares based on the Lagrange interpolation, and at the second level, each partial share generated at the first level is further divided into m parts using CRT. Dynamic threshold value is also used at each level.

4 Proposed Solution

In a mobile agent system, a multitier dynamic threshold offers the core security requirements against many types of threats. The proposed multilevel architecture based on the Shamir secret share and Chinese remainder theorem provides the security at multilevel with a dynamic threshold value.

4.1 Preliminaries

4.1.1 Shamir's Secret Sharing

In 1979, Shamir presented a secret share method based on a threshold. Secret keys are splits into 'n' partial shares with threshold 't'. At the time of regeneration, if 't' number of authentic participants is involved then generate a secret key. According to the Shamir share, consider 't' real number $\beta 0,\ \beta 1,\ \beta 2, \ldots \beta \mathrm{k}-1 \in \mathrm{GF}$ (p)

$$\mathrm{F(x)} = \left(\beta 0 + \sum_{i=1}^{k-1} \beta_{\mathrm{i}} \mathrm{x}^{\mathrm{i}} \right) \bmod \mathrm{p} \tag{1}$$

$\mathrm{F}(0) = \beta 0 =$ session key and 'p' is a large prime number and $\beta 1,\ \beta 2 \ldots,$ and $\beta \mathrm{k}-1$ are randomly chosen real numbers from Z/PZ. At the receiver side, select 't' randomly share out of 'n' partial share and generate the Lagrange polynomial.

$$\mathrm{F(x)} = \sum_{\mathrm{i}=1}^{\mathrm{k}} \Upsilon_{\mathrm{i}} \prod_{1 \le j \le k, j \ne 1} \frac{\chi - \chi_{\mathrm{i}}}{\chi_{\mathrm{i}} - \chi_{\mathrm{j}}} \tag{2}$$

Since f (0) $= \beta 0 =$ S, the secret key evaluates using

$$\text{Secret key(S)} = \sum_{i=1}^{k} P_i \Upsilon_i \tag{3}$$

where

$$P_i = \prod_{1 \le j \le k, j \ne i} \frac{\chi_j}{\chi_j - \chi_i} \tag{4}$$

Secret share is generated by using 't' partial share by using F (0) $= \beta 0$modp.

4.1.2 Chinese Remainder Theorem

Consider the co-prime integer p1, p2, p3 , …pn and $\alpha 1,\ \alpha 2,\ \alpha 3 \ldots \alpha \mathrm{n}$ random integer 'x' system of a simultaneous congruence relation

$$\begin{gathered} \mathrm{x} \equiv \alpha 1(\mathrm{modp1}) \\ \mathrm{x} \equiv \alpha 2(\mathrm{modp2}) \\ \ldots \\ \mathrm{x} \equiv \alpha n(\mathrm{modpn}) \end{gathered} \tag{5}$$

has a unique solution modulo.

p1, p2, ... pn, for any given integers $\alpha 1, \ \alpha 2, \ldots \alpha$n.

$$\begin{aligned} & \mathrm{P} = \mathrm{p} * \mathrm{p2} * \ldots * \mathrm{pn} \\ & \mathrm{x} \equiv \alpha 1\mathrm{P1c1} + \alpha 2\mathrm{P2c2} + \cdots + \alpha \mathrm{nPncn}(\mathrm{mod p}) \end{aligned} \tag{6}$$

where Pi $=$ P$\big/$ni and ci $\equiv$ Pi $-$ 1(modpi).

4.1.3 Mignotte's Sequence

Let us consider 'n' positive integer, be n $\geq$ 2, and 2 $\leq$ t $\leq$ n. The consecutive numbers are pairwise co-prime such that it satisfies the condition on n integers

$$\prod_{i=0}^{t-2} Pn - i < \prod_{i=1}^{t} Pi \tag{7}$$

4.2 Proposed Model

Here, a multilevel dynamic variance threshold technique for mobile agent is proposed to provide the security of secret share among participants. This model shown in Fig. 2 works as a two-level hierarchy; in the first level of hierarchy, the platform breaks the secret key among the n mobile agents using the Lagrange interpolation with modular arithmetic with a dynamic threshold value. At the second level, each mobile agent has a partial share generated by first level; further, this partial share is split into 'm' shares using the Chinese remainder theorem dynamic threshold value. This model provides a higher level of security against the attacker by confusion and diffusion.

