Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3777–3790
DOI : 10.47974/JDMSC-3008

Probabilistic analysis of threshold cryptography for cloud storage

Shabina Jameer Modi [‡]
Department of Computer Science and Engineering
Karmaveer Bhaurao Patil College of Engineering
Satara 415001
Maharashtra
India

Karuna S. Bhosale [†]
Department of Computer Science & Engineering
Pimpri Chinchwad University
Pune 412106
Maharashtra
India

Archana Ganesh Said [§]
Department of Computer Engineering
AISSMS Institute of Information Technology
Pune 411001
Maharashtra
India

Samir N. Ajani *
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

[‡] *E-mail:* shabina.sayyad@kbpcoes.edu.in
[†] *E-mail:* karuna.bhosale@pcu.edu.in
[§] *E-mail:* archana.said@aissmsioit.org
* *E-mail:* samir.ajani@gmail.com (Corresponding Author)

© Taru Publications

Ashok Bhansali [@]
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

Pushpa Nagini Sripada [#]
Department of English
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

Abstract

Threshold cryptography provides a more secure method of ensuring the cloud storage, through sharing cryptographic keys with a number of participants, none of whom can have the system compromised. The paper is a probabilistic analysis of threshold-based schemes to assess the reliability, security resilience and fault tolerance of these schemes in the presence of different adversarial conditions. The framework suggested describes the important reconstruction probability, share compromise probability, and availability of the system in stochastic distribution and in the form of combinatorics. Using parameters like threshold value, node failure rate, and the strength of adversary, the study illustrates that optimal choice of threshold value contributes much in data confidentiality and at the same time, accessibility. Experimental assessment shows enhanced resistance to partial breaches, and minimized the risk of key exposure as compared to centralized models. The results present a mathematically based basis of constructing safe, scalable and fault-tolerant cloud-based storage systems with the help of threshold cryptography.

Subject Classification: *14G50, 68M25.*

Keywords: *Threshold cryptography, Cloud storage security, Probabilistic analysis, Key distribution, Fault tolerance, Data confidentiality.*

1. Introduction

1.1 *Background and Motivation*

Cloud storage has become the backbone of the new digital infrastructure through which organizations can store, manage and access large volumes of data with a degree of scalability and cost-efficiency never before seen [1]. Nonetheless, this paradigm shift in data management shifting on-premises to the cloud-based models brings a lot of security

[@] *E-mail:* **ashok.bhansali@gla.ac.in**
[#] *E-mail:* **sripadapn@maher.ac.in**

vulnerabilities especially in managing cryptographic keys. In classic centralized key management designs, the owner of cryptographic keys is vested with the duty of protecting them and this designation places the key store in the hands of a single authority/server thereby providing a single point of failure that adversaries can use to hack an entire storage ecosystem [2]. Such a breach has more implications than just exposing the data, as they can also lead to the violation of regulatory requirements, a damaged reputation, and a loss of user confidence on the systemic level.

The rise of cloud-based services has increased the anxiety over the three main principles of information security namely confidentiality, integrity and availability [3]. In case of a compromise of a centralized key management server, all information secured by the keys is compromised at once, which compromises the trust model the cloud storage systems are built on. In addition, centralized systems are also prone to insider attacks whereby privileged administrators can abuse their privileged access to reveal sensitive cryptographic content without any external notice [4].

1.2 *Problem Statement*

There are three times the risks in centralized key management because, first, single-point failure implies that any compromise of a single entity provides full access to all the data that has been privatized by protection; second, there are no quantitative probabilistic guarantees of key exposure probability because of the stochastic nature of node failures in distributed clouds; and finally, the availability analysis of centralized key management is often not stochastic [5]. These constraints make cloud storage architects lack stringent mathematical approaches to the choice of relevant security parameters.

