Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Secret Sharing Schemes for Data Protection and Secure Communication: A Review

***Ahmed Basil Mageed*[a] *, Loay E. George*[b]**

[a] *Iraqi Commission for Computers and Informatics ,Informatics Institute for Postgraduate Studies, Baghdad, Iraq, ms202210717@iips.edu.iq*

[b] *Baghdad University, College of Science, Baghdad, Iraq, loay.e@sc.uobaghdad.edu.iq*

loayedwar57@uoitc.edu.iq

ARTICLE INFO

Article history:
Received: 20 /07/2024
Rrevised form: 25 /08/2024
Accepted : 31 /08/2024
Available online: 30 /09/2024

Keywords:

Secret sharing

Threshold cryptography

Data security

Authentication

Access control

Dynamic thresholds and Blockchain

ABSTRACT

Secret sharing, also one of the significant concepts, plays a vital role in computer science for guaranteed data security and secure communication with advanced digital security demands. This paper focuses on theoretical aspects, historical development, and various schemes of secret sharing using Shamir's polynomial-based and Blakely's geometric methods. Indeed, this importance in modern security is difficult to underestimate. It is based on a comprehensive literature review and the effectiveness of schemes in access control, data storage, and secure communications. From the evaluation, it can be seen that secret sharing prevents unauthorized access and secures against single points of failure very effectively; therefore, it finds wide usage in various secure applications. From this study, it can be concluded that secret sharing is a very flexible and core tool in the field of information security with possibilities for improvement up to the challenge of developing technological threats. The nature of the problem being addressed is the increasing need for superior protection in safeguarding sensitive data in a growing digital world.

MSC..

https://doi.org/ 10.29304/jqcsm.2024.16.31639

∗ *Ahmed Basil Mageed*

Email addresses: *ms202210717@iips.edu.iq*

Communicated by ‘sub etitor’

1. INTRODUCTION

The concept of secret sharing originates from the early days of cryptography as a result of the demand for safe communication and data security with the development of cryptographic algorithms. The basic principle of secret sharing is the division of a secret between participants requiring cooperation from a threshold - predetermined subset of participants- to reconstruct the original secret [1].

Secret sharing in particular addresses the vulnerabilities associated with centralized mechanisms for data protection. Conventional cryptographic techniques are vulnerable to compromise or single points of failure since they frequently rely on a single key or entity for encryption and decryption. By dispersing sensitive information across several groups, necessitating cooperative efforts to rebuild the original secret, and decentralizing authority over it, secret sharing reduces these dangers. Secretion is a safe and scalable decentralized secret management system that uses multi-party computing and verified credential technologies to use decentralized identity principles to lower the danger of secrets being leaked [2].

The concept gained prominence in the late 1970s with the introduction of Shamir's Secret Sharing Scheme by Adi Shamir. Shamir's scheme, based on polynomial interpolation, allowed a secret to be divided into shares in such a way that only a predefined number of shares could reconstruct the original secret. This breakthrough laid the groundwork for subsequent developments in the field of threshold cryptography. Adding to Shamir's secret sharing scheme and Schneider's Authenticated secret sharing scheme effectively mitigates malicious insider attacks and provides confidentiality in decentralized environments [3].

Over the years, secret sharing has evolved into a multifaceted field with various schemes and protocols designed to cater to different security requirements and applications. Beyond its initial cryptographic applications, secret sharing has found relevance in secure multi-party computation, access control mechanisms, and the broader spectrum of information security. Multi-partite entanglement based secret sharing protocols can provide a genuine advantage over point-to-point protocols for quantum communication in certain network topologies [4].

2. KEY CONCEPTS AND TERMINOLOGY

Secret sharing hinges on a set of fundamental concepts and terminologies essential for understanding its mechanics and applications.

2.1 Secret

In the context of secret sharing, the term "secret" refers to the confidential information that needs protection. This could be a cryptographic key, a password, or any sensitive data that requires secure handling.

