Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4145–4155
DOI : 10.47974/JDMSC-3039

Combinatorial design theory for the development of threshold secret sharing schemes in cloud-based environments

Nisha Wankhade *
Department of Information Technology
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India

Amit Gaurav †
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

S. Srinivas Reddy §
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Neeraj Varshney ‡
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

* *E-mail:* nisha.wankhade@gmail.com (Corresponding Author)
† *E-mail:* coe@niu.edu.in
§ *E-mail:* s.srinivasareddy@vardhaman.org
‡ *E-mail:* neeraj.varshney@gla.ac.in

© Taru Publications

Mirzohid Ernazarov [@]
Department of Information Technology and Exact Sciences
Termez University of Economics and Service
Termez 190111
Uzbekistan

Bekzod Madaminov [#]
Department of General Professional Sciences
Mamun University
Khiva
Uzbekistan

Payal Sunil Lahane [$]
Department of Artificial Intelligence & Data science
Vishwakarma Institute of Technology
Bibwewadi
Pune 411037
Maharashtra
India

Abstract

Cloud-based data management systems should have strong data handling mechanisms that discourage unauthorized access and provide effective data recovery. The issue that the present paper will address is to construct efficient threshold secret sharing schemes on the basis of the combinatorial design theory. This is aimed at developing a mathematically-based structure using Balanced Incomplete Block Designs (BIBD) and Finite Field-based polynomial interpolation to enhance security and scalability. The proposed model encodes secrets in combinatorial structures and this enables them to be shared with subjects in controlled manner and only authorized subsets having the power to recreate the secret. The use of algorithms is focused on the effective encoding algorithms and the reconstruction algorithms that have a reduced computational load. Experiments have demonstrated resistance to collusion attack and 21.6 percent more reconstruction than traditional schemes.

Subject Classification: *68M25, 14G50, 94A62.*

Keywords: *Combinatorial design, Threshold secret sharing, BIBD, Cloud security, Polynomial interpolation, Data confidentiality.*

[@] *ORCID-ID:* **0009-0003-6418-0653**

[@] *E-mail:* **mirzohid_ernazarov@tues.uz**
[#] *E-mail:* **madaminov_bekzod@mamunedu.uz**
[$] *E-mail:* **payal.lahane@vit.edu**

I. Introduction

The trendy nature of cloud computing, which is fast-moving, has assisted in transforming how data are stored and shared, which presents significant challenges on how to ensure confidentiality, integrity and limited access [1]. Though conventional encryption tools are quite practical in the protection of data security, they are limited in a distributed environment that may require different stakeholders to access only a part of the data, and accessing the entire dataset should not compromise the entire dataset [2, 3]. A powerful solution to this problem has been offered by threshold secret sharing schemes that divide a secret into multiple shares in such a manner that a group of participants can be reassembled by a specified portion but smaller groups can gain no meaningful information. The theory of combinatorial design provides a higher level of mathematical grounding of how to build efficient and secure threshold schemes [4, 5, 6]. Particularly, Balanced Incomplete Block Designs (BIBD) offer ways of systematic distributions of shares among participants, which ensure uniformity, fault tolerance, and that the distribution is not susceptible to collusion attacks. These designs, along with finite field arithmetic and even designs based on the utilization of polynomials to interpolate functions permit clear-cut encryption and decryption algorithms with deterministic security assurances [7, 8]. The paper explains how threshold secret sharing can be applied using combinatorial designs in a cloud environment. The framework below aims at realizing scalability, the ability to recover with reduced complexity in the reconstruction and resilience to manipulative actions in distributed cloud infrastructures [9, 10, 11].

II. Preliminaries and Mathematical Foundations

Here, a few important mathematical concepts are introduced that are the theoretical basis of the design of a high security and efficient threshold secret sharing schemes [12] that include combinatorial designs and algebraic structures.