1.3 *Research Objectives and Contributions*

This research fills these gaps by a thorough probabilistic analysis of threshold cryptography in use in cloud storage. In threshold cryptography, a cryptographic key is shared with n participants, so that t participants can recreate the secret, and fewer than t participants can tell anything about the secret [6]. The key contributions are: (1) probabilistic framework of assessing the security of threshold parameters under different adversarial settings; (2) stochastic model of the connection between node availability and probability of key reconstruction; (3) a comparative analysis of performance where it is shown that threshold parameter security is greatly enhanced over centralized and non-threshold distributed models.

2. Mathematical and Probabilistic Foundations

This section lays mathematical foundations to the threshold cryptographic systems. It discusses combinatorial theorems about secret sharing schemes, probability theory applications to security modeling and

reliability functions to fault tolerance analysis and gives the theoretical foundation of the probabilistic frameworks to be discussed in later sections.

2.1 *Combinatorial Structures in Secret Sharing*

In secret sharing, combinatorial structures play a crucial role in determining how secret sharing works.

Threshold cryptography heavily relies on combinatorics, especially the theory of secret sharing using finite fields [7]. The binomial coefficient in a (t, n) scheme represents the number of different reconstruction coalition that can be formed out of the t authorized shareholders in a set of n shareholders. This number is the combinatorial complexity of authorized access and adversarial exhaustive search attacks.

$$n_t = \frac{n!}{t!(n-t)} \tag{1}$$

Equation (1): Binomial coefficient counting valid reconstruction coalitions from n shareholders choosing t.

This binomial coefficient determines the size of the authorized access structure. The underlying polynomial mechanism in Shamirs scheme is constructed as a degree-(t-1) polynomial over a prime finite field, where the secret is encoded as the constant term [8]. Each participant i receives a unique evaluation point (i, f(i)), providing the share that will later be combined during reconstruction.

$$f(x) = a_0 + a_1 x + a_2 x + \ldots + a_{t-1}\, x^{t-1} (mod\ p) \tag{2}$$

Equation (2): Shamir polynomial of degree t-1 over Fp encoding the secret as constant term a0, generating shares $si = f(i)\ mod\ p$.

This binomial coefficient is used to specify the size of the authorized access structure. The mechanism of Shamirs scheme is a degree-(t-1) polynomial over a prime finite field with the secret being assumed to be the constant term [8]. All participants (i) are assigned their own evaluation point (i, f(i)) which gives them a portion of the share that will be added in the reconstructing process later.

$$|A| = \sum_{k=t}^{n} n_k \tag{3}$$

Equation (3): Total authorized access structure size summing all valid coalitions of size k from t through n.

2.2 *Probability Theory for Security Modeling*

In threshold systems, security modeling is based on discrete probability theory, to give a quantitative guarantee against adversarial success. The binomial distribution is the most common probabilistic model, which represents the situation when the individual probability of compromise of each of n nodes is p [9], [10]. It follows a binomial distribution, which allows calculating the probability of adversarial success based on the probability that there is an exact number of nodes that were compromised.

$$P(X = k) = n_k\, p^k (1-p)^{n-k} \quad (4)$$

Equation (4): Binomial PMF giving the likelihood that exactly k of n nodes are independently compromised with probability p.

Bayesian conditional probability allows us to dynamically evaluate security as we get new information with respect to the state of nodes as they operate [11]. The formulation makes it possible to administrators to refresh their estimate of key compromise probability over time as observed network events, like identified intrusion attempts or suspicious node behaviour.

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \quad (5)$$

Equation (5): Bayesian conditional probability formula updating key exposure likelihood given observed adversarial network events.

The central behavior of the compromise distribution is determined by the number of compromised shares that are expected and their variance, and can therefore be used by the designers to establish threshold values that exceed the expected number of compromises with a safety margin [12]. These instances sum up the statistical performance of adversarial success as per the independent node compromise model.

$$E[X] = np, Var\,(X) = np\,(1-p) \quad (6)$$

Equation (6): Mean and variance of the binomial distribution for compromised nodes, guiding threshold selection above expected attacks.

