International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT23902102

A Secured Data Storage in Cloud Computing by Using Block Design Based Key Agreement

Kamparapu Bhanu Rajesh Naidu[1], M V Anjana Devi[2], Pragathi Vulpala[3], Dr. Mahesh Kotha[4]

[1]Assistant Professor, Department of Computer Science &Technology, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India

[2]Associate Professor, CSE(AI&ML) Department, Guru Nanak Institutions Technical Campus, Hyderabad, India

[3]Assistant Professor, CSE Department, TKR college of engineering and technology, Hyderabad, India

[4]Associate Professor, Department of CSE (AI&ML), CMR Technical Campus, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 10 July 2023

Published: 28 July 2023

Publication Issue

Volume 9, Issue 4

July-August-2023

Page Number

231-240

ABSTRACT

Cloud computing has emerged as a dominant paradigm for storing and accessing data. In group data sharing scenarios, where multiple users collaborate and exchange sensitive information in the cloud, ensuring secure and efficient key agreement becomes crucial. This paper presents a comprehensive analysis of key agreement mechanisms for group data sharing in cloud computing environments. We explore various cryptographic techniques and protocols specifically designed for establishing secure communication channels among group members. The paper discusses the challenges associated with key agreement in the cloud, proposes potential solutions, and provides insights into the implementation and evaluation of such mechanisms. The proposed framework aims to protect data confidentiality, integrity, and availability, ensuring a robust and reliable cloud storage environment. We explore various cryptographic techniques, including encryption, key management, and authentication mechanisms, and discuss their application in securing cloud-based data storage. The framework addresses common security threats and provides guidelines for implementing a secure cloud storage solution.

Keywords: Key Agreement Protocol, Symmetric Balanced Incomplete Block Design, Data Sharing, Cloud Computing.

I. INTRODUCTION

Group data sharing in cloud computing offers tremendous opportunities for collaboration and knowledge exchange. However, it also poses significant challenges in terms of security, privacy, access control, and scalability. By implementing effective key agreement mechanisms, employing strong encryption algorithms, and ensuring proper access control and authentication mechanisms, organizations can establish secure group data sharing environments in the cloud. Continued research and

innovation in this field are necessary to address emerging challenges and further enhance the security and efficiency of group data sharing in cloud computing.

Cloud computing has revolutionized the way data is stored, processed, and shared among individuals and organizations. In various domains such as collaborative research projects, enterprise data sharing, and healthcare information exchange, group data sharing plays a pivotal role. Group data sharing in cloud computing refers to the collaborative sharing of data among multiple users within a defined group or community. It enables efficient collaboration, streamlined workflows, and enhanced productivity.

Challenges in Group Data Sharing:

While group data sharing offers numerous benefits, it also introduces several challenges related to security, privacy, access control, and scalability. Some of the key challenges include:

Security: Ensuring the confidentiality, integrity, and availability of shared data is crucial. Unauthorized access, data breaches, and insider threats pose significant risks to sensitive information shared within the group.

Privacy: Group data sharing requires careful consideration of privacy concerns. Users may have different privacy requirements, and mechanisms should be in place to protect individual data while enabling effective collaboration.

Access Control: Managing access permissions for shared data becomes complex in group settings. Fine-grained access control policies, user authentication, and authorization mechanisms need to be implemented to ensure that only authorized group members can access specific data.

Key Agreement: Establishing secure communication channels among group members is essential for secure data sharing. Key agreement mechanisms need to be implemented to generate and distribute cryptographic keys that enable secure encryption and decryption operations.

Scalability: As the number of group members and shared data grows, scalability becomes a significant concern. The system should be able to handle the increased load and accommodate the dynamic addition or removal of group members.

Key Agreement Mechanisms for Group Data Sharing:

Key agreement mechanisms play a crucial role in ensuring secure communication and data sharing within groups. Some commonly used mechanisms include:

Symmetric Key Agreement: In this approach, a shared secret key is pre-distributed to all group members. This key is used for encryption and decryption operations, ensuring secure communication within the group. Key pre-distribution schemes and key tree-based approaches are commonly used in symmetric key agreement.

Asymmetric Key Agreement: This approach utilizes public-key cryptography, where each user possesses a public-private key pair. Public keys are shared with other group members, and secure communication channels are established using various group key agreement protocols. Public Key Infrastructure (PKI) is commonly employed for managing public keys and enabling secure communication.

