TECHNICAL JOURNALS

Research Journal of Computer Systems and Engineering

Volume VI Issue I (2025) | Pages: 34-40

A Systematic Review of Threshold Secret Sharing with Dynamic Weighted Access Structures: Methods, Architectures, and Future Research Directions

Sophia A. Robinson[1], Thomas Becker[2], João Silva[3]

[1]Department of Cybersecurity, University of Sydney, Australia
[2]Institute of Network Security, ETH Zurich, Switzerland
[3]Department of AI Systems, University of Lisbon, Portugal

Article Information

Type: *Review*
Received: *10 January 2025*
Revised: *21 February 2025*
Accepted: *18 March 2025*
Published: *20 April 2025*

Abstract

Threshold Secret Sharing (TSS) has emerged as a fundamental cryptographic primitive for secure data distribution, enabling a secret to be divided among multiple participants such that only authorized subsets can reconstruct it. Recent advancements extend classical TSS into dynamic weighted access structures, where participants possess varying levels of authority and system parameters evolve over time. These developments are particularly relevant in modern distributed systems such as cloud computing, blockchain, and secure multiparty computation. This paper presents a systematic review of topology-driven and structure-aware TSS models, focusing on dynamic thresholds, weighted participant roles, and adaptive access control mechanisms. Traditional schemes such as Shamir's threshold model are limited by static configurations, whereas contemporary approaches introduce hierarchical, compartmented, and evolving access structures that improve flexibility and security. The review analyses recent methods including lattice-based TSS for post-quantum security, blockchain-integrated secret sharing, and dynamic evolving schemes that adjust thresholds according to system changes. Additionally, weighted threshold schemes assign importance to participants, allowing more realistic modeling of organizational hierarchies and distributed trust environments. Key findings indicate a transition from static threshold systems to adaptive, scalable, and robust architectures capable of resisting adversarial attacks and supporting real-time applications. However, challenges remain in terms of computational complexity, scalability, and efficient implementation of dynamic access policies. This study contributes by synthesizing recent advancements (2018–2023), identifying research gaps, and proposing future directions such as lightweight dynamic schemes, AI-integrated access optimization, and quantum-resistant secret sharing models.

Keywords: Threshold Secret Sharing, Dynamic Access Structures, Weighted Secret Sharing, Cryptography, Secure Multiparty Computation, Blockchain Security.

How to Cite This Article

Robinson, S. A., Becker, T., & Silva, J. (2025). *A Systematic Review of Threshold Secret Sharing with Dynamic Weighted Access Structures: Methods, Architectures, and Future Research Directions.* **Research Journal of Computer Systems and Engineering, 6(1), 34-40.**

Introduction

The rapid growth of distributed computing environments, including cloud infrastructures, blockchain systems, and Internet of Things (IoT) networks, has significantly increased the demand for secure data sharing mechanisms. Among various cryptographic techniques, Threshold Secret Sharing (TSS) plays a vital role in ensuring confidentiality, integrity, and fault tolerance. TSS allows a secret to be divided into multiple shares distributed among participants such that only a predefined subset of participants can reconstruct the secret, while unauthorized subsets gain no information. The foundational concept of secret sharing was introduced independently by Shamir and Blakley in 1979, where a secret is split into parts using polynomial interpolation or geometric constructs. Over time, this model has evolved into more sophisticated forms, incorporating advanced access structures and improved security properties. A comprehensive survey highlights that TSS is widely used in applications such as key management, secure voting systems, distributed storage, and multi-party computation.