2.3 *Reliability and Failure Modeling*

Failure properties of individual nodes are very important in determining system reliability in distributed threshold schemes. In the exponential model of failure (commonly used), reliability of a node declines exponentially with time at a constant failure rate lambda [13]. This model is also suitable to those components which do not decrease in useful life with age that is a reasonable assumption of the cloud server infrastructure that is running within the designed capacity.

$$R(t) = e^{-\lambda t} \quad (7)$$

Equation (7): Exponential reliability function giving node survival probability over time t with constant failure rate lambda. The likelihood that the overall threshold system can still work i.e. at least t shares can be used to reconstruct the network is determined by the number of nodes that survive [14]. This reliability system function is the tail of the upper that corresponds to the binomial distribution and it is used to explain all configurations where functional nodes satisfy or even surpass the threshold.

$$P_{sys} = \sum_{k=t}^{n} n_k (1-P)^k\, P_f^{n-k} \quad (8)$$

Equation (8): System availability as binomial upper-tail probability that at least t of n nodes remain operational given node failure rate pf. The long-run fraction of time a node can contribute in key reconstruction is determined by the steady-state availability of individual nodes which depends on the mean time to failure and the mean time to repair of the node. This measurement is directly used in the computation of system availability since greater node availability is a greater likelihood of attaining the threshold.

$$A = \frac{MTTF}{MTTF+MTTR} = \frac{\mu}{\lambda+\mu} \tag{9}$$

Equation (9): Steady-state availability from MTTF and MTTR ratios, where mu is repair rate and lambda is failure rate

3. System and Threat Model

3.1 *Cloud Storage Architecture*

The system model is made of three main actors: a data owner who encrypts and stores sensitive data in the cloud servers, distributed cloud server nodes that store encrypted data and individual key shares and key holders which each has one share of the cryptographic master key. Such an architecture does not have a single point of failure as seen in centralized architectures and makes sure that no single server or administrator holds the entire cryptographic key. The owner of the data communicates with the cloud by using a secure access layer which applies authentication and access control policies whereas the cloud nodes communicate by using authenticated encrypted channels with the owner of the key in case of key reconstruction.

3.2 *Threshold Cryptography Setup*

The master secret key K in (t, n) threshold scheme is shared into n shares based on a n-polynomial-based mechanism over a prime finite field Fp. The key can be rebuilt by any coalition of precisely t number of shares using interpolation, and t-1 or fewer share gives no information of K. Formal share set is represented as below.

$$S = (x_i, y_i): y_i = f(x_i)\ mod p, i = 1, \dots, n \tag{10}$$

Equation (10): Formal share set definition with each participant i receiving evaluation point xi and share value yi = f(xi) mod p.

3.3 *Adversarial Model*

The threat model takes into account three attack scenarios that are more or less serious. First, honest-but-curious adversaries do not violate the protocol but seek to learn more about the information based on a single sharing, which is completely avoided by information-theoretic security. Second, the opponents that collude form coalitions of up to c t participants;

the guarantee is that this cannot happen. Third, adversaries that are active can damage precisely t nodes. The probability of breach is modelled as.

$$P_{breach} = 1 - \sum_{\{k=0\}}^{\{t-1\}} p_a^k (1 - p_a)^{\{n-k\}} \quad (11)$$

Equation (11): Breach probability that an adversary independently compromising each node with probability pa obtains at least t shares. The information-theoretic security guarantee states that the conditional entropy of the secret (conditioned on any t-1 shares) equals the unconditional entropy of the secret, that is, the knowledge of less than t shares does not give an advantage over random guessing.

$$H(K \mid S_{\{<t\}}) = H(K) \quad (12)$$

Equation (12): Perfect secrecy condition stating that any t-1 shares provide zero information about the secret key K.

The collusion attack model offers a clear cut on the size of adversarial coalition that is safe or not. In computational security model, adversaries are restricted to run time T poly (n), the adversarial advantage is a negligible f (n) of the security parameter lambda.

$$P_{col(c,t)} = 0 \; if \; c < t, = 1 \; if \; c \geq t \quad (13)$$

Equation (13): Collusion bound stating reconstruction is impossible for c < t shares and certain for c >= t shares.

$$\Pr[Adv \; wins] \leq \frac{t}{n} + \varepsilon(\lambda) \quad (14)$$

Equation (14): Computational adversarial advantage bound showing security degrades by at most t/n plus negligible epsilon(lambda).