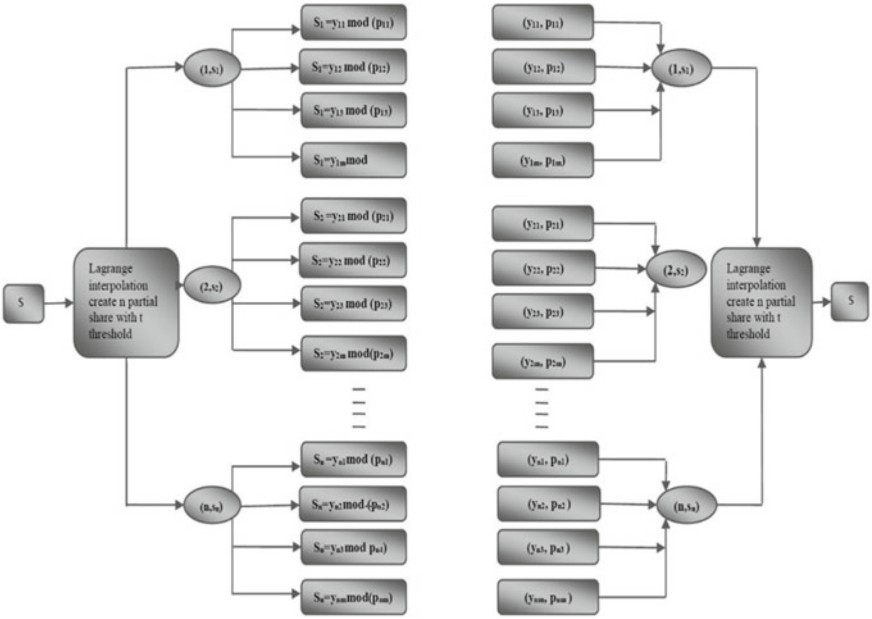
S
Lagrange interpolation create n partial share with t threshold
$(1,s_1)$
$S_1=y_{11}$ mod (p_{11})
$S_1=y_{12}$ mod (p_{12})
$S_1=y_{13}$ mod (p_{13})
$S_1=y_{1m}$mod
$(2,s_2)$
$S_2=y_{21}$ mod (p_{21})
$S_2=y_{22}$ mod (p_{22})
$S_2=y_{23}$ mod (p_{23})
$S_2=y_{2m}$ mod(p_{2m})
(n,s_n)
$S_n=y_{n1}$mod (p_{n1})
$S_n=y_{n2}$mod (p_{n2})
$S_n=y_{n3}$mod $p_{n3})$
$S_n=y_{nm}$mod(p_{nm})
(y_{11}, p_{11})
(y_{12}, p_{12})
(y_{13}, p_{13})
(y_{1m}, p_{1m})
$(1,s_1)$
(y_{21}, p_{21})
(y_{22}, p_{22})
(y_{23}, p_{23})
(y_{2m}, p_{2m})
$(2,s_2)$
(y_{n1}, p_{n1})
(y_{n2}, p_{n2})
(y_{n3}, p_{n3})
(y_{nm}, p_{nm})
(n,s_n)
Lagrange interpolation create n partial share with t threshold
S

Fig. 2 Multitier dynamic threshold-based mobile agents secure migration

A. Share generation

Input: *Take input (i, S_i) using Lagrange interpolation*
Output: *Generate (y_i, p_i) using CRT*

i. At level 1 Select any secret share in such a way S<p
ii. Using Lagrange interpolation splits the secret key s in to ‘n’ partial shares S_1, S_2, S_3….S_n
iii. At level 2 for all i=1 to n
iv. For each S_i 0< i < m Generate m number of share using CRT (y_i , p_i) at different threshold value

B. Regenerate the secret key

Input: *for each level take input (y_i, p_i)*
Output: *Generate (i, S_i)*

i. for i=1 to n
ii. for j=1tom
iii. Generate (i , S_i), by applying Chinese remainder theorem
iv. Apply Lagrange interpolation generate secrete key for every transaction.

