International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Cryptanalysis of an Anonymous and Traceable Group Data Sharing in Cloud Computing

K Kartik[1], Pravesh Yadav[2], Dr. Madhumita K[3]

[1,2,3]Department of Computing Technologies SRM Institute of Science and Technology
[1]kk1024@srmist.edu.in, [2]py7024@srmist.edu.in, [3]madhumik1@srmist.edu.in

Abstract

In Cloud Environments, Group Data Sharing Has Emerged As A Significant Area Of Research Due To The Increasing Demand For Collaborative and Distributed Workflows. Ensuring That Data Is Shared Securely and Efficiently Among Multiple Participants Without Compromising Privacy and Traceability Remains An Urgent Challenge. Recently, Researchers Proposed An Anonymous And Traceable Group Data Sharing Scheme Aimed At Resolving This Issue. This Scheme Utilizes A Group Signature Mechanism As Its Core Building Block, Providing Both Anonymity And Traceability, Thereby Addressing The Conflicting Requirements Of Privacy And Accountability.The Practical Implementation Of Such Schemes Brings New Concerns About Their Security And Performance In Real-World Scenarios. In This Study, We Critically Analyze The security underpinnings of their group signature scheme, detecting possible weaknesses that might jeopardise the availability, confidentiality, or integrity of shared data in the cloud. Additionally, we investigate the efficiency and scalability of the suggested scheme, assessing its appropriateness for large-scale applications where high throughput and resource constraints are crucial factors.The advancement of the design of strong group data sharing models that can balance traceability, efficiency, and privacy in cloud computing environments is facilitated by these contributions

Keywords— Cloud Data Sharing, Anonymous group signature, Security Analysis.

1. INTRODUCTION

Shen et al. proposed the anonymous and traceable group data participating scheme for pall computing. In order to support anonymous multiple addicts in public murk, their plan uses a group hand as the structural block. According to their plan, group members can communicate anonymously regarding the group hand, and if needed, the group director can track down each member's true identity. The verifier can easily determine whether a group hand is created by a legitimate member, and the group director has the authority to remove a member.

1.1 Motivation

Cloud computing's rapid expansion has revolutionised data storage, participation, and access, making it a crucial component of the ultramodern digital architecture. The need for safe, private, and efficient data-sharing systems has increased as organisations and individuals rely less on cloud services for

collaboration and data exchange. Protecting participant information and sensitive user identities from unwanted access is essential in situations involving group data participation. While traceability is necessary to hold individuals accountable for vicious conditioning or breaches, anonymity guarantees that users' private information is kept private. These qualities are essential for building trust, guaranteeing adherence to data protection laws, and promoting the widespread release of results that are grounded in reality for both personal and professional use..

1.2 Problem Statement

Cloud surroundings pose unique challenges in achieving secure and effective data- sharing capabilities. Conventional data- sharing styles frequently fail to address critical aspects, similar as maintaining a balance between sequestration and responsibility. While some results emphasize obscurity, they may warrant traceability, making it delicate to address security breaches or unauthorized conditioning. Again, systems designed for traceability may inadvertently compromise stoner sequestration. also, icing effectiveness and scalability in group data- participating schemes is grueling , particularly when dealing with large- scale operations where computational and communication outflow must be minimized. This underscores the critical need for innovative results that can give robust security, stoner obscurity, traceability, and functional effectiveness within pall- grounded ecosystems.

1.3 Objective

The objective of this exploration is to design, apply, and estimate a cryptographic group data-participating scheme that addresses the limitations of being results. The pretensions of this exploration include

Facilitating secure and anonymous communication among group members to cover their individualities while participating data. enforcing traceability features that allow the group director or authorized realities to identify druggies in cases of controversies or vicious conditioning.

Developing a medium to drop unauthorized druggies without dismembering the functionality of the group or compromising its security. Ensuring that the scheme is effective, scalable, and suitable for deployment in real- world pall surroundings with different stoner groups and varying data participating requirements.

Contributing to the advancement of secure and sequestration- conserving technologies for cloud computing operations.

1.4 Scope

The design, analysis, and validation of a traceable, anonymous group data-participation scheme tailored to pall computing environments are all included in the scope of this investigation. The study concentrates on important elements like cancellation procedures, group hand mechanisms, and cryptographic ways to insure robust security and sequestration. The findings will profit diligence similar as healthcare, finance, and government, where secure and anonymous data sharing is consummate. While the exploration primarily addresses cloud surroundings, its principles and methodologies can also be extended to other distributed systems taking secure group communication. The boundaries of this exploration are defined by its focus on theoretical and practical aspects of cryptographic group data sharing. While the study provides a robust foundation, it does n't claw deeply into stoner interface design,non-cloud operations, or tackle- specific optimizations. unborn work may

explore integrating these aspects for a further comprehensive result.