Implementation Considerations:

Implementing group data sharing in cloud computing requires careful consideration of the following aspects:

System Architecture: The architecture should support the secure storage, retrieval, and sharing of data among group members. It should include components for user authentication, access control, and key management.

Cryptographic Algorithms: The selection of appropriate cryptographic algorithms for encryption, decryption, and key agreement is crucial. Algorithms with strong security properties and efficient performance should be chosen based on the specific requirements of the group data sharing scenario.

Scalability and Performance: The system should be designed to handle a growing number of group members and increasing data volumes. Efficient algorithms and optimized data storage and retrieval mechanisms should be employed to ensure scalability and performance.

Security Analysis: A comprehensive security analysis should be conducted to identify potential vulnerabilities and mitigate risks. Threat modeling, risk assessment, and regular security audits should be performed to maintain a robust and secure group data sharing environment.

2.REALTED WORKS

There have been several existing works and research efforts focused on addressing the challenges and improving group data sharing in cloud computing environments. Here are some notable works in this field:

"A Secure and Efficient Group Data Sharing Scheme for Cloud Storage" by Li et al. (2014): This work proposes a secure and efficient group data sharing scheme that utilizes attribute-based encryption (ABE) to provide fine-grained access control and confidentiality for shared data in the cloud. The scheme enables dynamic group membership and revocation of user access privileges.

"Group Key Management for Secure Group Data Sharing in Cloud Computing" by Sharma et al. (2016): The paper presents a group key management scheme that utilizes a hierarchical structure for secure group data sharing in the cloud. The scheme efficiently manages group keys, supports dynamic group membership, and enables secure communication among group members.

"Secure Data Sharing in Cloud Computing Using Proxy Re-encryption" by Zeng et al. (2017): This work introduces a secure data sharing scheme based on proxy re-encryption (PRE) for group data sharing in the cloud. The scheme enables a data owner to delegate access rights to multiple users while maintaining data confidentiality and integrity.

"Efficient and Secure Group Data Sharing in Cloud Computing Using Proxy Re-encryption" by Wang et al. (2018): The paper proposes an efficient and secure group data sharing scheme that combines proxy re-encryption and elliptic curve cryptography (ECC). The scheme provides secure and fine-grained access control for group data sharing in the cloud.

"Privacy-Preserving Group Data Sharing in Cloud Computing" by Wu et al. (2019): This work presents a privacy-preserving group data sharing scheme that utilizes homomorphic encryption and secure multi-party computation techniques. The scheme ensures privacy protection while allowing group members to perform collaborative computations on shared data in the cloud.

"Secure and Efficient Group Data Sharing with Dynamic Policy Updating in Cloud Computing" by Wang et al. (2020): The paper proposes a secure and efficient group data sharing scheme that supports dynamic policy updating in cloud computing environments. The scheme combines attribute-based

encryption and proxy re-encryption to achieve fine-grained access control and efficient key management.

These works, among others, contribute to the development of secure and efficient group data sharing mechanisms in cloud computing. They address various aspects such as access control, confidentiality, integrity, scalability, and privacy to provide robust solutions for collaborative data sharing scenarios. Continued research in this field is essential to address emerging challenges and ensure the effective and secure sharing of data among groups in the cloud.

The key agreement protocol is relevant to promote data sharing in cloud computing for the following reasons, which are motivated by the aforementioned observation.

1. A public channel, appropriate for cloud computing settings, is used to generate a shared conference key.
2. 2. Where data sharing occurs in a many-to-many pattern, the key agreement protocol may allow and offer safe data sharing for various data owners within a group. The many-to-many pattern of group data sharing offers more efficiency in the setting of cooperative storage when compared to the one-to-many design.
3. 3. The key agreement protocol is built on a decentralised approach, which eliminates the need for a reliable third party. This implies that each data owner in a group equitably participates and chooses the shared conference key, ensuring that all data owners in a group have control over the outsourced data.

3.WORKING MODELS

When it comes to proposed approaches for group data sharing in cloud computing, several techniques and mechanisms have been suggested to address the challenges and ensure secure and efficient collaboration among group members. Here are some proposed approaches:

Attribute-Based Encryption (ABE):
ABE is a cryptographic technique that allows fine-grained access control based on user attributes. It enables data owners to encrypt data using a set of attributes, and only users possessing the required attributes can decrypt and access the data. ABE provides flexibility in defining access policies and is well-suited for group data sharing scenarios where different users may have varying access privileges.