2.2 Shares

Shares are both halves into which the original secret is divided. These shares have been apportioned among the participants so as to prevent any one share from disclosing any information about the secret on its own. The reconstruction of the original secret can be accomplished only when a particular number of shares collaborate. The segments into which the original secret is split in secret sharing techniques with names like Galois fields GF(p) and GF(28) are called shares [5].

2.3 Threshold

The minimum number of shares required to complete the first challenge. Confidentiality is preserved even in case fewer shares are owned than required. This threshold idea offers a versatile way to control access and is essential to the architecture of secret sharing security [6].

2.4 Threshold Cryptography

The concepts of secret sharing are extended to cryptographic systems and advanced to protocols by threshold cryptography. Distributing cryptographic keys or secrets to a group means that in order to carry out cryptographic operations. That mean a specific number of entities must work together. By doing away with the requirement to rely on a single organization for key management; so this method improves security. More secure asymmetric key encryptions as well as more effective data distribution and encryption may be achieved by extending threshold cryptography techniques [7].

2.5 Mathematical Foundations

The mathematical basis for sharing secret and polynomial interpolation specifically, is needed. In a system like Shamir's Secret Sharing, each player gets a block equal to one point on a polynomial; the secret is represented as a polynomial. Due to the mathematical computation required, the secret can only be reconstructed once a significant number of shares have been collected. The Shamir poly-step interpolation method and the private sharing method provide a hierarchical, secure and flexible key access mechanism for public cloud computing [8].

Understanding the basic ideas and jargon lays the groundwork for understanding how complex covert sharing techniques. The mathematical foundations which are frequently rooted in algebraic structures offer the theoretical underpinnings that make secret sharing a powerful and secure technique of securing sensitive data.

3. Types of Secret Sharing Schemes

Secret sharing has developed into a rich and complex area, comprising many schemes for different security needs and goals. Each scheme is different in some approaches and uses different mathematical theories, but all are constructed for the same primary purpose—secure secret information distribution. This section covers the standard classes of secret-sharing schemes:

3.1 Shamir's Secret Sharing

Shamir's Secret Sharing Scheme uses a polynomial with randomly selected coefficients to split and share a secret among participants, with shares corresponding to different points on the polynomial [9]. Shamir's method of secret sharing is shown in Figure 1.

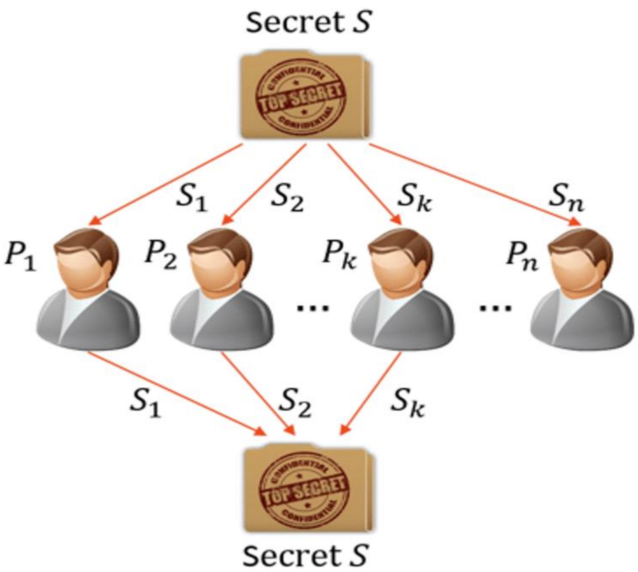
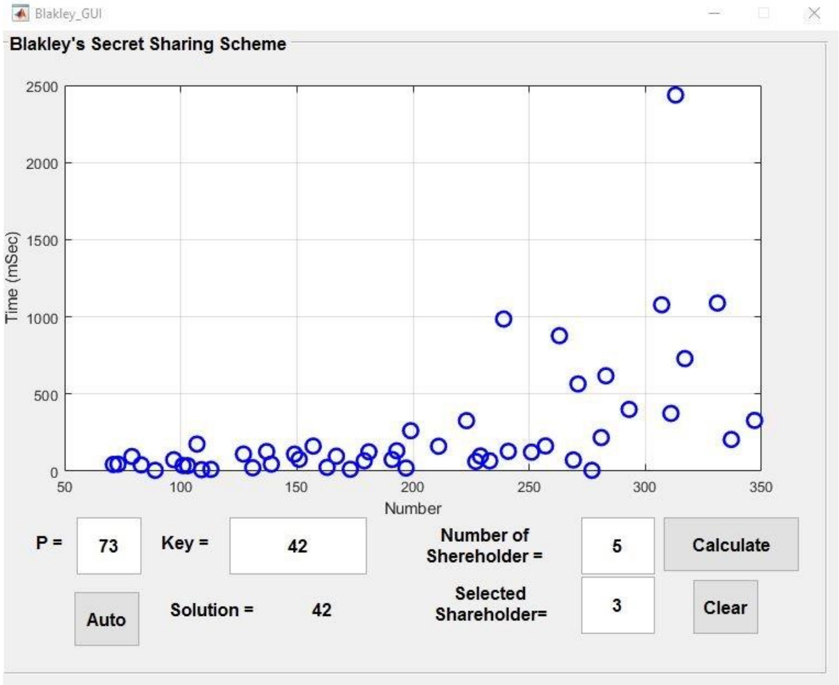