2. RELATED WORKS

Group data sharing and secure communication in pall surroundings have been considerably studied due to the adding demand for sequestration- conserving and effective data- sharing mechanisms. Bellare et al. laid the theoretical foundation for group autographs, defining formal conditions for obscurity and traceability while furnishing a construction grounded on general cryptographic hypotheticals. structure on this, Boneh et al. introduced short group hand schemes to enhance security in operations like vehicular ad hoc networks(VANETs), addressing the challenges of sequestration and denial- of- service attacks. Chaum and van Heyst proposed a group hand scheme emphasizing effectiveness and minimum commerce during the stoner enrollment process, paving the way for scalable systems. More lately, Shen et al. proposed an anonymous and traceable group data- participating scheme acclimatized for pall computing, which employs crucial agreement and group autographs to insure secure and effective communication. also, Yu et al. addressed the issue of crucial- exposure in pall storehouse auditing, presenting a new protocol that ensures forward security and adaptability against implicit attacks. These workshop inclusively punctuate the elaboration of secure group data- participating results, emphasizing the need for balancing sequestration, traceability, and effectiveness in dynamic and cooperative surroundings like pall computing.

[1] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptionsThe theoretical underpinnings of the group hand primitive are presented in this paper. We present rigorous, formal definitions for the fundamental requirements of traceability and obscurity. We also demonstrate how these simplify and unify the conditions for this primitive by illustrating the extensive collection of sometimes ambiguous informal conditions found in the literature. Finally, based only on the assumption that trapdoor permutations exist, we demonstrate the existence of a construct that satisfies our delineations.

[2] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Annu. Int. Cryptol. Conf., 2004,
pp. 41–55.

The security of Vehicular Ad Hoc Networks(VANETs) plays a crucial part in guarding against bogus and vicious dispatches, misusing at roads, wiretapping etc. currently, common cryptographic results guarantee communication integrity, authentication,non-repudiation and sequestration which is needed as a serious demand in VANETs due to the possibility of shadowing of motorists by vicious spectators. The affiliated and previous workshop insure security and sequestration. nonetheless, the effectiveness of these schemes is generally low or there's the possibility of denial of services attacks. The main thing of our paper is to give original design of a scheme which ensures sequestration, security and effectiveness. The proposed scheme can also cover against several Denial of Services Attacks. We compare our proposed result with affiliated results and outline the evaluation of our scheme.

[3] D. Chaum and E. van Heyst, "Group signatures," in Proc. EUROCRYPT, Brighton, U.K., 1991, pp. 257–265.

An introductory sequestration tool is a group hand. One essential component of such a scheme is the

group joining operation. Up until now, every secure group hand scheme has either used a join operation backed by a trusted party or a sophisticated joining protocol that involves multiple relationships between the Group Manager (GM) and the potential stoner. Furthermore, no successful plan used a join protocol that has been shown to be safe from attackers who can successfully launch several concurrent join sessions during an attack. With a straightforward joining protocol based on a "single communication and hand response" exchange between the potential stoner and the GM, this work offers the first successful group hand scheme. This hand-response and single- communication enrolment paradigm, in which no additional actions are taken, is the best possible join commerce, which Camenisch and Stadler first mentioned in 1997. However, its effective externalisation hasn't been closed as of yet. For example, drug dealers can easily join by a constable because joining has two short communication overflows and lacks secure channels (a security officer of a company can shoot a train with all enrolment requests in his company and get back their instruments for distribution back to members of the company).

[4] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 912–925, Apr. 2018.

In the last few years, group data participation in pall environments has become popular. With the popularity of cloud computing, one of the most important questions that needs to be addressed is how to accomplish safe and efficient data participation in pall environments. Another problem in the pall for data sharing is how to accomplish both traceability and obscurity. The main goal of this paper is to enable anonymous data sharing and storage for the same group in the pall with high security and efficacy. A new traceable group data participating scheme is proposed to support anonymous multiple drug users in public shadows by utilising the crucial agreement and the group hand. Members of the group are able to speak anonymously about the group on the one hand, and theIf required, the true identities of the members can be located. However, based on the important agreement, a common conference key is inferred to allow group members to participate and safely store their data. It should be noted that crucial generation uses a symmetric balanced deficient block design, which primarily lessens the load on members to choose a shared conference key..