Proxy Re-encryption (PRE):
PRE is a cryptographic mechanism that allows a trusted third-party (the proxy) to transform ciphertexts encrypted under one key into ciphertexts encrypting the same message under a different key. In the context of group data sharing, PRE enables data owners to delegate access rights to other group members without revealing the underlying plaintext. This approach ensures confidentiality and fine-grained control over shared data.

Key Hierarchy and Management:
In group data sharing, a key hierarchy can be established to manage access control and ensure secure communication. A group key is shared among all members, while individual keys are derived from the group key for secure data encryption and decryption operations. Key management protocols, such as key distribution, revocation, and updates, play a vital role in maintaining the security and integrity of the shared data.

Secret Sharing:
Secret sharing is a technique where a secret is divided into multiple shares and distributed among group members. Only when a threshold number of shares are combined, the original secret can be reconstructed. This approach ensures data confidentiality and protects against single-point vulnerabilities. Secret sharing

schemes can be employed for secure storage and sharing of sensitive information in the cloud.

Homomorphic Encryption:
Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. This approach enables group members to perform collaborative computations on shared data while preserving privacy and confidentiality. Homomorphic encryption schemes can be leveraged to enable secure data processing and analysis in group data sharing scenarios.

Blockchain Technology:
Blockchain technology provides a decentralized and tamper-resistant platform for group data sharing. It ensures transparency, integrity, and accountability in data transactions among group members. Blockchain-based approaches can be utilized for secure and auditable data sharing, especially in scenarios where trust and data provenance are crucial.

Secure Multi-Party Computation (SMPC):
SMPC allows multiple parties to jointly perform computations on their private data without revealing individual inputs. This approach ensures privacy and confidentiality in group data sharing scenarios. SMPC techniques can be used to perform collaborative analyses and computations on sensitive data while preserving data privacy.

These proposed approaches offer different perspectives and solutions for group data sharing in cloud computing. Depending on the specific requirements and constraints of the application domain, a combination of these approaches or customized variations can be adopted to achieve secure and efficient group data sharing in the cloud. Continued research and innovation in this field are crucial to address evolving challenges and cater to diverse collaboration scenarios.

4.BLOCKCHAIN TECHNOLOGY FOR GROUP DATA SHARING IN CLOUD COMPUTING

Blockchain technology has gained significant attention in recent years due to its potential to enhance security, transparency, and accountability in various domains. When applied to group data sharing in cloud computing, blockchain can offer several advantages. Here are some key aspects of utilizing blockchain technology for group data sharing in cloud computing:

Data Integrity and Immutability: Blockchain provides a decentralized and tamper-resistant ledger, ensuring the integrity and immutability of shared data. Each transaction or data update is recorded as a block and linked to the previous blocks, creating an immutable chain. This characteristic ensures that group data remains unchanged and can be audited, providing a reliable and trustworthy platform for collaboration.

Decentralized Trust and Consensus: Blockchain eliminates the need for a central authority or trusted third party to validate transactions. The decentralized nature of blockchain allows group members to collectively maintain and validate the integrity of shared data. Consensus mechanisms, such as proof-of-work or proof-of-stake, enable agreement among participants on the validity and ordering of transactions, enhancing trust and mitigating the risk of data manipulation.

Access Control and Data Privacy: Blockchain can provide granular access control mechanisms for group data sharing. Smart contracts, self-executing code deployed on the blockchain, can define access rules and permissions for different group members. This ensures that only authorized participants can access and modify the shared data. Moreover, blockchain's transparent yet pseudonymous nature preserves data privacy by associating transactions with cryptographic keys rather than revealing personal identifiers.

Auditability and Accountability: Blockchain's transparent and immutable nature allows for easy auditability of group data sharing activities. Each transaction or data modification is recorded on the blockchain, providing an audit trail that can be reviewed and verified by authorized entities. This facilitates accountability within the group, enabling participants to trace the history of shared data and identify the responsible parties for any changes or breaches.

Smart Contract Execution: Smart contracts can facilitate automated execution of predefined rules and conditions for group data sharing. These self-executing contracts can enforce access control policies, trigger actions based on specific events, and ensure compliance with predefined agreements. Smart contracts enable secure and automated data sharing workflows, reducing the need for manual intervention and enhancing efficiency.

Data Consistency and Synchronization: Blockchain can address the challenge of data consistency and synchronization among group members. By maintaining a shared and distributed ledger, blockchain provides a single source of truth for all participants. Data updates are recorded in a decentralized manner, ensuring that all participants have the most up-to-date and consistent view of the shared data, eliminating the need for centralized data repositories and potential data inconsistencies.

