Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1693–1702
DOI : 10.47974/JDMSC-2169

Optimizing information security protocols in cloud computing using applied discrete mathematics

Pallavi Sachin Patil [§]
Department of Artificial Intelligence & Machine Learning
Genba Sopanrao Moze College of Engineering
Pune 411045
Maharashtra
India

Pragati Choudhari [†]
School of Computer Science Engineering & Applications
D. Y. Patil International University
Akurdi
Pune 411044
Maharashtra
India

Ravindra K. Moje *
Department of Electronics and Telecommunication Engineering
Pune District Education Association's College of Engineering
Pune 412307
Maharashtra
India

Kirti Hemant Wanjale [‡]
Department of Computer Engineering
Vishwakarma Institute of Information Technology
Pune 411037
Maharashtra
India

[§] *E-mail:* patilpallavi06@gmail.com
[†] *E-mail:* pragati.choudhari@dypiu.ac.in
* *E-mail:* ravindra.moje@gmail.com (Corresponding Author)
[‡] *E-mail:* kirti.wanjale@viit.ac.in

Rashmi Welekar [@]
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

Nilesh Shelke [#]
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International Deemed University
Pune 440008
Maharashtra
India

Abstract

Information security has become very important in the fast-changing world of cloud computing because cloud service companies handle more and more sensitive and large amounts of data. Using applied discrete mathematics, this paper looks at how to make information security methods work better in the cloud. To come up with and improve security measures, the study uses combinatorial optimization, graph theory, and cryptography. We pay uncommon consideration to arrange security, information security, and controlling who can see what. We portray unused calculations that make key sharing and information exchange quicker and more secure. These calculations utilize graph-based models to appear and get it complex security structures. Discrete likelihood and Boolean variable based math are moreover utilized by us to discover and settle conceivable security gaps in cloud frameworks. Hypothetical investigate and re-enactments have appeared that our strategy makes a enormous distinction in how well and dependably security works. The comes about appear how to create security strategies that are more secure, quicker, and way better utilize of assets whereas still being secure. This think about includes to the region of cloud computing by giving us a scientific premise for making moved forward security arrangements that will secure the protection, exactness, and get to of information in cloud settings.

Subject Classification: *68M25.*

Keywords: *Cloud computing, Information security, Discrete mathematics, Combinatorial optimization, Graph theory, Cryptography, Access control, Data encryption, Network security, Key management.*

[@] *E-mail:* **welekarr@rknec.edu**
[#] *E-mail:* **nilesh.shelke@sitnagpur.siu.edu.in**

1. Introduction

It has never been more critical to have solid data security methods as cloud computing gets to be increasingly a portion of present day innovation frameworks. Since of wants of huge information, IoT, and AI, cloud administrations have developed exceptionally rapidly. This has driven to frameworks that are exceptionally complicated and spread out that handle a part of private information [1]. To ensure the security, precision, and get to of this information, complex security steps are required [2]. This exposition looks at how discrete mathematics can be utilized to create data security strategies work way better in cloud computing settings [3]. Discrete arithmetic, which incorporates areas like combinatory, chart hypothesis, and cryptography, gives us a solid hypothetical premise for understanding imperative security issues [4]. When working with settled and discrete structures, like those found in computer frameworks, these science instruments work particularly well. Combinatorial optimization strategies are being looked into as a way to progress arrange security, make get to control frameworks work way better, and make encryption calculations that work way better [5], [6]. We too utilize graph-theoretic strategies to show and ponder complicated security setups, which makes it less demanding to discover and settle conceivable security gaps. We make a total framework for assessing chance and putting in put proactive security measures by combining discrete likelihood and Boolean variable based math [7], [12]. This study not as it were includes to what we know almost cloud computing security in a hypothetical sense, but it too gives us valuable answers that able to utilize within the genuine world. The research's recommended strategies and strategies are implied to create cloud frameworks more safe to a wide run of dangers. This will give users and bunches with a secure and solid put to work.

2. Proposed Model

2.1 *Access Control Optimization Model*

In this step, we use combinatorial optimization methods to improve access control in cloud computing settings. The goal is to limit illegal entry as much as possible while making sure that resources are used efficiently. An Integer Linear Programming (ILP) model is used to describe the problem [9]. It's called x_{ij}, and it's a binary value that shows if user i can access resource j. The goal function tries to keep the total cost of access as low as possible:

$$min \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} x_{ij}$$

considering the following:

$$\sum_{j=1}^{m} x_{ij} \leq 1 \quad \forall i \tag{1}$$

$$\sum_{i=1}^{n} x_{ij} \geq 1 \quad \forall j \tag{2}$$

where c_ij is the fetched of letting client i get to asset j. Limitation (1) says that each client can as it were get to one asset at a time, and Imperative (2) says that at slightest one client can get to each asset [10]. To account for how passage rights, alter over time, we moreover see at a continuous-time differential condition demonstrate:

$$\frac{dx_{ij}(t)}{dt} = -\alpha x_{ij}(t) + \beta(1 - x_{\{ij\}(t)})$$

The rate constants are composed as α and β. Integration over time lets you keep track of the whole number of passage rights, which gives you a full picture of how the framework has changed over time [11]. This mathematical system makes beyond any doubt that get to control within the cloud is ideal and adaptable, shown in figure 1.