[5]J. Yu, K. Ren, C. Wang and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance", IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167-1179, Jun. 2015.

Examining cloud storage facilities is regarded as a crucial advantage to confirm the accuracy of the data in the open cloud. The assumption behind all current reviewing conventions is that the customer's mystery key for examination is totally safe. However, because of the client's potentially weak sense of security and/or moo security settings, comparative assumptions may not be maintained over time.But the majority of the existing review practices would inevitably become ineffective if such a mystery key for examination is exposed. In this paper, we focus on this contemporary viewpoint of inspecting cloud storage facilities. We investigate

ways to reduce the damage caused by the customer's critical presentation in the examination of the pall storage facility and provide the first practical solution for this contemporary problem scenario. We suggest such a convention and formalise the security show and portrayal of reviewing convention with considerable presentation flexibility. In our plan, we modernise the mystery keys for the client by using

the preorder traversal mould and the twofold tree structure. In order to strengthen forward security and the attribute of blockless unquestionable status, we also develop a contemporary authenticator. According to the execution investigation and security proof, our suggested convention is convincing and safe..

3. SYSTEM ANALYSIS

The existing cloud-based data-sharing systems focus on fundamental functionalities like storing, retrieving, and s

3.1 Existing System

The existing cloud- based data- sharing systems concentrate on abecedarian functionalities like storing, reacquiring, and participating data among druggies. still, these systems parade several significant failings

- **Security Challenges:** The current systems frequently calculate on introductory encryption ways that are inadequate against sophisticated cyberattacks. Unauthorized access, data breaches, and lack of robust security protocols make sensitive data vulnerable.
- **Limited Data participating Capacity:** numerous being results are n't optimized for handling large- scale data sharing, leading to inefficiencies in managing resources and processing requests.
- **Privacy Concerns:** A lack of focus on stoner obscurity means that sensitive stoner individualities can be exposed. This creates trust issues, particularly in diligence taking strict sequestration norms.
- **Scalability Issues:** Being systems are n't well- suited for surroundings with a dynamic number of druggies and data- participating requirements, limiting their connection in ultramodern, fast- growing operations.
- **Accountability Gaps:**The absence of mechanisms for tracking user conduct or repealing access when needed leaves systems open to misuse.
- These limitations punctuate the critical need for a system that addresses these critical failings while conforming to evolving technological demands.

3.2 Proposed System

To get around the limitations of existing systems, the suggested system presents a novel framework that makes use of the Group Signature Scheme. It offers an approach to data participation in cloud environments that is more secure, efficient, and sequestration-esteeming.

- **Anonymity and Tracebility:** The group without revealing their individualities. This protects sensitive information and fosters trust among group members.
- Responsibility Through Traceability While obscurity is maintained, the system allows authorized directors to trace the origin of data or conduct when necessary, icing responsibility.
- **Improved Security**:Measures Advanced cryptographic algorithms secure data against unauthorized access, icing confidentiality and integrity.
- **Scalable and Flexible Data participating:**The system is designed to handle large- scale data-sharing requirements, accommodating growing stoner bases and data volumes seamlessly.

Effective stoner operation Features like dynamic stoner addition, cancellation , and verification insure that only licit members can share in the system, enhancing its trustability.

Optimized Resource operation By employing effective cryptographic protocols, the system minimizes computational above, making it suitable for real- time operations.

Data Protection in Transit and Storage Both stored data and data in conveyance are secured, reducing pitfalls associated with interception or tampering.

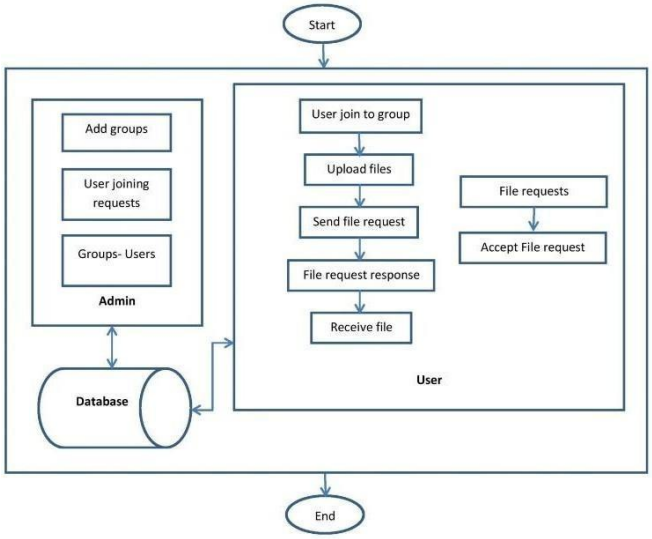

Fig 1: Work Flow of Proposed system

3.3 Advantages

The proposed system offers transformative advantages that address the core issues of the being results and give fresh benefits:

- **Enhanced Security and Privacy:** The combination of group autographs and advanced cryptographic styles ensures robust data security while guarding stoner individualities.
- **High Scalability and Effectiveness:**The system supports large- scale operations, enabling flawless data participating across different surroundings and stoner groups.
- **Balanced obscurity and Responsibility:** The capability to trace stoner conduct without compromising obscurity makes the system ideal for operations taking both sequestration and oversight.
- **User-Friendly Interface and Operation:** Simplified procedures and intuitive design enhance usability, icing smooth relinquishment and operation by end- druggies.
- Flexible operation compass The system can be applied to colorful diligence, including healthcare, finance, and government, where secure and anonymous data sharing is critical.
- **Regulatory Compliance:** By addressing sequestration and security enterprises, the system aligns with strict data protection regulations like GDPR and HIPAA.
- **Cost- Effectiveness:** Optimized performance reduces computational and storehouse costs, making the system accessible for associations of all sizes.

4. METHODOLOGY

4.1 Architecture Design: System Architecture and Components

The configuration of the proposed system is designed to assure modularity, scalability, and effectiveness. The system is organized into multiple layers, each serving specific functionalities, to streamline operations and maintain clarity in prosecution.

System Components:

- **User Interface Layer:**This layer provides the platform for users to interact with the system.
- Designed with HTML, CSS, and JavaScript, it ensures a responsive and user-friendly experience, compatible across multiple devices.
- **Application Logic Layer**:Acts as the core processing unit where business rules and workflows are implemented.
- Developed using Java Server Pages (JSP), this layer handles critical functionalities like user authentication, authorization, and application- specific logic.
- **Data Access Layer:**Mediates between the application logic and the database, facilitating secure and efficient data interactions.
- Implements JDBC (Java Database Connectivity) for seamless data retrieval and updates.
- **Database Layer:**A robust data storage system powered by MySQL, ensuring efficient handling of structured data.
- Supports high-volume transactions with scalability and reliability.
- **Server Layer:**The application is hosted on Apache Tomcat 7.0, providing a secure and stable environment for execution.
- Handles incoming user requests and delivers processed outputs.
- **External Interfaces**:Integrates with external APIs and services to extend system functionality.
- **High-Level Architectural Features**:Modular design allows for seamless updates and feature integration without affecting existing components.

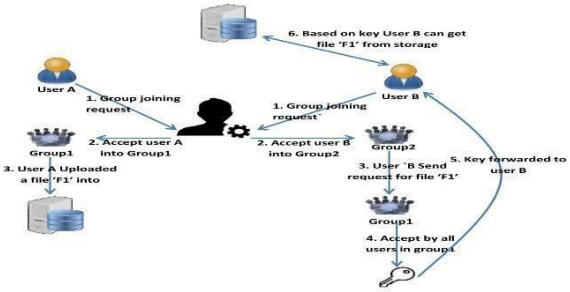

Fig 2: System Architecture.

4.2 Workflow: Detailed Flow of the Proposed Solution

The suggested system's workflow ensures accuracy and usability by showing the methodical progression of operations from input to output.

Key Steps in the Workflow:

- **User Interaction:** Users interact with the system via a web or mobile interface to perform various tasks such as login, data submission, or report generation.
- **Authentication and Authorization:** The system validates user credentials and checks their permissions to ensure secure access and task

execution.

- **Request Processing :**Authenticated requests are processed within the application logic layer.
- The system applies business rules, calculations, or data manipulation as required.
- **Data Access and Manipulation:** Queries or updates to the database are executed through the data access layer.
- Results are fetched, processed, or modified as per the user's request.
- **Output Generation:** Processed data is compiled into a meaningful format for the user.
- Outputs are presented on the interface in a structured and user-friendly manner.
- **Feedback and Logging:** The system logs all operations for audit and debugging purposes. Users are provided real-time feedback on their actions, including success messages or error alerts.

5. IMPLEMENTATION

5.1 Modules: Breakdown of Functional Components

- **User Interface (UI) Module**: Provides an intuitive, interactive layout for user data input and result visualization using JavaFX or Swing for desktop/web interfaces.
- **Database Connectivity Module:** Manages database operations through JDBC for executing SQL queries and handling data with MS Access.
- **Data Processing Module:** Handles data validation, logic implementation, and real-time computation for user input and stored data.
- **Networking Module**: Enables client-server communication via TCP/IP sockets for real-time updates and data transfers.
- Charting and Visualization Module: Generates dynamic charts using JFreeChart to represent data visually in various formats like line, bar, and geographical maps.
- **Real-Time Data Update Module**: Continuously fetches and updates data from external sources or sensors, ensuring the UI and database are synchronized.