Now considering the following example.

Level 1: At level 1, using the Shamir secret sharing based on the Lagrange interpolation, now user considers secret key 25 which is randomly selected by a random number generator.

After applying the Lagrange interpolation number of user n = 3 and threshold at level 1 is t = 3. Generate 3 partial shares (3, 43), (9, 79), and (2, 37).

Level 2: At level 2, each partial share generated by the Shamir secret further divide into m parts here m = 6 for (3,43) and $t_l = 3$ at each level applying Chinese remainder theorem with variable threshold for each transition.

m = 6 for (3, 43) and $t_{l\,=}$ 3 (y_1: 102, m_1: 149), (y_2: 22, m_2: 151), (y_3: 127, m_3: 157), (y_4: 116, m_4: 163), (y_5: 103, m_5: 167), and (y_6: 160, m_6: 173).

m_0: 47, $m_=$ 6 for (9, 79) and $t_{2\,=}$ 2 (y_1: 89, m_1: 251), (y_2: 135, m_2: 257), (y_3: 205, m_3: 263), (y_4: 30, m_4: 269), (y_5: 155, m_5: 271), and (y_6: 0, m_6: 277).

m0: 83, m = 6 for (2, 37) and $t_{3\,=}$ 4, (y_1: 33, m_1: 127), (y_2: 122, m_2: 131), (y_3: 44, m_3: 137), (y_4: 114, m_4: 139), (y_5: 141, m_5: 149), and (y_6: 32, m_6: 151).

m0: 41.

Mobile agent migrating automatically in a malicious environment when mobile agent reaches another platform generates partial secret keys by applying inverse Chinese remainder theorem with a respective threshold value. If the sufficient number of shares is not available at the time of the regeneration phase, it cannot generate partial secret keys.

Xi = $y_i * \text{mod}* p_i$ t $\leq$ i.

$t_l = 3$ for generate secret share required 3 authenticate share out of 6 shares.

s = 102mod 149, s = 22mod151, and s = 127mod157, $m_0 = 47$.

Applying CRT s mod m_0 = 43.

$t_2 = 2$ for generate secret share required 2 authenticate share out of 6 shares.

s = 89mod 251 and s = 135 mod257 m0 = 83.

Applying CRT s mod m_0 = 79.

$t_3 = 4$ for generate secret share required 4 authenticate share out of 6 shares.

s = 33mod 127, s = 122mod131, s = 44mod137, and s = 141mod151 $m_0 = 41$.

Applying CRT s mod m_0 = 37.

After getting these partial shares, applying the Shamir secret share to generate a secret key, we require 2 shares out of 3 shares because the threshold value in the Shamir secret share initially considered t = 2. Generated secret share is 25.

5 Implementation and Results

Based on Shamir's secret share and the Chinese remainder theorem, a framework is proposed with two levels of security; at level one generates 'n' partial share using the Shamir secret share, and each partial share generated at level two is further divided into 'm' parts. Table 1 presents response time of security/authentication of Reputation-based Model, Trust Scoring System, Trust Ranking System, and Multilevel security. From the results, it has been observed that the response time of the

Table 1 Comparison of response time among Reputation-Based Model (TBM), Trust Scoring System (TSS), Trust Ranking System (TRS), and Multilevel security model