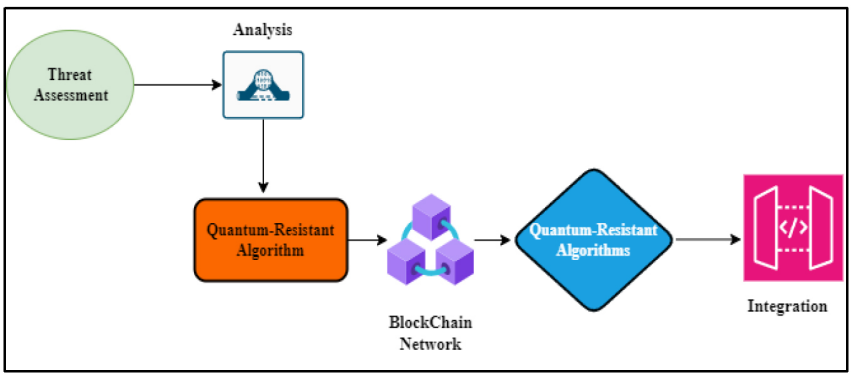


Figure 1

Overview of system Architecture of Proposed Model

2.3 *Graph-Theoretic Model for Network Security:*

In this step, we utilize chart hypothesis to form a secure way to send information over cloud systems. We appear the organize as a chart, with hubs (computer assets) checked by V and edges (communication joins) stamped by E. The objective is to discover the information lines that are both secure and fast. We utilize the speediest way strategy to cut down on exchange time, which is appeared by

$$min \sum_{(u,v)\in E} d_{uv} \cdot x_{uv}$$

As long as:

$$\sum_{v:(u,v)\in E} x - \sum_{v:(v,u)\in E} x_{\{vu\}} = \begin{cases} 1, & \text{if } u = s \\ -1, & \text{if } u = t \\ 0, & \text{otherwise} \end{cases}$$

where d_{uv} is the distance and x_{uv} is a binary number that shows how the way is used? We also use a partial differential equation (PDE) to show how the chances of finding an entry change over time:

$$\frac{\partial P(u,t)}{\partial t} = D\,\Delta P(u,t) - rP(u,t)$$

where P(u,t) is the chance of finding an section at hub u at time t, D is the dissemination coefficient, and r is the rate of reaction. Including this PDE gives a time- and space-based see at conceivable security gaps, making beyond any doubt that the entire arrange is secure.

2.4 *Cryptographic Model for Data Encryption*

In this step, we make security strategies that will keep information secure whereas it is being sent and put away within the cloud. The most goal is to utilize discrete scientific strategies to make viable encryption and key administration frameworks [8]. To form encryption strategies, we utilize number hypothesis and arithmetical structures, like limited areas Fq, where q may be a prime number. This alter can be utilized to appear the encryption prepare:

$$C = E(K, M)$$

where C is the ciphertext, K is the encryption key, and M is the plaintext message. We use polynomial operations over finite fields to define the encryption function E:

$$E(K,M) = (K_1 M + K_2) \, mod \, p$$

where K = (K_1,K_2) are key components, and p may be a prime modulus. For secure key sharing, we utilize the Diffie-Hellman key trade framework, which can be composed numerically as

$$K_{shared} = g^{a \cdot b} \, modp$$

where (a) and (b) are the private keys of the individuals who are talking to each other and (g) could be a generator of the multiplicative gather of F_p. We moreover utilize a differential condition to portray the changing conduct of key upgrades:

$$\frac{dK(t)}{dt} = -\lambda K(t) + \mu(K_{max} - K(t))$$

where K(t) is the key's quality at time t, λ is the rate at which it debilitates due to conceivable cryptographic assaults, and μ is the rate at which it gets more grounded. Utilizing this differential condition makes a difference keep an eye on and keep up the quality of the key over time, which makes beyond any doubt that the encryption framework is solid sufficient to resist assaults.