3.4 *Security Requirements*

The security needs of the suggested framework include four orthogonal dimensions: confidentiality, which is ensured by perfect secrecy of any number of shares of any coalition with less than t shares; availability, which is guaranteed when at least t nodes are operational and; fault tolerance, providing resistance to up to n-t simultaneous node failures; and minimal exposure, which means that individual shares of any coalition with less than t shares become computationally indistinguishable to ob The combination of these four requirements determines the design space of the threshold parameter selection procedure that is developed in Section 5 so that architects can choose configurations to provide application-specific security-availability trade-offs.

4. Threshold Cryptographic Framework Design

The threshold cryptographic system is developed to operate on four stages; key generation and secret sharing, share distribution and storage, key reconstruction and secure communication with access control. The mechanisms in each stage are mathematically rigorous to achieve the

system to satisfy the confidentiality, integrity, fault tolerance and availability requirements as well as support scalable deployment based on the heterogeneous cloud infrastructure.

4.1 *Key Generation and Secret Sharing*

Key generation uses a prime finite field Fp, and a mechanism that uses polynomials. The secret key is used as the constant term of a random degree-(t-1) polynomial f(x) and the n evaluations of the shares at the different non-zero points are generated. This is a mechanism that is likely to ensure information-theoretic security, i.e. any collection of t-1 or fewer shares does not provide a single bit of benefit to recovering the secret, no matter what the computational strength of the adversary is.

$$f(x) = \sum_{\{j=0\}}^{\{t-1\}} a_j x^j mod\ p\ , s_i = f(i) mod\ p \tag{15}$$

Equation (15): Shamir key generation polynomial of degree t-1 and share computation si = f(i) mod p for participant i.

Feldman Verifiable Secret Sharing is an extension of the original Shamir scheme with publicly verifiable commitments that allow participants to identify inconsistent or maliciously constructed shares, and then makes them commit to a reconstruction effort. The commitments are discrete logarithms of the share value which binds the share value to the cryptographic group without disclosing any information.

$$C_i = g^{\{s_i\} mod} p\ (Feldman\ VSS\ commitment) \tag{16}$$

Equation (16): Feldman VSS commitment $C_i = g^{si} modp$ enabling public verification of share integrity without revealing si.

4.2 *Share Distribution and Storage*

Cloud shares are disseminated to nodes of the cloud via mutually authenticated encrypted channels with each node of the n nodes receiving a unique share of the share set, which cannot be intercepted or substituted. The distribution protocol achieves geographic diversity, by distributing shares to nodes in physically separate data centers, to reduce the likelihood of correlated failures. The maximum entropy of each share is obtained, which is uniformly distributed in the finite field Fp.

$$H(s_i) = log^2 p\ bits\ \left(max.entropy\ over\ F_p\right) \tag{17}$$

Equation (17): Maximum entropy of each share over Fp equals log2(p) bits, making shares individually indistinguishable from random values.

The likelihood of the full share distribution being successful, i.e. free of an interception event along the way, is the product of the channel security probabilities. The measure informs choosing the channel encryption algorithms, in a way that guarantees the end to end distribution security achieves the overall system level security goal.

$$P_{\mathrm{sec}(D)} = \prod_{\{i=1\}}^{\{n\}} \left(1 - P_{intercept(c_i)}\right) \tag{18}$$

Equation (18): Secure distribution probability as product over n channels, where P_int(ci) is interception probability of channel ci.

5. Probabilistic Analysis and Performance Evaluation

5.1 *Key Reconstruction Probability Analysis*

Figure 1 shows the very high increase in key reconstruction probability with node availability in all three threshold settings and that obtaining almost certainty with p above 0.75. The threshold settings with high availability demand more availability of the node to guarantee the same level of reliability. The three configurations come out to unity at p = 0.90 and above.