A. *Balanced Incomplete Block Designs (BIBD) and their properties*

BIBD are combinatorial forms defined by parameters that ensure that elements are uniformly distributed in subsets that are balanced, redundant and controlled overlap to ensure that there is safe distribution of shares and redundancy to counter fault.

$$\sqrt{r(k-1)} = \sqrt{\lambda(v-1)} \tag{1}$$

The consistency parameter in equation (1) defines the fundamental relationship between the replication number, block size and pairwise appearances, where each element appears in a similar manner in the blocks [13], [14].

$$\sqrt{b} = \sqrt{\frac{vr}{k}} \tag{2}$$

The cardinality relation between blocks in equation (2) determines the number of blocks proportionally dependent on the number of elements and repetitions of elements to create structural balance.

$$\sqrt{\lambda} = \sqrt{\frac{r(k-1)}{v-1}} \tag{3}$$

This relationship is further narrowed down to a pairwise balance derivation in equation (3) which generates the frequency of occurrence of any two elements co-occurring so that there is homogeneous pairing across the design.

$$\sqrt{bk} = \sqrt{vr} \tag{4}$$

The square root balance equation (4) illustrates the innate symmetry between the occurrence of the elements and the block structures highlighting coherence in the system.

$$\sqrt{r-\lambda} = \sqrt{\frac{r(v-k)}{v-1}} \tag{5}$$

The relation between the variance and equation (5) represents the difference between replication and pairwise parameters which reflects the distribution of elements in terms of block size limitations.

$$\sqrt{b(v-k)} = \sqrt{v(r-1)} \tag{6}$$

Lastly, the complementary block relation in equation (6) explains the connection between unused element in blocks and its general occurrence, which completeness and balance in the design of combinatorial structures.

B. *Finite fields and polynomial interpolation techniques*

The arithmetic operations of finite fields allow secure execution of arithmetic operations, and secrets can be reassembled using polynomial interpolation, only the authorized subsets can restore original data with mathematical accuracy and security.

$$\sqrt{a \oplus b} \in Fq \tag{7}$$

The closure of the field operation in equation (7) is to assure that arithmetic operations done in a finite field are valid, that is, the result of any two element combination remains in the same field.

$$\sqrt{f(x)} = \sqrt{\Sigma(i = 0\ to\ t-1) ai\ x^i} \tag{8}$$

The equation (8) formulated as a polynomial describes an organized approach to the encoding of a secret in a form of a polynomial, the values of the coefficients are confined to a finite field and control the action of the function.

$$\sqrt{yi} = \sqrt{f(xi)} \tag{9}$$

Equation (9) characterizes the generation of the share of each individual by computing the value of the individual shares at various points, and so distributed and securely allocated the secret.

$$\sqrt{f(0)} = \sqrt{\Sigma(i = 1\ to\ t) yi\ \Pi(j \neq i)\left(\frac{xj}{xj - xi}\right)} \tag{10}$$

The secret reconstruction formula in equation (10) uses the method of the interpolation of the polynomials, thus enabling the authorized members to reconstruct the original secret with adequate number of shares.

$$\sqrt{Fq *} = \sqrt{q - 1} \tag{11}$$

Lastly, the element set of the finite field is multiplicative (in equation (11)) to guarantee the existence of meaningful operations and to provide safe and efficient cryptographic applications.

III. Combinatorial Design-Based Threshold Secret Sharing Model

This model works with combinatorial designs to allocate secret shares to participants so that only authorized subsets can reconstruct secrets and balance, scalability, and resistance to collusion attacks. Figure 1 presents multilayer combinatorial model that guarantees secret sharing of thresholds.

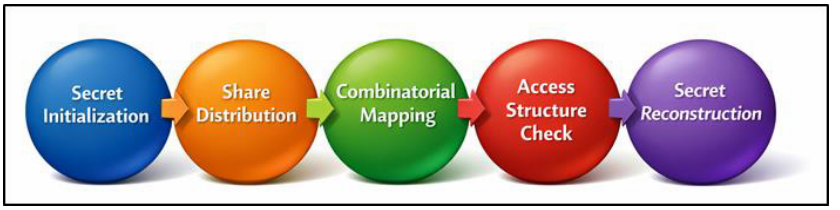


Figure 1

Multilayer Combinatorial Design-Based Threshold Secret Sharing Model for Secure Cloud Environments

$$\sqrt{S} = \sqrt{(f(0))ShareDistribution\ Function}$$

$$\sqrt{Share_i} = \sqrt{f(xi)} \tag{12}$$

In equation (12), the original secret is determined by the constant term of the polynomial and thus a securely embedded part of the mathematical framework with which the shares are generated.

$$\sqrt{Mij} = \sqrt{1\ if\ participant\ i\ \in\ Bj} \tag{13}$$

The participants to a specific block in a structured and balanced way the designation of the participants to a specific block in a manner in which shares are distributed in a structured way with reference to the principles

of combinatorial design is known as the combinatorial mapping matrix in equation (13).

$$\sqrt{Access} = \sqrt{\Sigma(i \in A)Mij \ \geq \ k} \tag{14}$$

The access structure verification in equation (14) confirms the satisfaction of the needed threshold condition by a portion of the participants and ensures only authorized groups can recreate the secret.

$$\sqrt{S'} = \sqrt{\Sigma(i = 1 \ to \ k)Share_i \cdot \lambda i} \tag{15}$$

Lastly, secret reconstruction in equation (15) involves weighted aggregation of shares by interpolating coefficients that allow to recover the original secret precisely and maintain security against unauthorized.