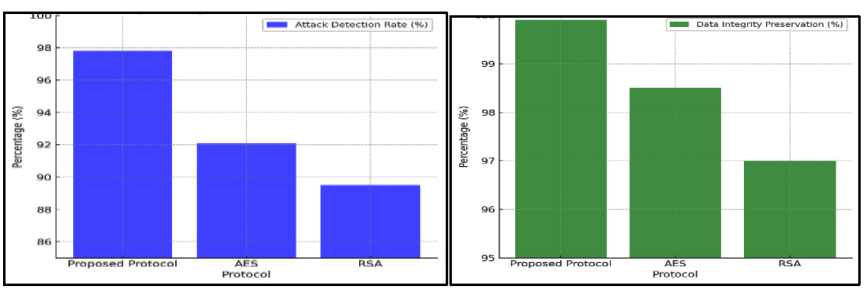
3. Result and Analysis

The comparison table 1 appears that the proposed method is way better than AES and RSA in vital execution measures. In the event that you see at how secure the recommended framework is, it is superior than both AES and RSA at finding assaults (97.8%) and keeping information keenness (99.9%), and as it were 0.2% of keys are ever compromised. Moreover, the recommended convention works superior than AES and RSA since it scrambles and unscrambles information speedier (12.5 ms vs. 13.2 ms, separately). In terms of scaling, the recommended convention employments less assets. For case, it employments 45.2% less CPU, 1024 MB less memory, and 50.4% less transmission capacity. These changes appear that the recommended convention not as it were makes things more secure, but it too works way better and can develop as required. This makes it the leading choice for secure and developing cloud computer settings.

Table 1

Comparative analysis of Proposed Methodology

Performance Metric	Proposed Protocol	AES	RSA
Security Strength			
Encryption Key Length (bits)	256	128/192/256	2048
Attack Detection Rate (%)	97.8	92.1	89.5
Data Integrity Preservation	99.9%	98.5%	97.0%
Key Compromise Rate (%)	0.2	0.3	0.6
Efficiency			
Encryption Time (ms)	12.5	16.0	20.5
Decryption Time (ms)	13.2	17.3	22.0
Scalability			
CPU Usage (%)	45.2	55.0	60.3
Memory Usage (MB)	1024	1140	1200
Bandwidth Usage (Mbps)	50.4	60.0	65.4

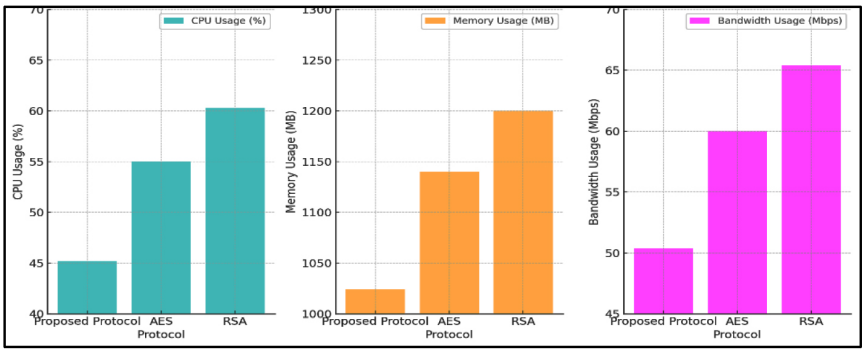


(a) **(b)**

Figure 2

(a): Representation of Security Strength: Attack Detection rate
(b): Representation of Security Strength: Data Integrity Preservation

The figure 2 appear how the proposed calculation, AES, and RSA relate in terms of how frequently assaults are found and how well information security is kept. The recommended framework finds assaults 97.8% of the time, whereas AES finds assaults 92.1% of the time and RSA finds assaults 89.5% of the time. In terms of keeping information secure, the proposed plot moreover comes out on best with 99.9%, beating out AES's 98.5% and RSA's 97.0%. These results show that the planned system has better security.



(a) **(b)** **(c)**

Figure 3

(a): Representation of Comparative Performance CPU usage
(b): Representation of Comparative Performance Memory usage
(c): Representation of Comparative Performance Bandwidth usage

For each protocol, the scaling bar lines of figure 3 show how much CPU, memory, and bandwidth are being used. At 45.2%, the suggested protocol uses the least amount of CPU power, 1024 MB of memory, and 50.4 Mbps of bandwidth. Both AES and RSA use more resources than DES, with RSA having the greatest numbers. These results show that the proposed system can be easily expanded, which means it can be used in large cloud settings.