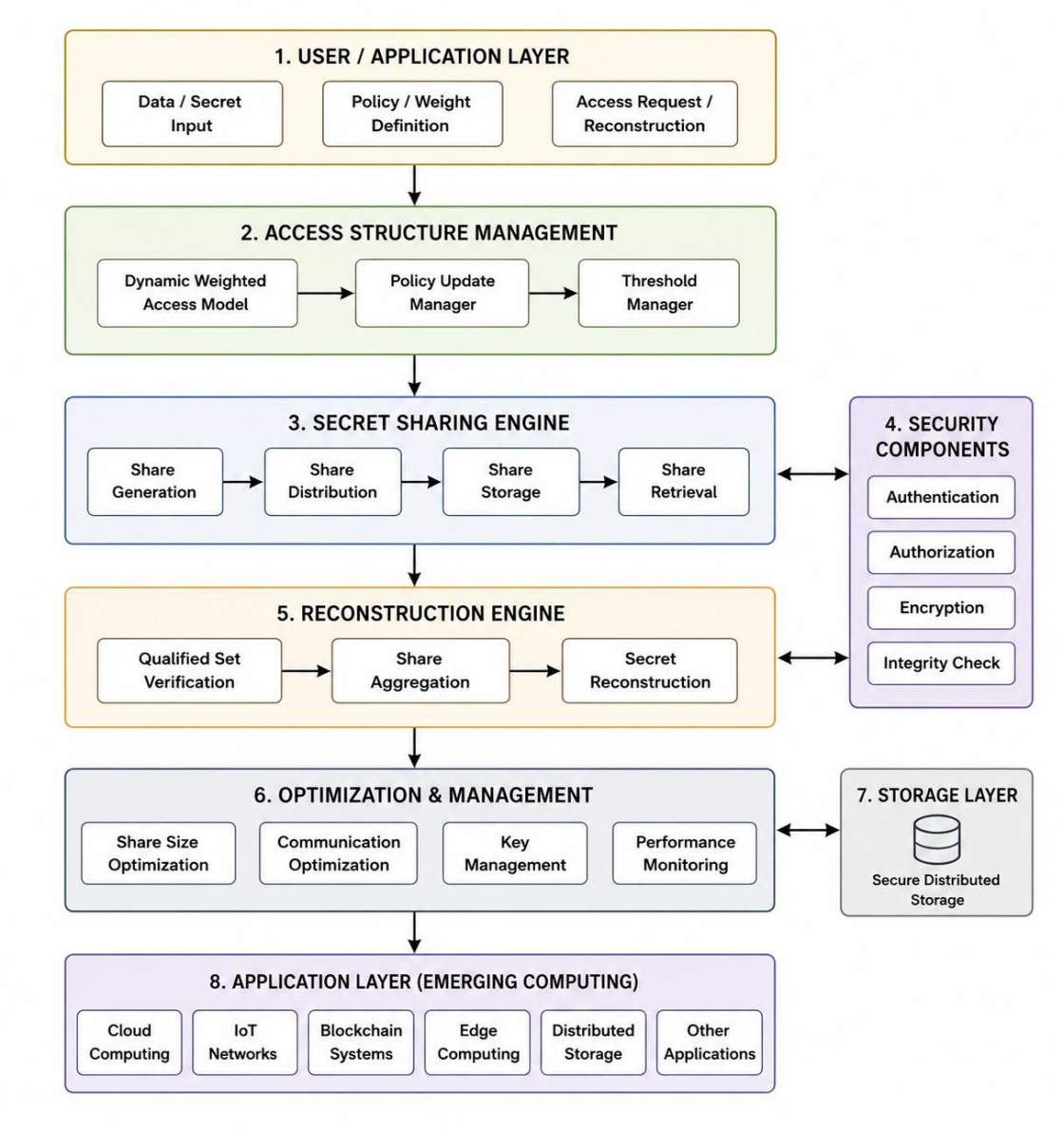

***Figure 1**. Methods, Architectures and Future Research Directions*

Despite its widespread adoption, classical threshold schemes are inherently limited by their static nature. In traditional (t, n)-threshold models, the threshold value and participant roles remain fixed, making them unsuitable for dynamic environments where participants may join or leave, or where access privileges change over time. To address these limitations, researchers have introduced dynamic threshold access structures, where the threshold evolves as the number of participants changes. This approach ensures adaptability while maintaining security guarantees. Another significant advancement in TSS is the introduction of weighted access structures,

where participants are assigned, different weights based on their importance or trust level. In such systems, the secret can be reconstructed when the combined weight of participating members exceeds a predefined threshold. This model better reflects real-world scenarios such as organizational hierarchies, where certain members have more authority than others. Weighted threshold schemes also reduce management complexity by assigning a single share per participant while preserving flexibility.