While blockchain technology offers significant benefits for group data sharing in cloud computing, it is essential to consider its limitations, such as scalability, performance, and energy consumption. Blockchain implementations may require trade-offs between decentralization, performance, and storage requirements. Careful design and optimization are necessary to strike a balance between security, efficiency, and scalability in real-world group data sharing scenarios. Nonetheless, blockchain technology has the potential to revolutionize group data sharing in the cloud by providing enhanced security, transparency, and trust among group members.

5.BLOCK DESIGN BASED KEY AGREEMENT FOR GROUP DATA SHARING

Block design-based key agreement for group data sharing in cloud computing is an innovative approach that leverages the principles of block design theory to establish secure communication channels and enable efficient sharing of data among group members. This approach addresses the challenges of key management, access control, and confidentiality in group data sharing scenarios. Here are the key aspects of the block design-based key agreement for group data sharing:

Block Design Theory:
Block design theory is a mathematical framework that deals with the construction of designs or arrangements of elements into blocks. In the context of key agreement for group data sharing, block design theory provides a systematic approach to generate secret keys and distribute them among group members. It ensures that each member possesses a unique key and that the keys collectively form a robust and secure structure.

Key Generation and Distribution: Using block design theory, secret keys are generated based on the design's structure. The design specifies the number of blocks, the block size, and the relationship between the blocks. Each block corresponds to a unique key. These keys are distributed to the respective group members based on the design configuration, ensuring that each member has a distinct key for secure communication.

Access Control and Confidentiality: The block design-based key agreement approach enables fine-grained access control and confidentiality in group data sharing. Each key corresponds to a specific block, and the access permissions of a group member are determined by their possession of the corresponding

key. Only members with the correct keys can decrypt and access the shared data, ensuring confidentiality and restricting unauthorized access.

Key Revocation and Update: The block design structure allows for efficient key revocation and update mechanisms. When a group member needs to be revoked or added, the block design can be modified accordingly, and new keys can be generated and distributed to the relevant members. This ensures that revoked members no longer have access to the shared data, while new members are securely incorporated into the group data sharing framework.

Scalability and Efficiency: Block design-based key agreement offers scalability and efficiency benefits. The design structure enables the system to handle a large number of group members and shared data without significant overhead. Key distribution, revocation, and update operations can be performed efficiently, ensuring the system's responsiveness and enabling seamless group data sharing even in dynamic environments.

Security and Resilience: The block design-based approach provides a secure foundation for group data sharing. The use of unique keys corresponding to specific blocks enhances the security of the system, as compromised keys only affect the associated block and do not jeopardize the security of the entire group. Additionally, the block design structure offers resilience against attacks, as compromising a limited number of keys does not compromise the security of other keys or shared data.

By applying block design theory, the block design-based key agreement approach provides a systematic and secure method for group data sharing in cloud computing. It ensures efficient key management, access control, and confidentiality while maintaining scalability and security. This approach offers a promising solution for organizations and individuals seeking secure and collaborative data sharing in cloud computing environments.

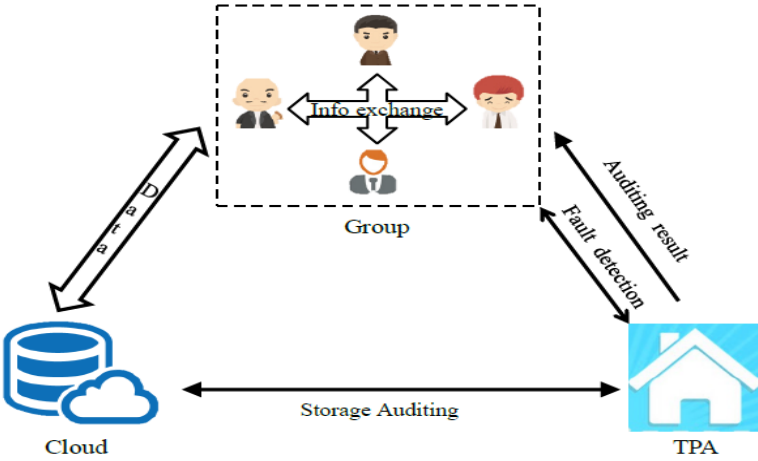

Fig. 1: System model of data sharing in cloud computing.