S. No	No of mobile agents	Response time in seconds			
		Reputation-based model	Trust scoring system	Trust scoring system	Multilevel security
1	5	0.48	0.36	0.18	0.23
2	10	0.93	0.69	0.34	0.3
3	15	1.39	1.05	0.53	0.48
4	20	1.94	1.41	0.71	0.8
5	25	2.28	1.82	0.9	0.83
6	30	2.85	2.15	1.1	0.98
7	35	3.44	2.48	1.2	1.23
8	40	3.84	2.85	1.4	2.11
9	45	4.35	3.25	1.6	2.12
10	50	4.76	3.54	1.74	2.27
11	55	5.22	3.89	1.95	2.38
12	60	5.96	4.33	2.18	2.46
13	65	6.25	4.65	2.34	2.72
14	70	6.68	5.05	2.5	2.78
15	75	7.14	5.38	2.69	2.96
16	80	7.67	5.73	2.85	3.16

multilevel model is far better than among the Reputation-based Model and Trust Scoring System, but has a slightly high response time as compared to Trust Ranking System. In this framework, at the first level secret, if divided into ‘n’ share, and each ‘n’ share is further divided into ‘m’ share for security point of view. In the proposed model at level 1, ‘n’ number of shares are created on the basis of the Lagrange interpolation, out of n secret required ‘t1’ share to regenerate the secret share at level 1. We are using different thresholds at different levels. If less than ‘t1’ share wants to construct secret shareholder can’t generate. At the second level, we are using different thresholds for each share. Security of this mechanism is based on the Lagrange interpolation and Chinese remainder theorem. Experimental results are shown in Table 1 and graph Fig. 3. It was observed that the response time of the proposed model is much better than the other two models.

6 Conclusion and Future Scope

Security of mobile agent during migration in a non-trusted environment is still a major issue. In this article, design a multilayer framework by fusion of the Shamir secret share and Chinese remainder theorem to authenticate mobile agent at different levels.

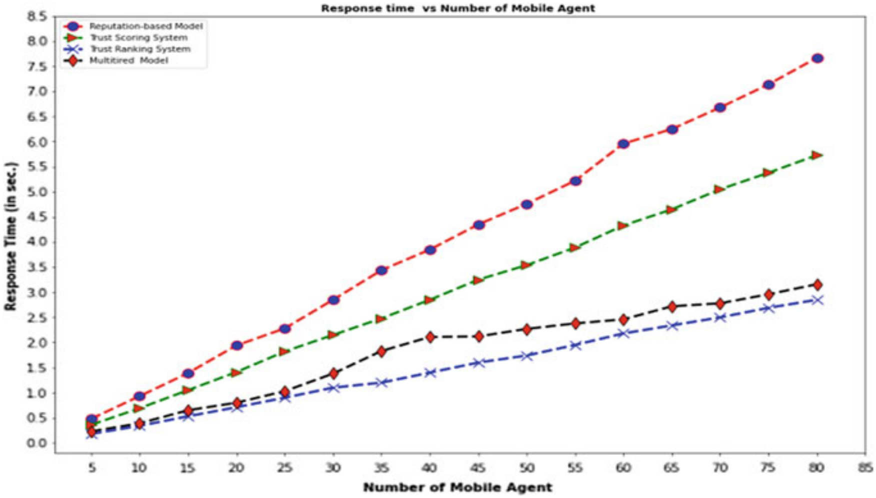

Fig. 3 Number of mobile agents versus response time

The dynamic threshold value, a combination of the Shamir and CRT, provides high-level security. This model helps to identify the unauthorized group of shareholders at a double level with a dynamic threshold value. Agent authentication is an important aspect in terms of security. The proposed model for agent migration increases the security of key as well as optimized key scheme. It focused on improving secure mobile agent migration in an open environment. In future work, such types of models will be designed that identify malicious agents from the set of agents. This would help to avoid the unwanted computation for authentication.