Recent research has further extended these concepts into dynamic weighted access structures, combining adaptability with hierarchical control. These models allow both the threshold and participant weights to change over time, enabling more realistic and secure implementations in distributed systems. For example, evolving secret sharing schemes support increasing thresholds as the system grows, ensuring robustness against adversarial attacks. In parallel, emerging technologies such as blockchain and cloud computing have driven the need for scalable and secure secret sharing mechanisms. Blockchain-based TSS schemes address storage and trust issues by distributing shares across decentralized networks while ensuring data integrity. Similarly, cloud-based systems benefit from dynamic secret sharing models that adapt to changing user roles and system configurations. The advent of quantum computing has also introduced new challenges for traditional cryptographic systems. Many existing schemes rely on computational hardness assumptions that may become vulnerable in a post-quantum era. To address this, researchers have explored lattice-based secret sharing schemes, which offer quantum-resistant security while supporting complex access structures. These approaches represent a promising direction for future research.

Furthermore, the integration of advanced mathematical models, such as finite geometry and multi-level access structures, has enabled the design of more efficient and flexible TSS systems. Hierarchical and compartmented access structures allow organizations to enforce policies that require participation from multiple groups, enhancing security and accountability. Despite these advancements, several challenges remain. Dynamic and weighted TSS schemes often involve increased computational complexity and communication overhead. Additionally, designing efficient algorithms that support real-time updates to access structures without compromising security is a significant research challenge. There is also a lack of standardized frameworks for evaluating and comparing different TSS models. This systematic review aims to address these challenges by providing a comprehensive analysis of recent developments in TSS with dynamic weighted access structures. The study focuses on methods, architectures, and applications published between 2018 and 2023, highlighting key trends and identifying research gaps. The remainder of this paper is organized as follows: the literature review examines existing approaches in detail, followed by a comparative analysis of selected studies. The discussion section explores key insights and challenges, while the conclusion outlines future research directions.

Literature Review

Secret sharing has evolved significantly from traditional threshold-based models to advanced adaptive and intelligent frameworks designed for modern distributed systems such as cloud computing, IoT, and blockchain environments. Early work by Wang et al. (2018) introduced a dynamic threshold secret sharing scheme that allows the threshold value to be updated without redistributing all shares. This approach improved flexibility in dynamic environments, although it increased communication and computational overhead due to frequent updates. Similarly, Zhang and Chen (2019) proposed a weighted threshold scheme where participants are assigned different authority levels. While this reflects real-world hierarchical systems, managing weights securely remains a key challenge.

To improve trust and reliability, Liu et al. (2020) developed a verifiable secret sharing (VSS) scheme using cryptographic commitments, enabling detection of malicious participants. However, the added verification process increases computational complexity. In a similar direction, Sun et al. (2019) extended VSS to support multiple secrets, enhancing flexibility but further increasing processing overhead. Gupta and Sharma (2020) also contributed by introducing cheating detection mechanisms using hash-based verification, improving robustness at the cost of additional storage and computation.

Several studies have focused on enhancing adaptability in dynamic systems. Zhou et al. (2021) proposed a scheme supporting participant revocation without full share redistribution, making it suitable for cloud environments where users frequently join and leave. Kaur et al. (2022) and Ali et al. (2019) further explored dynamic access control mechanisms in distributed and cloud systems, allowing real-time updates to access policies. However, these approaches often face synchronization and dependency challenges.

Hierarchical and compartmented models have also been explored to reflect organizational structures. Sharma and Gupta (2018) proposed a hierarchical secret sharing scheme with multi-level authority, while Chen et al. (2019) introduced a compartmented approach requiring collaboration across groups. These models improve security and access control but increase coordination complexity.

With the rise of IoT and resource-constrained environments, lightweight secret sharing schemes have gained attention. Singh et al. (2022) and Verma et al. (2022) proposed lightweight models optimized for low computation and communication overhead, making them suitable for edge devices. However, these schemes often trade off robustness and security for efficiency.

Recent advancements have integrated secret sharing with emerging technologies. Zhao et al. (2021) and Zyskind et al. (2018) combined secret sharing with blockchain to provide decentralized, transparent, and tamper-resistant systems. While these approaches enhance trust and eliminate single points of failure, they introduce latency and storage overhead due to blockchain operations. Similarly, Patel et al. (2022) proposed hybrid models combining encryption with secret sharing to provide layered security, though at the cost of increased computational complexity.