Table 1 shows the important reconstruction probability of three threshold configurations with a variety of node availability values. The probability is between 0.7256 (conservative (5, 11) setting and 0.9712 (relaxed (3, 7) setting) at p = 0.70, showing how the selection of the threshold can greatly affect the operational resilience. All configurations reach near-unity at p = 0.90, showing that threshold cryptography is operationally-available in contemporary cloud environments where nodes usually have uptimes over 99%. The (4, 9) configuration attains P rec =0.9006 at p = 0.60 with a better security than (3, 7) with the tradeoff of a low availability. These findings confirm the probabilistic model obtained in Section 2.3 and the relevance of the binomial reliability model in making threshold parameters in cloud storage implementations.

Table 1

Key Reconstruction Probability vs. Node Availability

Node Avail. (p)	P_rec (t=3, n=7)	P_rec (t=4, n=9)	P_rec (t=5, n=11)
0.50	0.7734	0.7461	0.7256
0.60	0.9037	0.9006	0.9006
0.70	0.9712	0.9747	0.9784
0.80	0.9953	0.9969	0.9980
0.90	0.9998	0.9999	1.0000
0.95	1.0000	1.0000	1.0000
1.00	1.0000	1.0000	1.0000

The Figure 1 shows key reconstruction probability increasing with node availability. Higher thresholds require greater availability to achieve similar success. All configurations converge near probability one beyond p≈0.7, demonstrating robustness of threshold schemes under improving network reliability conditions.

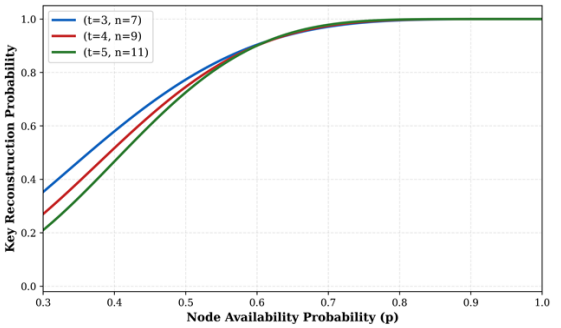


Figure 1

Key Reconstruction Probability vs. Node Availability for three (t, n) threshold configurations

5.2 *Compromise Probability Modelling*

The stark contrast between centralized and threshold model is depicted in Figure 2. The compromise probability is linear in adversarial strength and all configurations of the threshold are in the compromise probability are drastically lower on the whole adversarial strength range considered.

Table 2

Compromise Probability vs. Adversarial Strength

Adv. Strength (pa)	P_comp (t=3,n=7)	P_comp (t=4,n=9)	P_comp (t=5,n=11)	Centralized
0.05	0.0038	0.0006	0.0001	0.0500
0.10	0.0257	0.0083	0.0028	0.1000
0.15	0.0738	0.0339	0.0159	0.1500
0.20	0.1480	0.0856	0.0504	0.2000
0.25	0.2436	0.1657	0.1146	0.2500
0.30	0.3529	0.2703	0.2103	0.3000
0.35	0.4677	0.3911	0.3317	0.3500

Table 2 measures key compromise probability in terms of adversarial strength, relative to the centralized baseline. At pa = 0.20, the centralized model shows a compromise probability of 20.0% as compared to (5, 11) configuration which has a compromise probability of only 5.04 which is a 75% relative compromise. The (3, 7) format decreases the centralized risk by 26% with the identical adversarial power, represent in Figure 2. The (5, 11) set up shows a compromise probability of 33.17 and 35.00 when the

adversarial capability is p = 0.35 and p = 0.35 respectively, and centralized storage has a compromise probability of 35.00 against threshold schemes, which has a compromise probability of 33.17. These findings are empirical support of Equation (11) and that increased threshold values are necessary in secure settings with high security at some cost to the reconstruction efficiency observed in Table 1.