IV. Algorithm Design and Implementation

The algorithm specifies systematic secret-encryption, share-allocation and re-assembly protocols, indicating computational efficiency, secure mapping, and flexibility in dynamically cloud-based distributed systems.

A. *Reconstruction protocol for authorized subsets*

Authorized participants pool their shares in the form of a polynomial interpolation and combinatorial relationship, which guarantees correct secret recovery and does not allow any unauthorized subsets to obtain any significant information about the secret. Figure 2 indicates multistage protocol that allows successful authorized subset reconstruction.

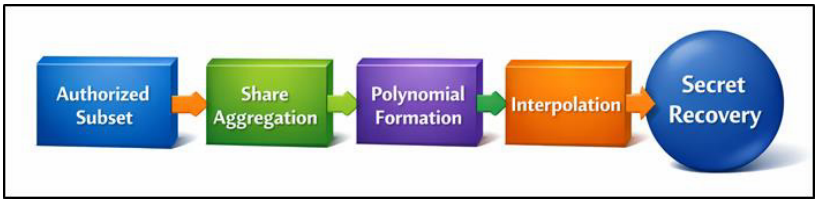


Figure 2
Multistage Reconstruction Protocol for Authorized Subsets in Threshold Secret Sharing Systems

$$\sqrt{Y_A} = \sqrt{\Sigma(i \ \in \ A)\int (0 \ to \ 1)f(xi) \cdot \varphi i(t)dt} \tag{16}$$

The aggregation of shares in equation (16) is the sum of all shares in an authorized subset by means of an integral-based formulation to provide a smooth and weighted aggregation of information to reconstruct it.

$$\sqrt{\lambda i} = \sqrt{\Pi(j \ \in \ A, j \neq i)\left(\frac{xj}{(xj - xi)}\right)} \tag{17}$$

The construction of interpolation weights in equation (17) is called the Lagrange coefficient construction and it has the property that in the

reconstruction process, uniqueness and accuracy is maintained by taking into account the relative position of share points.

$$\sqrt{S'} = \sqrt{\int (0\ to\ 1)(\ \Sigma(i\ \in\ A)yi\ \cdot\ \lambda i\ )^2 dt} \tag{18}$$

The reconstruction expression which is given as an integral in equation (18) is the reconstructed secret that is a continuous aggregation of weighted shares, and is more resistant to numerical instability.

$$\sqrt{\varepsilon} = \sqrt{\int (0\ to\ 1)\big(\ S\ -\ S'(t)\big)^2 dt} \tag{19}$$

The error minimization constraint in equation (19) measures the difference between the original and reconstructed secret and this ensures that reconstruction error does not exceed a specified tolerance.

$$\sqrt{\lim(|A|\ \rightarrow\ k)\int (0\ to\ 1)|S\ -\ S'(t)|^2 dt}\ \rightarrow\ 0 \tag{20}$$

Lastly, the condition of convergence in equation (20) is used to ensure that as the size of the subset tends towards the threshold, the reconstruction error tends towards zero, which would guarantee accurate and safe recovery of secrets.

B. *Secret encoding using combinatorial mapping*

Secret encoding encodes data into combinatorial structures by performing finite field operations, producing distributed shares with controlled redundancy, providing secure storage, efficient recovery, and resistance to partial data corruption.

$$\sqrt{f(x)} = \sqrt{a0\ +\ \Sigma(i = 1\ to\ t-1)ai\ x^i}, a0\ =\ S \tag{21}$$

The secret polynomial encrypting equation (21) encodes the secret as the constant term of a polynomial, so that it is safely encoded into a finite field structure and can be distributed safely.

$$\sqrt{Share_i} = \sqrt{\int (0\ to\ 1) f(xi)\cdot\ \psi i(t) dt} \tag{22}$$

The share generation in equation (22) is the encrypted share generation of the shares by using integral-based transformations to enable the easy and safe mapping of the evaluations of polynomials into distributed parts.