References

1. K Meng F Miao W Huang Y Xiong 2019 Tightly coupled multi-group threshold secret sharing based on Chinese Remainder Theorem Discret Appl Math 268 152 163 https://doi.org/10.1016/j.dam.2019.05.011
2. X Jia D Wang D Nie X Luo JZ Sun 2019 A new threshold changeable secret sharing scheme based on the Chinese Remainder Theorem Inf Sci (Ny) 473 13 30 https://doi.org/10.1016/j.ins.2018.09.024
3. X Yan Y Lu 2019 Generalized general access structure in secret image sharing J Vis Commun Image Represent 58 89 101 https://doi.org/10.1016/j.jvcir.2018.11.031
4. J Li X Wang Z Huang L Wang Y Xiang 2019 Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing J Parallel Distrib Comput 130 91 97 https://doi.org/10.1016/j.jpdc.2019.04.003
5. M Muhil UH Krishna RK Kumar EAM Anita 2015 Securing multi-cloud using secret sharing algorithm Procedia Comput Sci 50 421 426 https://doi.org/10.1016/j.procs.2015.04.011
6. Liu D, Zhang L, Fu Y, Zhang C, Yin M, Liu Y (2016) A communication model in multilevel security network using quantum key. In: Proceedings—2015 Chinese Automation Congress CAC, pp 915–918. https://doi.org/10.1109/CAC.2015.7382628

7. Takahashi S, Iwamura K (2013) Secret sharing scheme suitable for cloud computing. In: Proceedings—international conference on advanced information networking and applications AINA, pp 530–537. https://doi.org/10.1109/AINA.2013.124
8. Narad S, Sayankar M, Alone S, Mahiskar P (2017) Secret sharing scheme for group authentication—a review. In: International conference on electronics and communication and aerospace technology ICECA, vol 2017-Janua, pp 12–16. https://doi.org/10.1109/ICECA.2017.8203663
9. Abdallah A, Salleh M (2016) Secret sharing scheme security and performance analysis. In: Proceedings—2015 international conference on computing, control, networking, electronics and embedded systems engineering. ICCNEEE, vol 1, pp 173–180. https://doi.org/10.1109/ICCNEEE.2015.7381357
10. Basit A, Kumar NC, Venkaiah VC, Moiz SA, Tentu AN, Naik W (2017) Multi-stage multi-secret sharing scheme for hierarchical access structure. In: Proceeding—international conference on computing, communication and automation. ICCCA, vol 2017, pp 557–563. Janua. https://doi.org/10.1109/CCAA.2017.8229863
11. L Yuan M Li C Guo KKR Choo Y Ren 2016 Novel threshold changeable secret sharing schemes based on polynomial interpolation PLoS ONE 11 10 1 19 https://doi.org/10.1371/journal.pone.0165512
12. Phiri KK, Kim H (2019) Linear (t, n) Secret sharing scheme with reduced number of polynomials. Secur Commun Netw 2019. https://doi.org/10.1155/2019/5134534
13. D Shehada 2017 BROSMAP: a novel broadcast based secure mobile agent protocol for distributed service applications Secur Commun Netw 2017 13 15 https://doi.org/10.1155/2017/3606424
14. M Fragkakis N Alexandris F Georgiakodis 2012 A survey on the trust and security models of mobile agent platforms J Discret Math Sci Cryptogr 15 1 31 47 https://doi.org/10.1080/09720529.2012.10698362
15. John Joseph AJ, Mariappan M (2018) A novel trust-scoring system using trustability co-efficient of variation for identification of secure agent platforms. PLoS One 13(8):1–19. https://doi.org/10.1371/journal.pone.0201600
16. S Srivastava GC Nandi 2014 Self-reliant mobile code: a new direction of agent security J Netw Comput Appl 37 1 62 75 https://doi.org/10.1016/j.jnca.2013.01.004
17. Raji F, Tork Ladani B (2010) Anonymity and security for autonomous mobile agents. IET Inf Secur 4(4):397–410. https://doi.org/10.1049/iet-ifs.2009.0217
18. Chen H, Chang CC (2019) A novel (t, n) secret sharing scheme based upon Euler's Theorem. Secur Commun Netw 2019(c). https://doi.org/10.1155/2019/2387358