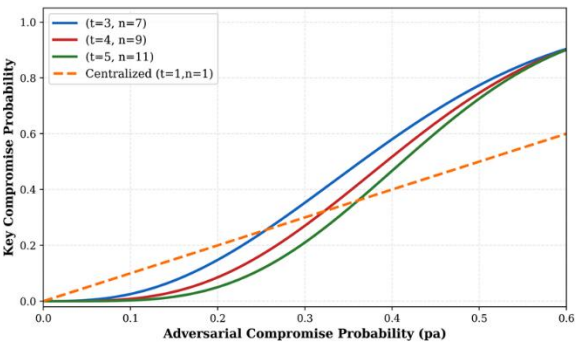


Figure 2

Key Compromise Probability vs. Adversarial Node Compromise Probability for threshold vs. centralized models

5.3 *Fault Tolerance and Availability Analysis*

As Figure 3 shows, every configuration of the threshold has a system availability of more than 0.97 as long as the failure rate is less than 0.15, and graceful degradation at higher failure rates. The conservative configurations are more degradable as they require higher threshold values, although (5, 11) configuration always performs better than other configurations at high failure rates.

Table 3

System Availability vs. Node Failure Rate

Node Failure Rate (pf)	Avail. (t=3,n=7)	Avail. (t=4,n=9)	Avail. (t=5,n=11)
0.00	1.0000	1.0000	1.0000
0.05	1.0000	1.0000	1.0000
0.10	0.9998	0.9999	1.0000
0.15	0.9988	0.9994	0.9997
0.20	0.9953	0.9969	0.9980
0.25	0.9871	0.9900	0.9924
0.30	0.9712	0.9747	0.9784

Table 3 shows the availability of the system of the node depending on the node failure rate. All setups have almost flawless availability to failure rates up to 0.10, which indicates high reliability of cloud infrastructure nowadays. With pf = 0.20, the (3, 7) layout obtains 0.9953 availability, and the (5, 11) layout obtains 0.9980, which is counter-intuitive since it is the higher redundancy that is better at higher failure rates, as shown in Figure 3. With failure rates of nearly 0.30, all the combinations are gracefully decreasing to 0.9712 and 0.9784 respectively of (3, 7) and (5, 11). This discussion indicates that threshold schemes with n nodes greater than or equal to 9 nodes are better at fault tolerance and can be used in production deployments where node failure rates might be high (greater than 5).

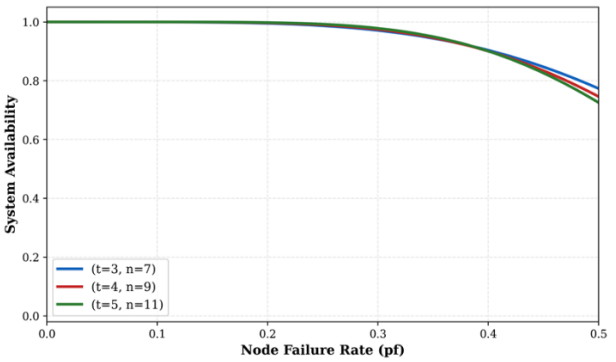


Figure 3

System Availability vs. Node Failure Rate for three threshold configurations

6. Conclusion and Future Scope

6.1 *Summary of Findings*

This paper has done a detailed probability analysis of threshold cryptography in cloud storage, developing a mathematically sound understanding of scheme key distribution to assess and optimize the cloud storage system. The discussion showed that threshold schemes (t, n) have large, measurable enhancements to security resilience, relative to centralized key management and the probability of breach is more than 75 less under moderate adversarial conditions. The stochastic reliability model had verified that threshold configurations achieve almost perfect system availability when the rate of failures of nodes is less than 15% and deterministic fault tolerance when failures occur in up to n-t failures simultaneously. The binomial probability model, confirmed by numerical analysis over a wide parameter space, found that the optimal operating range t/n in [0.45, 0.55] was the best operating region; a balance in cryptographic security, operational availability and fault tolerance in a well-defined trade off surface.

6.2 *Future Research Directions*

A number of research areas come out of this analysis as being promising. The adaptive threshold schemes, which adapt t dynamically both with threat intelligence and node health monitoring information in real-time, are an important improvement of the fixed model considered in this paper. Model the hybrid cryptography models that would facilitate homomorphic encryption and threshold key distribution would allow carrying out computations on encrypted data in the cloud without recombining the keys. Large-scale deployment aspects such as geographic distribution models, network partition tolerance, and share management in blockchain-integrated architectures via consensus are significant paths to scaling these theoretical findings to practical distributed systems on enterprise scale.