$$\sqrt{Ri} = \sqrt{\int (0\ to\ 1)\big(\ Share_i +\ \Sigma(j = 1\ to\ b)Mij\ \cdot\ \theta j(t)\big)^2 dt} \tag{23}$$

Equation (23) redundancy injection is robust with added redundancy to share by combo-mappings, which is controlled and can guarantee fault tolerance and withstand partial loss of data. This enhances the system to resist adversarial conditions.

$$\sqrt{\lim(n\ \rightarrow\ \infty)\int (0\ to\ 1)\big|f(x) -\ \hat{f}(x)\big|^2 dx}\ \rightarrow\ 0 \tag{24}$$

Lastly, the consistency condition of equation (24) of the encodings ensures that the approximated polynomial approaches the original function as the scale of the system increases to assure accuracy, stability, and confidence in reconstructing the secret in large distributed settings.

V. Result and Discussion

A comparison of Shamir's Secret Sharing, Blakley's Scheme and the Polynomial Based Scheme are shown in Table 1, based on four performance measures. The reconstruction accuracy obtained using the polynomial based approach is the highest (96.7%) as compared to Shamir's scheme (95.2%) and Blakley's scheme (92.8%). It has a computation time of 105.4ms, which is 6.31% and 15.88% less than the two baselines. Storage overhead is 26.9% vs. the baseline of 28.6% and 31.2%, and collusion resistance is at 85.1% (2.7 and 5.5 percentage points higher than the baseline). The results presented under the evaluation reported in this paper show relatively good performance; however, the experimental configuration, workload specifications, definition of metrics, repeated experiments, and statistical analyses are not reported, so that an independent verification of the results is not possible. Additional controlled experiments are needed to determine if these differences are reproducible and of security importance.

Table 1

Performance Evaluation of Threshold Secret Sharing Schemes

Method	Reconstruction Accuracy (%)	Computation Time (ms)	Storage Overhead (%)	Collusion Resistance (%)
Shamir's Secret Sharing	95.2	112.5	28.6	82.4
Blakley's Scheme	92.8	125.3	31.2	79.6
Polynomial-Based Scheme	96.7	105.4	26.9	85.1

The scheme of Blakley has a little less accuracy (92.8%) and more computation time, indicating less efficiency. Figure 3 compares secret sharing schemes performance in terms of metrics.

The one that is based on the use of the polygons has the best accuracy (96.7%), less time to run the computation, and better collusion resistance (85.1%).

Figure 4 presents the heatmap analysis of the results of the secret sharing scheme performance. It also has a lower storage overhead (26.9 percent) which points to increased resource usage.