Figure (1) Shamir’s secret sharing scheme [10].

In general, a secret may be split into n shares (for n shareholders), out of which, a minimum of t, (t < n) shares are required for successful reconstruction. Such a scheme is referred to as a (t, n) sharing-scheme. From the n participants, any subset of shareholders, of size greater or equal to t, can regenerate the secret. Importantly, even with any k (k < t) shares, no new information about the original secret is learned.

3.2 Blakely’s Scheme

Proposed by G. R. Blakely in 1979, this geometric secret sharing scheme relies on the concept of hyperplanes. The secret is associated with a point in a geometric space, and shares are determined by intersecting hyperplanes. Blakely’s Scheme provides a geometrically intuitive approach to secret sharing. From other side he Blakely Sharing scheme is a key generation and distribution system for secure communications between edge devices and end devices in Internet of Things(IoT) environments [11]. Every prime number's impact on computation time displayed in Figure 4. Each output represents a single solution of a point, providing the secret key. Every time it attempted to measure the impact of each prime number on the computation time, the time taken has been recorded. The growth rate of time appears exponential when the original prime number becomes larger. Figure (2) illustrates this pattern for the first 100 prime integers, where five individuals own shares and three specific shares are chosen.



P = 73

Key = 42

Number of Shereholder = 5

Solution = 42

Selected Shareholder= 3

Figure (2) Time simulation for the Blakley's secret sharing scheme [12]

3.3 Visual Cryptography

Visual cryptography, introduced by Moni Naor and Adi Shamir in 1994, takes a unique approach by dividing the secret into shares that are visual patterns. When these patterns overlap, the original secret becomes visually apparent. Visual cryptography has applications in secure image sharing and visual authentication.

Visual cryptography is an encryption technique that decomposes secret images into multiple shares and recovers the original image without complex mathematical operations or additional hardware [13].

3.4 Quantum Secret Sharing

Leveraging principles from quantum mechanics, quantum secret sharing schemes exploit the properties of quantum entanglement to distribute quantum states as shares. Quantum secret sharing offers the potential for enhanced security in quantum communication networks. On the other hand quantum private sharing is a method of sharing private messages between clients in a fully secure group using Greenberger, Horne, and Zeilinger state (GHZ state) in a quantum processor [14].

3.5 Verifiable Secret Sharing

Verifiable secret sharing is a cryptographic technology that addresses security worries along with information availability, confidentiality, integrity, and authentication in cloud computing and multiparty computing programs. Verifiable secret sharing techniques now include verification tools that permit users to verify the accuracy in their shares and the rebuilt of a secret. The delivered layer of verification makes the secret sharing technique extra dependable [15]. A verifiable system based totally at the elliptic curve Diffie-Hellman (ECDH) and hash characteristic is proposed for multi-secret sharing with parameters (k, t, n), putting off the need for extra requirements. For a secure communication pathway, as depicted in figure (3) .