A trustworthy third party is not necessary because the group data sharing architecture is based on the SBIBD. To establish a single conference key in this approach, all participants exchange messages from intended entities in accordance with the SBIBD's structure. The protocol that is being discussed includes participants, volunteers, and adversaries as well. Each of these entities operates as a probabilistic polynomial-time Turing computer. Passive and active opponents both have a chance of being involved in the protocol.

A passive enemy is someone who listens in on the multicast channel in an effort to obtain the conference key, whereas an active adversary tries to impersonate a member or disrupt a conference. It should be noted that the participants generate and update the key. The participants may also verify the accuracy of the shared conference key thanks to our protocol's fault tolerance feature. Since storage auditing can adhere to modern auditing protocols (such as those found in [25]), we restrict our attention in this study to the design of group data sharing schemes for cloud computing.

Algorithm 1 Generation of a $(v, k+1, 1)$-design

```
for i = 0; i ≤ k; i++ do
  for j = 0; j ≤ k; j++ do
    if j == 0 then
      B_{i,j} = 0;
    else
      B_{i,j} = ik + j;
    end if
  end for
end for
for i = k + 1; i ≤ k^2 + k; i++ do
  for j = 0; j ≤ k; j++ do
    if j == 0 then
      B_{i,j} = ⌊(i − 1)/k⌋;
    else
      B_{i,j} = jk+1+MOD_k(i−j+(j−1)⌊(i −
    end if
  end for
end for
```

Multiple users can freely share the group data in cloud computing, increasing the effectiveness of work in collaborative settings and opening up a wide range of possible applications. However, there are significant issues in how to effectively communicate the outsourced data across a group while maintaining data security. Note that with cloud computing, group data sharing has been made safe and effective thanks in large part to key agreement protocols. In this paper, we present a novel block design-based key agreement protocol that supports multiple participants and can flexibly increase the number of participants in a cloud environment according to the block design's structure by utilising the symmetric balanced incomplete block design.

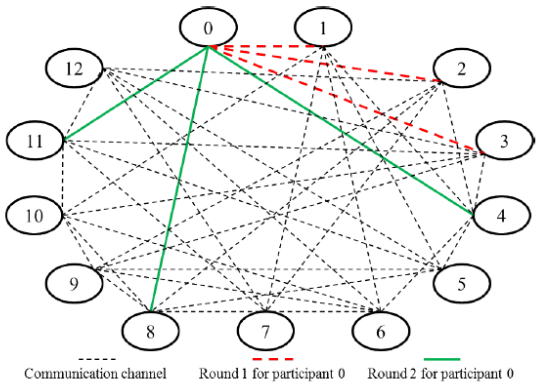

Fig 2. Design group data sharing model

A key agreement protocol may be used in cloud computing to promote safe and effective data sharing by generating a shared conference key for numerous participants to assure the security of their subsequent interactions. The key agreement protocol has evolved into one of the most important cryptographic primitives since Diffie-Hellman first described it in their landmark article [4].

The issue of establishing a shared secret key between two participants is effectively solved by the Diffie-Hellman protocol's fundamental version. A key agreement protocol in cryptography is a means for two or more parties to agree on a key so that both have an impact on the result.

The conferees can securely transmit and receive communications from one another using the shared conference key they pre-agree upon by utilising the key agreement protocol. A secure key agreement protocol, in particular, makes sure that the attacker cannot access the created key by executing malicious operations like eavesdropping.

In interactive communication situations with high security demands, such as remote board meetings, teleconferences, collaborative workspaces, radio frequency identification [5], cloud computing, and others, the key agreement protocol can thus be widely employed.

By expanding the SBIBD structure to allow many participants, we provide an effective and safe block design-based key agreement protocol in this work. This protocol enables numerous data owners to freely share the outsourced data with high levels of security and efficiency. To allow group data sharing in cloud computing, the SBIBD is built as the group data sharing paradigm. Additionally, the protocol can offer fault tolerance and authentication services. The following is a summary of this paper's significant contributions.

1. A model of group data sharing based on the SBIBD's structure is created. Based on the description of the SBIBD, a group data sharing model is created in this study and may be used to decide how members will communicate with one another. The standard formulae for computing the shared conference key for numerous participants are derived from mathematical representations of the SBIBD structure.
2. 2. The protocol may provide fault tolerance and fault detection. The proposed protocol has fault detection capabilities to guarantee that a shared conference key is successfully created among all participants. In order to support the fault tolerance attribute, a volunteer will be utilised to substitute a malicious participant during the fault detection phase.
3. The volunteer makes the protocol resistant to certain key assaults [7], which increases the security of group data sharing in cloud computing.
4. 3. The protocol may be able to facilitate safe group data exchange in the cloud. The SBIBD-based data sharing concept suggests that several players can come together to effectively share the outsourced data. The security of the group data that has been outsourced is then ensured by each member of the group performing the key agreement to create a shared conference key. It should be noted that only group members can create the shared conference key. The created key is not accessible to attackers or the semi-trusted cloud server.