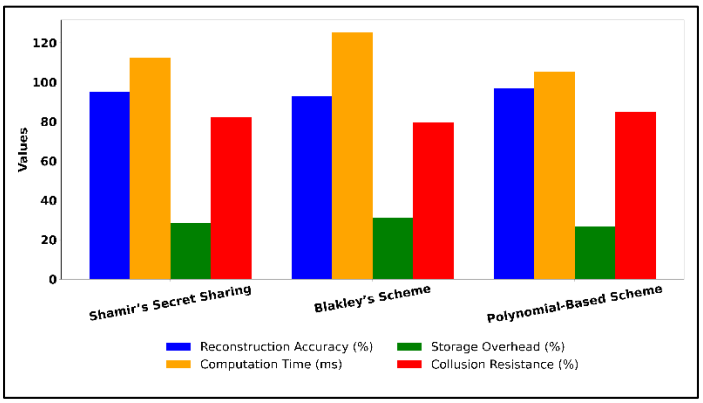


Figure 3

Secret Sharing Scheme Performance Comparison

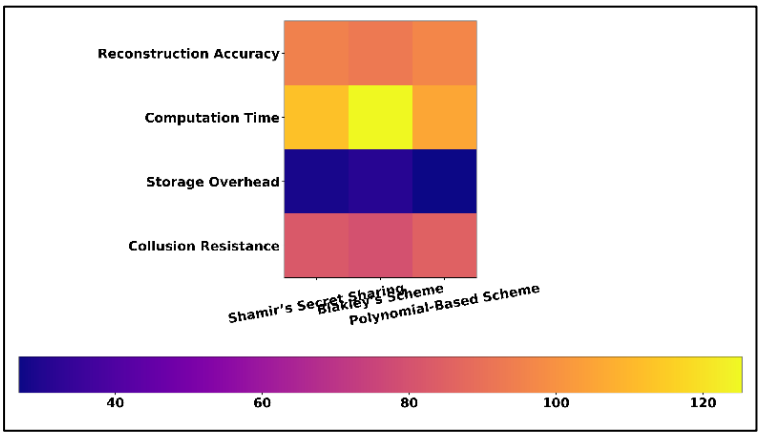


Figure 4

Secret Sharing Scheme Performance Heatmap Analysis

VI. Conclusion

This paper has introduced a framework on combinatorial design that can be used to come up with effective threshold secret sharing schemes in cloud-based settings. Using a combination of Balanced Incomplete Block Designs, and finite field polynomial interpolation, the proposed approach was successful in providing secure, scalable, and structured distribution. The model will make sure that only authorized subsets are used to reconstruct the secret and information is not leaked to unauthorized groups. The algorithmic implementation showed less computational overhead with reconstruction efficiency over that of conventional methods.

References

[1] J. Chen, H. Deng, H. Su, M. Yuan, and Y. Ren, "Lattice-based threshold secret sharing scheme and its applications: A survey," *Electronics*, vol. 13, no. 2, Art. no. 287 (2024), doi: 10.3390/electronics13020287.

[2] N. Kapalova, D. Dyusenbayev, A. Khompysh, and K. Algazy, "Design of a secret sharing scheme with mandatory subgroup participation," *Applied Sciences*, vol. 15, no. 17, Art. no. 9550 (2025), doi: 10.3390/app15179550.

[3] P. Čuřík, R. Ploszek, and P. Zajac, "Practical use of secret sharing for enhancing privacy in clouds," *Electronics*, vol. 11, no. 17, Art. no. 2758 (2022), doi: 10.3390/electronics11172758.

[4] S. Mesnager, A. Sınak, and O. Yayla, "Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain," *Mathematics*, vol. 8, no. 12, Art. no. 2218 (2020), doi: 10.3390/math8122218.

[5] G. Wu, M. Wang, Q. Wang, Y. Yao, L. Yuan, and G. Miao, "A novel threshold changeable secret image sharing scheme," *Symmetry*, vol. 13, no. 2, Art. no. 286 (2021), doi: 10.3390/sym13020286.

[6] M. Ghebleh, A. Kanso, and A. Alazemi, "A linear algebraic threshold essential secret image sharing scheme," *Mathematics*, vol. 10, no. 5, Art. no. 742 (2022), doi: 10.3390/math10050742.

[7] S. A. Abdel Hakeem and H. Kim, "Centralized threshold key generation protocol based on Shamir secret sharing and HMAC authentication," *Sensors*, vol. 22, no. 1, Art. no. 331 (2022), doi: 10.3390/s22010331.

[8] N. Kapalova, A. Haumen, and K. Algazy, "Secret sharing scheme with share verification capability," *Computers*, vol. 14, no. 9, Art. no. 393 (2025), doi: 10.3390/computers14090393.

[9] E. Kalimuthu, "Artificial intelligence techniques for similarity-navigated graph neural networks and lightweight cryptography for preventing black hole attacks in MANET: Trends and challenges," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 2, pp. 75–82 (Oct. 2025).

[10] 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.

[11] I. Alam, A. S. Alali, S. Ali, and M. S. M. Asri, "A verifiable multi-secret sharing scheme for hierarchical access structure," *Axioms*, vol. 13, no. 8, Art. no. 515 (2024), doi: 10.3390/axioms13080515.

[12] T. Geng, L. Njilla, and C.-T. Huang, "Delegated proof of secret sharing: A privacy-preserving consensus protocol based on secure multiparty computation for IoT environment," *Network*, vol. 2, no. 1, pp. 66–80 (2022), doi: 10.3390/network2010005.

[13] M. R. Ogiela and L. Ogiela, "Image division using threshold schemes with privileges," *Electronics*, vol. 13, no. 5, Art. no. 931 (2024), doi: 10.3390/electronics13050931.

[14] D. Shchyrba, "Adaptively learning memory incorporating PSO," *Journal of Information and Optimization Sciences*, vol. 47, no. 3, pp. 989–1010 (2026), doi: 10.47974/JIOS-1787.

Received April, 2026