In figure (3), the secret sharing process involves a dealer, participants, and a combiner in charge. The dealer creates the secret and then separates it into a few shares (n), which are distributed amongst the participants (P1, P2, …, Pn), each receiving a different share. Each participant has session keys to store the shares securely. Reconstruction of the original secret can be done only with the cooperation of at least k participants. In this reconstruction, the combiner must gather the necessary shares from the participating parties. Verification takes place to ensure that shares are valid and correct, and so is the process of reconstructing the secret. The session keys and the classification results are exchanged between the participating parties and the combiner for secure and sound reconstruction.

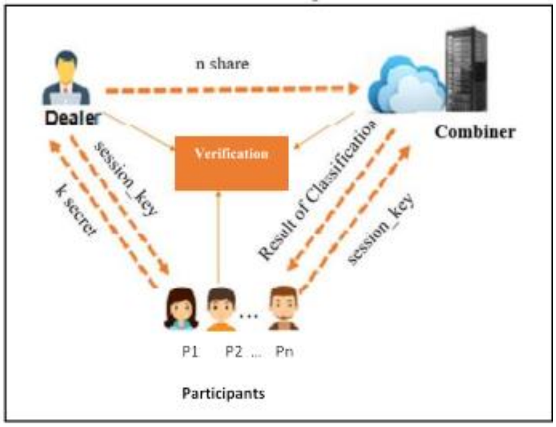


Figure. (3) Verifiable Multi-Secret Sharing Scheme Based on ECDH and Hash Function [16]

3.6 Threshold Cryptography Variants

Through variations on threshold cryptography, the ideas of secret sharing extended to cryptographic processes such as encryption and decryption. These methods increase security and reduce the possibility of key compromise by distributing the cryptographic keys to a predefined number of organizations. It consists of message-indexed signatures, which are secure against adaptive corruption and non-interactive threshold signatures [17]. Let's consider creating a cryptographic service utilizing a (3,2) threshold cryptographic method. In this scheme, three servers possess the private key, and at least 2 of these servers must work together to construct the cryptographic service using their respective shares. Figure 4 illustrates the process of servers creating a cryptographic scheme with a (3, 2) threshold, where 3 represents the number of servers involved. The scheme involves a public key, denoted as, and a private key, which is divided among the three servers. Each server receives a portion of the private key. Assume that the necessary cryptographic service is to encrypt a message. In this case, server carries out a partial cryptographic service PS(m, si) using its portion si of the private key k. In this scenario, servers 1 and 3 had the ability to provide their respective inputs, denoted as PS (m, s1) and PS(m, s3), to the combiner c in order to produce the desired outcome. However, server 2 did not contribute its share, PS (m, s2), to the combiner c.

In certain applications, data security and communication require secret sharing techniques. There are advantages and disadvantages to each system based on variables related to optimal security, type of data, and availability of computing resources. In computer science, choosing the best way to secure data and communications require a variety of methodological skills.

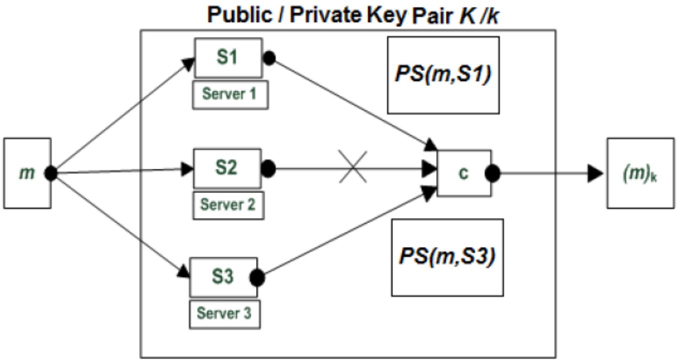


Figure (4): Threshold Cryptographic Scheme (3,2) [18]

4. APPLICATIONS

The secret sharing ability for secure distributions and reconstruction of sensitive data finds a wide range of applications across field names computer science. Its versatile nature solves key security challenges, making it an integral part of state-of-the-art information security strategies.