As a result, they are unable to access the actual data that was outsourced (and instead only receive some gibberish). The suggested key agreement protocol can therefore allow efficient and safe group data sharing in cloud computing.

6.CONLCUSION

Group data sharing in cloud computing has expanded the utility of computer networks as a result of advancements in Internet and cryptography technologies. The conference key agreement protocol may significantly increase the efficiency and security of group data sharing in cloud computing. In particular, the shared conference key encryption protects the outsourced data of the data owners from the attacks of adversaries. The conference key agreement provides advantages of increased safety and dependability compared to conference key distribution. The conference major agreement calls for greater system information exchange and higher computational costs, nevertheless. The SBIBD is used in the protocol design to address the issues with the conference key agreement. In this work, we introduce a unique key agreement technique based on block architecture that facilitates group data sharing in cloud computing. Multiple participants may be included in the protocol thanks to the definition and mathematical descriptions of the structure of a (v; k + 1; 1)- design, and generic formulae for the shared conference key for participants are obtained. Additionally, the inclusion of volunteers makes it possible for the provided protocol to support the fault tolerance attribute, making it more useful and secure. In our upcoming work, we hope to add more qualities to our protocol, such as anonymity and traceability, to make it more adaptable to other situations.

II. REFERENCES

[1]. B. Dan and M. Franklin, “Identity-based encryption from the Weill pairing,” Siam Journal on Computing, vol. 32, no. 3, pp. 213–229, 2003.

[2]. S. Blakewilson, D. Johnson, and A. Menezes, “Key agreement protocols and their security analysis,” in IMA International Conference on Cryptography and Coding, 1997, pp. 30–45.

[3]. I. Chung and Y. Bae, “The design of an efficient load balancing algorithm employing block design,” Journal of Applied Mathematics and Computing, vol. 14, no. 1, pp. 343–351, 2004.

[4]. O. Lee, S. Yoo, B. Park, and I. Chung, "The design and analysis of an efficient load balancing algorithm employing the symmetric balanced incomplete block design." Information Sciences, vol. 176, no. 15, pp. 2148–2160, 2006.

[5]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[6]. Ravindra Changala, "Secured Activity Based Authentication System" in " in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[7]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[8]. H. Guo, Z. Li, Y. Mu, and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," Computers and Security, vol. 27, no. 1-2, pp. 16–21, 2008.

[9]. Z. Tan, "An enhanced three-party authentication key exchange protocol for mobile commerce environments," Journal of Communications, vol. 5, no. 5, pp. 436–443, 2010.

[10]. Y. M. Tseng, "An efficient two-party identity-based key exchange protocol." Informatica, vol. 18, no. 1, pp. 125–136, 2007.

[11]. Ravindra Changala, "Retrieval of Valid Information from Clustered and Distributed Databases" in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1, Pages 21-25, September 2016.ISSN: 2455-3506.

[12]. A. Shamir, "Identity-based cryptosystems and signature schemes," Lecture Notes in Computer Science, vol. 21, no. 2, pp. 47–53, 1985.

[13]. E. Bresson, O. Chevassut, D. Pointcheval, and J. J. Quisquater,"Provably authenticated group diffie-hellman key exchange," AcmTransactions on Information and System Security, vol. 10, no. 3, pp.89–92, 2001.

[14]. Ravindra Changala, "Diminution of Deployment Issues in Secure Multicast System with Group Key Management" published in International Journal of Computer Application (IJCA), Impact Factor 2.52, ISSN No: 2250-1797, Volume 2, Issue 3, June 2012.

[15]. D. R. Stinson, Combinatorial designs: constructions and analysis. Springer Science and Business Media, 2007.

Cite this article as :

Kamparapu Bhanu Rajesh Naidu, M V Anjana Devi, Pragathi Vulpala, Dr. Mahesh Kotha, "A Secured Data Storage in Cloud Computing by Using Block Design Based Key Agreement", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.231-240, July-August-2023. Available at doi : https://doi.org/10.32628/CSEIT23902102
Journal URL : https://ijsrcseit.com/CSEIT23902102