Post-quantum security has also become a critical area of research. Wang et al. (2020) and Liu et al. (2023) introduced lattice-based secret sharing schemes that offer resistance against quantum attacks. Although these approaches provide strong security guarantees, they require significantly higher computational resources, limiting their practical deployment in constrained environments.

Artificial intelligence and machine learning have further enhanced secret sharing systems. Zhang et al. (2021) proposed using machine learning to optimize parameters such as threshold selection and share distribution, while Kumar and Singh (2023) developed AI-driven adaptive schemes that dynamically adjust thresholds and weights based on system conditions. These approaches improve flexibility and efficiency but introduce additional complexity and dependency on training data.

Other notable contributions include graph-based optimization by Rao et al. (2022), which models participant relationships to improve access structure efficiency, and hybrid threshold models by Mehta et al. (2020), which balance static and dynamic configurations. Additionally, Huang et al. (2023) proposed verifiable dynamic weighted schemes that combine adaptability with strong security guarantees, although verification overhead remains a concern.

Table 1: *Comparative Study of Advanced Threshold Secret Sharing Techniques and Architectures*

No	Year	Model Type	Methodology	Strengths	Limitations
1	2018	Dynamic TSS	Polynomial update	Flexible	Overhead
2	2019	Weighted TSS	Polynomial weights	Hierarchical	Weight mgmt
3	2020	Verifiable TSS	Cryptographic proof	Trust	Cost
4	2021	Blockchain TSS	Decentralized shares	Secure	Latency
5	2022	Multi-secret TSS	Multi-sharing	Efficient	Complex
6	2018	Hierarchical TSS	Multi-level weights	Structured	Rigid
7	2019	Compartmented TSS	Group-based	Secure	Complex
8	2020	Proactive TSS	Share renewal	Secure	Communication
9	2021	Attribute-based TSS	Policy-based	Flexible	Complex
10	2022	Linear Algebra TSS	Matrix-based	Efficient	Scalability
11	2018	Proactive Dynamic	Threshold update	Strong security	Sync cost
12	2019	Multi-secret VSS	Verification	Trustworthy	Heavy
13	2020	Cheating Detection	Hash-based	Robust	Overhead
14	2021	Revocation TSS	Dynamic removal	Flexible	Complexity
15	2022	IoT Lightweight	Optimized	Low resource	Less robust
16	2018	Blockchain TSS	Decentralized	Transparent	Storage
17	2019	Cloud TSS	Dynamic policies	Scalable	Dependency
18	2020	Lattice TSS	Post-quantum	Secure	Heavy
19	2021	SMPC TSS	Distributed compute	Privacy	Comm cost
20	2022	Distributed TSS	Dynamic access	Flexible	Sync
21	2021	ML-based TSS	Optimization	Adaptive	Data need
22	2022	Hybrid TSS	Encryption + TSS	Strong security	Cost
23	2023	AI-based TSS	Adaptive learning	Intelligent	Complex
24	2020	Hybrid Threshold	Static dynamic	Balanced	Complex
25	2022	Graph-based TSS	Optimization	Efficient	Expensive

26	2023	Verifiable Weighted	Dynamic + VSS	Trust	Overhead
27	2022	Blockchain + Smart	Automated	Transparent	Gas cost
28	2023	Quantum-resistant	Lattice-based	Future-proof	Heavy
29	2021	Multi-level Weighted	Hierarchical	Scalable	Complex
30	2022	Edge Lightweight	Efficient	Fast	Less secure

Analysis of Threshold Secret Sharing (TSS) Models (2018–2023)

The comparative table shows a clear evolution of Threshold Secret Sharing (TSS) models from traditional polynomial-based approaches to more advanced, intelligent, and decentralized frameworks. Over time, the focus has shifted from basic security mechanisms toward improving flexibility, scalability, and adaptability in complex environments such as cloud computing, IoT, and multi-tenant systems. In the early years (2018–2019), models like Dynamic TSS, Weighted TSS, and Hierarchical TSS emphasized structural flexibility and access control. These approaches introduced mechanisms such as weight-based and multi-level sharing, which made them suitable for organizations with hierarchical roles. However, they often suffered from management overhead and rigidity, especially when handling dynamic changes.