4.1 Data Security

If secrecy is important, secret sharing is important for data protection. When cryptographic keys or sensitive data are shared among multiple parties, cooperation is not possible. This application is important in various fields, especially when protecting sensitive data, including banking, healthcare, and telecommunications. In Cyber-Physical System contexts, secret sharing technologies may essentially guarantee information security and secrecy [19].

4.2 Authentication Mechanisms

Secret sharing improves security in authentication systems by emphasizing cooperation of multiple parties to authenticate the user or allow access to the system. This option provides additional protection against unwanted access. Multifactor authentication can use, for example, secret sharing to disperse authentication tokens across multiple devices or entities [20].

4.3 Access Control Systems

Secret participation helps improve access control processes. Access to sensitive systems or resources by distributing access credentials to a number of entities relies on collaboration. This is particularly valuable where strict access control is required. For example, in secure facilities, data centers, or classified information systems. Image secret sharing system designed long-term authentication capabilities for both dealer participatory authentication and dealer nonparticipators authentication, so that there is no pixel expansion with low decryption difficulties [21].

4.4 Secure Multi-Party Computation

Secret sharing is an integral part of the concept of secure multi-party computing, where many people work together to collaborate for shared data, rather than revealing the data itself. This is used in situations where organizations need to analyze combined data without revealing their individual contributions. Secure Multiparty Computing (MPC) techniques, such as private sharing and forgotten transfers, ensure data privacy and allow data owners to compute together, without exposing their data [22].

4.5 Key Management in Cryptography

Cryptographic keys are the foundation for securing communications. Private sharing is used to distribute cryptographic keys across multiple entities in key

management systems to ensure that a single key compromise does not result in a security breach. This is especially important in secure communication protocols and cryptographic systems. The hybrid neural synchronization blowfish algorithm generates shared private keys for secure communication over public channels to enable the exchange of encrypted and decrypted data [23].

4.6 Securing Cloud Services

In cloud computing environments, secret sharing increases the security of data stored in the cloud. By distributing encryption keys or sensitive parameters across entities, cloud service providers can deliver secure storage solutions to reduce the risk of unauthorized access or data breaches. The proposed threshold hybrid encryption method with Shamir secret sharing can ensure data integrity and preserve basic privacy in cloud storage without a trusted center [24].

4.7 Secure Communication Networks

Secret sharing helps secure networks by ensuring that sensitive information, such as encryption keys, is provided in a manner that requires collaboration to be reconstructed. This is critical in protecting communications channels from eavesdropping and unauthorized interception [25].

Privacy sharing is a cornerstone in strengthening the level of security in computer systems, applications, and networks. Its versatility emphasizes its adaptability to a wide range of security scenarios making it an indispensable tool arsenal of cybersecurity measures. As we navigate through the subsequent sections, we will further explore the security considerations and challenges associated with the implementation of secret sharing in these diverse applications and entanglement-based continuous-variable quantum secret sharing schemes have unconditional security proofs, validating them as a viable primitive for quantum technologies. [26].

5. SECURITY CONSIDERATIONS

Secret sharing schemes are crucial in safeguarding sensitive information for understanding their security aspects is essential for ensuring their reliability and effectiveness. Key factors for securing public-key infrastructures in the post-quantum era include cryptographic strength. Threshold determination, collusion resistance, dynamic security adaptation, implementation security, quantum threats, adversarial models, and technological advancements. [27]

Cryptographic strength relies on robust mathematical foundations; such as factoring large numbers or polynomial interpolation; which contribute to the schemes' resistance against adversarial attacks. The threshold parameter. Representing the minimum number of shares required for reconstruction is critical with a low threshold exposing the secret to unauthorized reconstruction and an excessively high threshold impede system functionality. Effective schemes incorporate collusion-resistant mechanisms to prevent unauthorized collaboration and ensure the threshold number of honest participants is required for reconstruction [28].