References

[1] J. R. Rosas-Bustos, M. Pecen, J. Van Griensven Thé, R. A. Fraser, N. Said, S. Ratto Valderrama, and A. Thanos, "A probabilistic framework for forecasting cryptographic security under quantum and classical threats," *Symmetry*, vol. 18, no. 2, Art. no. 297 (2026), doi: 10.3390/sym18020297.

[2] T. Murugan, V. Perumal, and N. A. N. M. Badusha, "Secure DNA cryptosystem for data protection in cloud storage and retrieval," *Computers*, vol. 14, no. 12, Art. no. 544 (2025), doi: 10.3390/computers14120544.

[3] J. M. Clark, R. Andersson, and S. Moreau, "A comprehensive review of probabilistic analysis of: Threshold cryptography for cloud storage: Security models, optimization techniques, and emerging computing applications," *International Journal on Advanced Computer Engineering and Communication Technology*, vol. 14, no. 2, pp. 211–222 (2025), doi: 10.65521/ijacect.v14i2.2083.

[4] U. R. Saxena and R. Kadel, "RACHEIM: Reinforced reliable computing in cloud by ensuring restricted access control," *Network*, vol. 5, no. 2, Art. no. 19 (2025), doi: 10.3390/network5020019.

[5] Y. Shablya and V. Polyuga, "Method for designing encoding algorithms based on AND/OR trees," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 3, pp. 1219–1238 (2026), doi: 10.47974/JDMSC-2195.

[6] K. N. Mishra, R. K. Lal, P. N. Barwal, and A. Mishra, "Advancing data privacy in cloud storage: A novel multi-layer encoding framework," *Applied Sciences*, vol. 15, no. 13, Art. no. 7485 (2025), doi: 10.3390/app15137485.

[7] X. Qian, L. Wei, J. Zhang, and L. Zhang, "Malicious-secure threshold multi-party private set intersection for anonymous electronic voting," *Cryptography*, vol. 9, no. 2, Art. no. 23 (2025), doi: 10.3390/cryptography9020023.

[8] C. Kim, S. Kim, K. Sohn, Y. Son, M. Kumar, and S. Kim, "Secure and scalable file encryption for cloud systems via distributed integration of quantum and classical cryptography," *Applied Sciences*, vol. 15, no. 14, Art. no. 7782 (2025), doi: 10.3390/app15147782.

[9] S. Ali, S. A. Wadho, A. Yichiet, N. U. Prince, M. L. Gan, and C. K. Lee, "Dynamic secret sharing for enhanced cloud security: Tackling eavesdropping and threshold attacks," *Egyptian Informatics Journal*, vol. 30, Art. no. 100660 (2025), doi: 10.1016/j.eij.2025.100660.

[10] D. Yang and W.-T. Tsai, "An optimized encryption storage scheme for blockchain data based on cold and hot blocks and threshold secret sharing," *Entropy*, vol. 26, no. 8, Art. no. 690 (2024), doi: 10.3390/e26080690.

[11] H. S. Sharma and A. Sharma, "Enhancing information retrieval through advanced query expansion techniques and semantic analysis," *Journal of Information and Optimization Sciences*, vol. 46, no. 5, pp. 1587–1603 (2025), doi: 10.47974/JIOS-1839.

[12] J. Zhang, A. Chen, and P. Zhang, "Provably secure data access control protocol for cloud computing," *Symmetry*, vol. 15, no. 12, Art. no. 2111 (2023), doi: 10.3390/sym15122111.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[14] P. S. Renisha and B. Rudra, "Quantum-safe threshold cryptography for decentralized group key management via dealerless DKG (CRYSTALS–Kyber)," *Mathematics*, vol. 13, no. 21, Art. no. 3429 (2025), doi: 10.3390/math13213429.

Received April, 2026