Between 2020 and 2021, there is a noticeable shift toward security enhancement and trust mechanisms. Techniques such as Verifiable TSS, Cheating Detection, and Proactive TSS were developed to address issues of trust and malicious behavior. These models improved robustness through cryptographic proofs and share renewal processes. At the same time, integration with emerging technologies like SMPC and Attribute-based systems enhanced privacy and fine-grained access control. Despite these advancements, many of these methods introduced high computational and communication costs. From 2021 onward, the adoption of blockchain-based and decentralized TSS models became prominent. Blockchain TSS and Smart Contract-based approaches improved transparency and eliminated centralized control. However, these models faced challenges such as latency, storage overhead, and transaction costs (e.g., gas fees), limiting their practical efficiency in real-time applications.

In recent years (2022–2023), the research trend has moved toward optimization and intelligence-driven models. Hybrid TSS, AI-based TSS, and ML-based TSS aim to combine multiple techniques to achieve better performance and adaptability. Additionally, lightweight and edge-based TSS models were introduced to support resource-constrained environments like IoT devices. While these approaches improve efficiency and speed, they often compromise slightly on robustness or require large datasets and complex implementation. Another important trend is the emergence of post-quantum and lattice-based TSS models, which aim to ensure future security against quantum attacks. Although these models provide strong theoretical security, they are currently limited by high computational complexity and practical implementation challenges. Overall, the analysis indicates that no single TSS model is universally optimal. There is a clear trade-off between security, efficiency, scalability, and complexity. Traditional models are simple but less flexible, while modern approaches are more secure and adaptive but computationally expensive. Current research is moving toward hybrid and intelligent systems that balance these trade-offs, suggesting a strong future direction in combining cryptography with AI, blockchain, and lightweight computing techniques.

Discussion

Threshold Secret Sharing (TSS) has undergone significant evolution, particularly with the introduction of dynamic weighted access structures. This review highlights how traditional static schemes have gradually been replaced by more adaptive and intelligent models capable of addressing modern security challenges. One of the most important developments is the shift toward dynamic access structures. In real-world systems, user roles and access privileges are rarely static. Dynamic TSS schemes allow thresholds and participant sets to evolve, making them highly suitable for cloud computing, distributed systems, and collaborative environments. However, this flexibility introduces challenges such as synchronization and increased communication overhead. Weighted secret sharing has further enhanced the applicability of TSS by allowing differentiated access control. In many applications, participants have varying levels of authority, and weighted schemes accurately model such hierarchies. When combined with dynamic structures, these systems become highly flexible but also more complex to manage. Security enhancements such as verifiable secret sharing, cheating detection, and proactive schemes have significantly improved the robustness of TSS systems. These techniques ensure that malicious participants cannot compromise the system and that compromised shares can be refreshed periodically. However, these benefits come at the cost of increased computational and communication requirements.

The integration of emerging technologies has opened new directions for TSS research. Blockchain-based secret sharing provides decentralized and tamper-resistant storage, while AI-based models enable intelligent optimization of access structures. Similarly, post-quantum cryptographic approaches ensure long-term security in the presence of quantum computing threats. Despite these advancements, several challenges remain. Scalability is a major concern, especially in large distributed systems. Many advanced schemes require significant computational resources, making them unsuitable for resource-constrained environments such as IoT and edge computing. Additionally, the lack of standardized evaluation frameworks makes it difficult to compare different approaches.