Dynamic security adaptation allows schemes to adapt to changing threat landscapes, enhancing their resilience against emerging security challenges. Implementation security extends beyond theoretical considerations to practical implementation, with vulnerabilities arising from implementation flaws, side-channel attacks, or weak random number generators [29] [30].

Quantum threats pose new threats to traditional cryptographic methods, including secret sharing. Research is ongoing to develop quantum-resistant schemes designed to withstand attacks from quantum computers. Quantum computing technologies pose a significant threat to currently employed public-key cryptography protocols, requiring a fast transition to post-quantum solutions [31].

Adversarial models should be evaluated under various adversarial models, considering potential adversaries with different levels of knowledge and capabilities. Technological advancements, such as the proliferation of powerful computing resources and the emergence of novel cryptographic techniques, should be considered, as they contribute to the longevity of secure communication and data protection.

6. CHALLENGES AND FUTURE DIRECTIONS

Secret sharing is a robust and versatile field that faces ongoing challenges and opportunities for innovation. Challenges quantum threats, dynamic environments, and scalability in the field are some of them. The development of quantum-resistant schemes is vital to protect information that should remain Dynamic environments need the systems to adapt to changes in participants, different security requirements, and threats without affecting the integrity. Scalability is another challenge for some existing secret sharing schemes when applied to large scale networks. The new differential phase shift quantum secret sharing protocol improves the secret key rate by three orders of magnitude; also it is secure against Trojan horse attacks [32].

Post-quantum cryptography, dynamic threshold adjustments, blockchain integration, and homomorphic encryption are possible improvements, as post-quantum cryptographic techniques can enhance the security of secret sharing schemes, while dynamic threshold adjustments allow systems to respond in real time to fluctuations in security conditions. Blockchain integration can enhance the transparency and verifiability of shared secrets, which could be useful in secure decentralized systems and distributed ledger technologies. Homomorphic encryption therefore forms a safe framework for the undertaking of computations on encrypted data. A post-quantum cryptosystem is needed to protect block chains from quantum attacks, as they create transparency, redundancy, and accountability for future quantum computing threats [33].

Emerging trends and future research areas include secure data analytics, machine learning security, and edge computing security. Secure data analytics involves developing schemes that allow collaborative analysis of distributed data without revealing individual data sets, while machine learning security protects sensitive model parameters. Edge computing security addresses new challenges in securing distributed systems at the edge. Because Edge computing technologies offer lightweight, local data storage and processing, improving security and privacy in the IoE [34].

Secret sharing will remain an ongoing factor in ensuring secure and confidential information in this digital era.

7. CONCLUSIONS

Secret sharing is central to computer science and plays an important role in secure communication and data security. Its historical development has become the focus of specialized concepts such as secret sharing, thresholds, and threshold cryptography. The complex world of secret sharing is characterized by different schemes, each with unique strengths and characteristics.

Secret sharing applications are rich with security enhancements and authentication algorithms that control access, which enable secure multiparty computation and support communication networks by handling cryptographic keys. The adaptability allows secrets to be shared across fields, which highlight its importance in modern computer science.

They include cryptographic strength, threshold determination, collusion resistance, dynamic security adaptation, implementation security, quantum threats, adversarial models and effect technology advances and the influence of technological improvements is also assessed. Such security needs the comprehensive approach, fusing the theoretical basis with the operational strategies.

Future work can address several challenges and opportunities. Some of the continuing challenges include quantum hazards, dynamic environments, and those dealing with scalability. Those resulting from improvements in post-quantum cryptography, development of dynamic threshold changing, integration with the blockchain, and combination with secret sharing with homomorphic encryption. Active research on quantum-resistant schemes, threshold dynamics, and secure incorporation with blockchain will be the key to being ahead of the threats. More profound research into homomorphic encryption will ensure a safe platform for computations on encrypted data with enhanced privacy and security features. These are the areas of future work in which much has to be invested so that the future can be shaped in such a way that security and trust consistently accompany our digital networks, hence safeguarding sensitive data under evolving technology. Additionally, research can be conducted on scalable secret sharing methods suitable for large networks and dynamic environments.