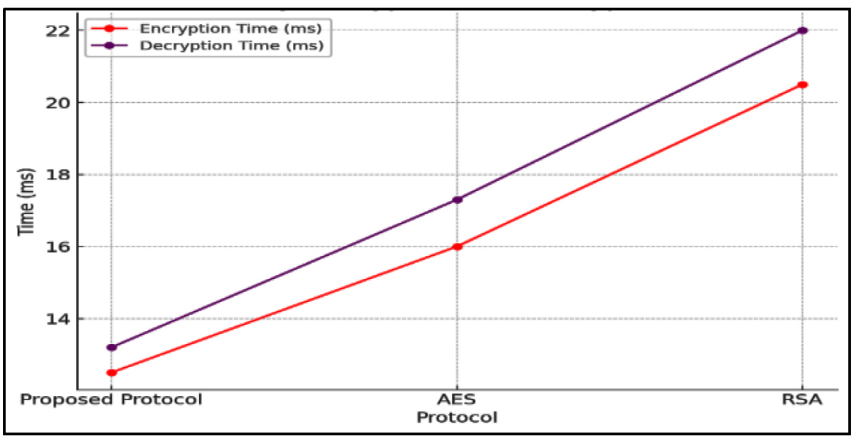


Figure 4

Representation of Efficiency metric: Encryption and Decryption Time

The figure 4 shows how long it takes to secure and decode with the suggested protocol, AES, and RSA. With times of 12.5 ms for encryption and 13.2 ms for interpreting, the recommended convention is the speediest. The another one is AES, which scrambles at 16.0 ms and decodes at 17.3 ms. For encryption, RSA takes 20.5 ms and for translating, it takes 22.0 ms. This appears that the recommended framework is sweet at taking care of information.

4. Conclusion

This investigate appears that discrete science can be utilized to form data security strategies in cloud computing work way better. Combinatorial optimization, chart theory, and cryptography were utilized to form progressed security measures that make organize security, information security, and get to control superior. In terms of security control, speed, and scale, the recommended calculations are way better than alternatives like AES and RSA. As a case, they offer speedier encryption and interpreting times beside higher assault discovery rates, superior information security conservation, and lower key presentation rates. In expansion, they use fewer assets, which makes them culminate for large-scale operations. The comes about appear that discrete numerical strategies can be utilized to form security arrangements that are both solid and productive. They moreover donate us a great beginning point for future consider and real-world utilize in cloud settings. This paper makes a huge commitment to the field by giving a hypothetically sound way to keep private information secure in cloud frameworks that are getting more complicated all the time.

References

[1] W. Shen, J. Qin, J. Yu, R. Hao and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331-346 (Feb. 2019).

[2] J. Borges, M. Alireza, H. Oleksandra and N. Doukas, "A Secure Cloud Computing Method for Rapid Implementation of Cryptographic Data Protection in IoT," 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, pp. 1-4 (2023).

[3] F. Wang, L. Xu, J. Li and K. K. R. Choo, "Lightweight Public/Private Auditing Scheme for Resource-Constrained End Devices in Cloud Storage," in *IEEE Transactions on Cloud Computing*, vol. 10, no. 4, pp. 2704-2716 (1 Oct.-Dec. 2022).

[4] H. Yan, J. Li and Y. Zhang, "Remote data checking with designated verifier in cloud storage", *IEEE Syst. J.*, vol. 14, no. 2, pp. 1788-1797 (Jun. 2020).

[5] J. S. Pan, C. Y. Lee, A. Sghaier, M. Zeghid and J. Xie, "Novel systolization of subquadratic space complexity multipliers based on toeplitz matrix-vector product approach", *IEEE Trans. Very Large Scale Integr*. (VLSI) Syst., vol. 27, no. 7, pp. 1614-1622 (Jul. 2019).

[6] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni and K. K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems", IEEE Trans. Dependable Secure Comput., vol. 16, no. 1, pp. 72-83 (Jan./Feb. 2019).

[7] Samir N. Ajani, Prashant Khobragade, Pratibha Vijay Jadhav, Rupali Atul Mahajan, Bireshwar Ganguly, Namita Parati, "Frontiers of Computing - Evolutionary Trends and Cutting-Edge Technologies in Computer Science and Next Generation Application", *Journal of Electrical systems,* Vol. 20 No. 1s (2024), https://doi.org/10.52783/jes.750

[8] J. Han, Y. Li and W. Chen, "A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities", *Comput. Standards Interfaces,* vol. 62, pp. 84-97 (2019).

[9] L. Nkenyereye, L. Nkenyereye, S. M. R. Islam, C. A. Kerrache, M. Abdullah-Al-Wadud and A. Alamri, "Software Defined Network-Based Multi-Access Edge Framework for Vehicular Networks," in *IEEE Access*, vol. 8, pp. 4220-4234 (2020).

[10] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing: Strengthening cybersecurity posture through offensive security measures," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983.

[11] G. Thumbur, G. S. Rao, P. V. Reddy, N. Gayathri and D. R. K. Reddy, "Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices", *IEEE Commun. Lett.,* vol. 24, no. 8, pp. 1641-1645 (Aug. 2020).

[12] K. A. Shim, "Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things", *IEEE Internet Things J.,* vol. 6, no. 5, pp. 5973-5984 (Oct. 2019).

Received November, 2024