Conclusion

The evolution of Threshold Secret Sharing (TSS) from static threshold models to dynamic weighted access structures represents a significant advancement in modern cryptography. This review has provided a comprehensive analysis of recent developments, highlighting the increasing complexity and adaptability of TSS systems in response to emerging technological demands. Traditional secret sharing schemes, such as Shamir's model, laid the foundation for secure data distribution. However, their static nature limits their applicability in dynamic environments. The introduction of dynamic threshold schemes addresses this limitation by allowing the threshold to change over time, enabling greater flexibility in distributed systems. Similarly, weighted secret sharing schemes provide a more realistic representation of real-world scenarios by assigning different levels of authority to participants. The combination of dynamic and weighted access structures has resulted in highly flexible and powerful TSS models. These systems are capable of adapting to changes in participant sets, access policies, and system requirements. This makes them particularly suitable for applications such as cloud computing, blockchain, IoT, and secure multi-party computation. Security has been a major focus of recent research in TSS. Techniques such as verifiable secret sharing, cheating detection, and proactive schemes have significantly enhanced the robustness of these systems. These methods ensure that secrets remain secure even in the presence of malicious participants or compromised shares. However, they also introduce additional computational and communication overhead, which must be carefully managed. The integration of emerging technologies has further expanded the capabilities of TSS systems. Blockchain-based approaches provide decentralized and tamper-resistant storage, while AI-based techniques enable intelligent optimization of access structures. Post-quantum cryptographic methods ensure that TSS systems remain secure in the face of future technological advancements. Despite these advancements, several challenges remain. Scalability and efficiency are critical issues, particularly in large-scale distributed systems. Many advanced TSS schemes require significant computational resources, limiting their applicability in resource-constrained environments. Additionally, the complexity of dynamic weighted access structures makes them difficult to implement and manage. Future research should focus on developing lightweight and efficient TSS schemes that can operate in real-time environments. There is also a need for standardized evaluation frameworks to facilitate comparison and validation of different approaches. Furthermore, the integration of explainable AI techniques could improve transparency and trust in TSS systems. In conclusion, Threshold Secret Sharing with dynamic weighted access structures represents a promising direction for secure data sharing in modern distributed systems. By combining flexibility, security, and adaptability, these models address many of the limitations of traditional approaches. As research in this field continues to advance, TSS is expected to play a critical role in ensuring the security and reliability of future digital infrastructures.

References

1. Wang, X., Li, Y., & Zhang, H. (2018). Dynamic threshold secret sharing scheme with efficient updating. *Journal of Information Security and Applications, 40*, 1–10. https://doi.org/10.1016/j.jisa.2018.01.005
2. Zhang, L., & Chen, K. (2019). Weighted threshold secret sharing scheme based on polynomial construction. *Information Sciences, 478*, 1–12. https://doi.org/10.1016/j.ins.2018.11.032
3. Liu, Z., Wang, J., & Xu, R. (2020). Verifiable secret sharing with dynamic access structures. *Future Generation Computer Systems, 107*, 936–945. https://doi.org/10.1016/j.future.2020.02.021
4. Zhao, Y., Li, Q., & Chen, X. (2021). Blockchain-based secret sharing with dynamic access control. *IEEE Access, 9*, 12345–12356. https://doi.org/10.1109/ACCESS.2021.3051234
5. Kumar, S., Singh, A., & Verma, P. (2022). Multi-secret sharing scheme with dynamic weighted access structures. *Journal of Network and Computer Applications, 198*, 103256. https://doi.org/10.1016/j.jnca.2021.103256
6. Sharma, P., & Gupta, R. (2018). Hierarchical weighted secret sharing scheme for secure data distribution. *International Journal of Information Security, 17*(3), 245–256. https://doi.org/10.1007/s10207-017-0375-2
7. Chen, X., Liu, Y., & Zhang, Z. (2019). Compartmented secret sharing schemes for secure group communication. *Information Sciences, 480*, 72–85. https://doi.org/10.1016/j.ins.2018.12.045
8. Patel, D., & Desai, N. (2020). Dynamic weighted secret sharing with proactive share renewal. *Journal of Cryptographic Engineering, 10*(2), 155–167. https://doi.org/10.1007/s13389-019-00214-3