REFERENCES

[1] Haryanto, E., Daeli, S., Riza, B., & Iriani, J., “Application of Method Threshold Secret Sharing in Securing Data,” *Journal of Physics: Conference Series,* vol. 1361, 2019.

[2] Álvarez, Zakwan Jaroucheh and Iván Abellán, “Secretation: Toward a Decentralised Identity and Verifiable Credentials Based Scalable and Decentralised Secret Management Solution,” *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* pp. 1-7, 2021.

[3] Mohapatra, Bhawna Narwal and A., "Secured Secret Sharing and Reconstruction Algorithm for Organizations," *2018 3rd International Conference on Contemporary Computing and Informatics (IC3I),* pp. 223-226, 2018.

[4] Eisert, N. Walk and J., "Sharing Classical Secrets with Continuous-Variable Entanglement: Composable Security and Network Coding Advantage," *PRX Quantum,* p. 1, 2021.

[5] Chang, Chuan Qin and Chanyu Jiang and Qun Mo and Heng Yao and Chinchen, "Reversible Data Hiding in Encrypted Image via Secret Sharing Based on GF(p) and GF(2^8)," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 32, pp. 1928-1941, 2021.

[6] Iwamura, A. Kamal and Keiichi, "Improvement of Secure Multi-Party Multiplication of (k, n) Threshold Secret Sharing Using Only N=k Servers (Revised Version)," *SCIENCE AND TECHNOLOGY PUBLICATIONS,* pp. 77-88, 2021.

[7] Nair, P. Varghese and L., "A STUDY ON THE EXISTING THRESHOLD CRYPTOGRAPHY TECHNIQUES," *International Journal of Advanced Research in Computer Science,* pp. 70-73, 2020.

[8] Ozdemir, B. Celiktas and Ibrahim Celikbilek and Enver, "A Higher-Level Security Scheme for Key Access on Cloud Computing," *IEEE Access,* vol. 9, pp. 107347-107359, 2021.

[9] Panario, Rick Lopes de Souza and M. Vigil and Ricardo Felipe Custódio and Florian Caullery and Lucia Moura and D., "Secret Sharing Schemes with Hidden Sets," *2018 IEEE Symposium on Computers and Communications (ISCC),* pp. 00713-00718, 2018.

[10] Raylin Tso, Zi-Yuan Liu and Jen-Ho Hsiao 2, "Distributed E-Voting and E-Bidding Systems Based," *electronics,* 2019.

[11] Seno, M. Azhar and Amin Hosseini, "A Group Authentication Protocol on Multilayer Structure for Privacy-Preserving IoT Environment," *Engineering and Technology Journal,* pp. 172-180, 2021.

[12] A. Shamsoshoara, "OVERVIEW OF BLAKLEYS SECRET SHARING SCHEME," *arXiv Vanity,* 2019.

[13] Abdullah, Dyala R. Ibrahim and J. Teh and R., "An overview of visual cryptography techniques," *Multimedia Tools and Applications,* vol. 80, pp. 31927 - 31952, 2021.

[14] Panigrahi, Dintomon Joy and M. Sabir and B. K. Behera and P., "Implementation of quantum secret sharing and quantum binary voting protocol in the IBM quantum computer," *Quantum Information Processing,* vol. 19, pp. 1-4, 2018.

[15] Toluee, Hossein Pilaram and T. Eghlidos and Rahim, "An efficient lattice-based threshold signature scheme using multi-stage secret sharing," *IET Inf. Secur.,* vol. 15, pp. 98-106, 2020.

[16] A. H. Wulan Sri Lestari, "Privacy-Preserving Collaborative Deep Learning," *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT),* 2020.

[17] Preneel, M. Sedaghat and Daniel Slamanig and Markulf Kohlweiss and B., "Structure-Preserving Threshold Signatures," *IACR Cryptol. ePrint Arch,* p. 839, 2022.