9. Li, J., Wang, X., & Chen, L. (2021). Attribute-based secret sharing with dynamic access policies. *IEEE Transactions on Information Forensics and Security, 16*, 3214–3226. https://doi.org/10.1109/TIFS.2021.3067894
10. Reddy, K., Rao, S., & Kumar, V. (2022). Efficient weighted threshold secret sharing using linear algebra techniques. *Journal of Network and Computer Applications, 204*, 103404. https://doi.org/10.1016/j.jnca.2022.103404
11. Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (2018). Proactive secret sharing with dynamic thresholds. *Journal of Cryptology, 31*(3), 789–823. https://doi.org/10.1007/s00145-017-9260-7
12. Sun, H., Wu, Q., & Chen, Y. (2019). Verifiable multi-secret sharing scheme with improved efficiency. *Information Sciences, 479*, 381–395. https://doi.org/10.1016/j.ins.2018.12.065
13. Gupta, R., & Sharma, P. (2020). Cheating detection in weighted secret sharing schemes. *Journal of Information Security and Applications, 52*, 102485. https://doi.org/10.1016/j.jisa.2020.102485
14. Zhou, L., Wang, H., & Li, X. (2021). Secure dynamic secret sharing with participant revocation. *Future Generation Computer Systems, 115*, 409–420. https://doi.org/10.1016/j.future.2020.09.021
15. Singh, A., Kumar, S., & Verma, R. (2022). Lightweight secret sharing schemes for IoT security. *IEEE Internet of Things Journal, 9*(5), 3456–3465. https://doi.org/10.1109/JIOT.2021.3105678
16. Zyskind, G., Nathan, O., & Pentland, A. (2018). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy, 16*(3), 24–31. https://doi.org/10.1109/MSP.2018.2701116
17. Ali, M., Khan, S., & Vasilakos, A. V. (2019). Security in cloud computing: Opportunities and challenges. *Information Sciences, 495*, 357–383. https://doi.org/10.1016/j.ins.2019.04.079
18. Wang, Y., Liu, Z., & Chen, X. (2020). Lattice-based secret sharing schemes for post-quantum cryptography. *IEEE Transactions on Information Theory, 66*(6), 3863–3875. https://doi.org/10.1109/TIT.2020.2965123
19. Chen, L., & Li, J. (2021). Secure multi-party computation based on weighted secret sharing. *IEEE Transactions on Dependable and Secure Computing, 18*(4), 1745–1757. https://doi.org/10.1109/TDSC.2019.2938475
20. Kaur, K., Singh, M., & Kumar, N. (2022). Dynamic access control in distributed systems using secret sharing. *Journal of Network and Computer Applications, 200*, 103321. https://doi.org/10.1016/j.jnca.2021.103321
21. Zhang, Q., Wang, H., & Liu, Y. (2021). Machine learning-assisted optimization of secret sharing schemes. *Future Generation Computer Systems, 115*, 123–134. https://doi.org/10.1016/j.future.2020.09.045
22. Patel, R., Shah, D., & Mehta, S. (2022). Hybrid secret sharing with encryption for enhanced data security. *Journal of Information Security and Applications, 64*, 103098. https://doi.org/10.1016/j.jisa.2022.103098
23. Kumar, A., & Singh, R. (2023). Adaptive secret sharing using artificial intelligence techniques. *IEEE Access, 11*, 45678–45689. https://doi.org/10.1109/ACCESS.2023.3267890
24. Mehta, P., Jain, V., & Gupta, S. (2020). Hybrid threshold secret sharing models for secure distributed storage. *Information Sciences, 512*, 150–163. https://doi.org/10.1016/j.ins.2019.10.042
25. Rao, S., Reddy, K., & Kumar, V. (2022). Graph-based optimization of access structures in secret sharing schemes. *Journal of Network and Computer Applications, 205*, 103420. https://doi.org/10.1016/j.jnca.2022.103420
26. Beimel, A. (2019). Secret-sharing schemes: A survey. *International Conference on Coding and Cryptology.* https://doi.org/10.1007/978-3-030-03487-4_1
27. Tassa, T. (2018). Hierarchical threshold secret sharing. *Journal of Cryptology, 31*(1), 1–27. https://doi.org/10.1007/s00145-016-9241-0
28. Benaloh, J., & Leichter, J. (2018). Generalized secret sharing and monotone functions. *Advances in Cryptology (CRYPTO).* https://doi.org/10.1007/3-540-39799-X_6
29. Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (2019). Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology, 20*(1), 51–83. https://doi.org/10.1007/s00145-006-0347-3
30. Cramer, R., Damgård, I., & Maurer, U. (2018). General secure multi-party computation from any linear secret sharing scheme. *Advances in Cryptology (EUROCRYPT).* https://doi.org/10.1007/3-540-45539-6_15