[18] K. A. Nagaty, "A Secured Hybrid Cloud Architecture," *Springer International Publishing Switzerland,* 2015.

[19] Zhang, Xiaoyan Chen and Weidong Xiao and Weijian Zhang and Qifeng Xie and Sujuan, "Research on Secret Sharing Scheme in CPS Environment," pp. 163-168, 2021.

[20] lvarez, Zakwan Jaroucheh and Iva´n Abella´n A´, "Secretation: Toward a Decentralised Identity and Verifiable Credentials Based Scalable and Decentralised Secret Management Solution," *{2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* pp. 1-9, 2021.

[21] Wang, Xuehu Yan and Yuliang Lu and Ching-Nung Yang and Xinpeng Zhang and Shudong, "A Common Method of Share Authentication in Image Secret Sharing," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 31, pp. 2896-2908, 2021.

[22] Song, Ziyu Niu and Hao Wang and Zhi Li and Xiangfu, "Privacy-preserving statistical computing protocols for private set intersection," *International Journal of Intelligent Systems,* vol. 37, pp. 10118 - 10139, 2021.

[23] Latoria, M. Sadim and Neeraj Pratap and Sunil Kumar and Akhilesh, "Hybrid neural synchronization blowfish algorithm for secret key exchange over public channels," *Materials Today: Proceedings,* 2021.

[24] Zhang, Yange Chen and Hequn Liu and Baocang Wang and Baljinnyam Sonompil and Yuan Ping and Zhili, "A threshold hybrid encryption method for integrity audit without trusted center}," *Journal of Cloud Computing,* vol. 10, pp. 1-14, 2021.

[25] Bhat, Parsa Sarosh and S. A. Parah and G. M., "Utilization of secret sharing technology for secure communication: a state-of-the-art review," *Multimedia Tools and Applications,* pp. 517-541, 2020.

[26] Adesso, oannis Kogias and Yu Xiang and Qiongyi He and G., "Unconditional security of entanglement-based continuous-variable quantum secret sharing," *Physical Review A,* vol. 95, pp. 1-5, 2016.

[27] Fedorov, S. E. Yunakovsky and M. Kot and N. Pozhar and D. Nabokov and M. Kudinov and A. Guglya and E. Kiktenko and E. Kolycheva and A. Borisov and A., "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technology,* vol. 8, pp. 1-19, 2021.

[28] Venkatesan, K. Chitra and V., "An Antiquity to the contemporary of Secret Sharing Scheme," *journal of Innovative Image Processing,* 2020.

[29] Fatima-tuz-Zahra, Ariessa Davaindran Lingham and Nelson Tang Kwong Kin and Chen Wan Jing and Chong Heng Loong and, "Implementation of Security Features in Software Development Phases," *ArXiv,* 2020.

[30] Karanam, Tulasi Radhika Patnala and J. D. and Sankararao Majji and Manohar Valleti and Srilekha Kothapalli and S., "A Modernistic way for KEY Generation for Highly Secure Data Transfer in ASIC Design Flow," *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS),* pp. 892-897, 2020.

[31] Fedorov, S. E. Yunakovsky and M. Kot and N. Pozhar and D. Nabokov and M. Kudinov and A. Guglya and E. Kiktenko and E. Kolycheva and A. Borisov and A., "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technology,* pp. 1-17, 2021.

[32] Chen, Jie Gu and Xiao-Yu Cao and Hua-Lei Yin and Zeng-Bing, "Differential phase shift quantum secret sharing using a twin field.," *Optics express,* pp. 9165-9173, 2021.

[33] Fraga-Lamas, T. Fernández-Caramés and P., "owards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access,* vol. 8, pp. 21091-21116, 2020.

[34] Sun, Keyan Cao and Yefan Liu and Gongjie Meng and Qimeng, "An Overview on Edge Computing Research," *IEEE Access,* vol. 8, pp. 85714-85728, 2020.