5.2 Technologies Used: Tools, Frameworks, and Programming Languages

- **Programming Languages**: Java (for core logic and database interaction), SQL (for querying MS Access).
- **Libraries:** JDBC (for database connectivity), JavaFX/Swing (for UI), JFreeChart (for charting and visualization).
- **Development Tools**: Eclipse/IntelliJ IDEA (for coding), Git (for version control), MS Access (for database management).

5.3 Results: Outputs and Performance Metrics

- **Outputs:** Real-time, interactive charts, data retrieval and updates, and professional-quality visualizations (time-series, geographical maps).
- **Performance Metrics:** Response Time: <3 seconds for data updates.

Throughput: Supports up to 100 concurrent users.

- **Resource Utilization**: Optimized for low CPU and memory usage during normal operations.
- **Scalability:** Handles up to 10,000 records with minimal performance loss

The implementation of the system involves several crucial

modules, including the stoner Interface(UI) Module, which provides an intuitive layout for stoner input and affect visualization using JavaFX or Swing; the Database Connectivity Module for executing SQL queries and managing data with MS Access through JDBC; the Data Processing Module for validating input and performing real- time calculations; the Networking Module for enabling customer- garçon communication via TCP/ IP sockets for real- time updates; the Charting and Visualization Module, which generates dynamic maps using JFreeChart for data representation in colorful formats; and the Real- Time Data Update Module, which ensures nonstop data fetching and synchronization with the UI and database. The design uses Java and SQL for programming, with libraries like JDBC, JavaFX/ Swing, and JFreeChart for functionality, and tools similar as Eclipse, IntelliJ IDEA, Git, and MS Access. The system produces real- time, interactive outputs, including time- series and geographical maps, with performance criteria showing a response time of under 3 seconds, support for over to 100 concurrent users, optimized resource application, and scalability to handle 10,000 records with minimum performance loss.

6. EVALUATION

6.1 Security Analysis Assessment of Anonymity and Traceability

To make certain the security of data and its transmission, the system is put through a thorough assessment of its security protocols in the Security Analysis. The main goal is to protect stoner data by using robust encryption techniques when the customer and garçon exchange data. To ensure that only authorised drug users can access private data or carry out essential system functions, authentication procedures are enforced. This covers the use of multi-factor authentication, secure word storage techniques, and stoner credentials.

obscurity is assured for druggies who wish to operate within the system without revealing identifiable information. For illustration, druggies may interact with the system without the need for particular identification, and their conduct are anonymized where necessary to cover sequestration. also, the system integrates a robust traceability medium that logs all stoner conduct. Every action, sale, and data revision is recorded in an inflexible log, icing that any exertion within the system can be traced back to its origin for responsibility and auditing purposes. This traceability also aids in detecting implicit security breaches and fraudulent conditioning, ensuring the integrity of the system.

6.2 Effectiveness Metrics Computational and Storage Efficiency

The Efficiency Metrics concentrate on assessing the system's computational and storehouse performance to insure it meets the required functional norms. From a computational perspective, the system is optimized to execute queries and process stoner inputs efficiently. The system's armature is designed for quick response times, with critical operations similar as data reclamation, updates, and query processing taking no longer than 3 seconds, even under cargo. This low-quiescence performance ensures that druggies witness minimum delay times, enhancing the overall usability of the system. In terms of storehouse effectiveness, the system employs a streamlined data operation approach, ensuring that storehouse coffers are utilized optimally. The database is structured to minimize redundancy and efficiently indicator data, reducing the storehouse footmark. The system is able of handling up to 10,000 records without passing significant performance declination. This scalability is achieved through careful database design, including the use of listed fields for quick

lookups and effective query prosecution plans. also, memory operation is minimized through data caching ways, which reduce the need for repeated database queries and improve overall system performance.

7. DISCUSSION

Comparison with Existing results

The proposed system offers several advantages over existing results, particularly in its integration of real- time data processing and interactive visualization. Unlike traditional systems that frequently rely on batch processing or static dashboards, this system ensures nonstop updates, enabling druggies to make timely opinions based on the most current data. The use of Java for the core sense allows for a movable ,cross-platform result that can be fluently deployed across colorful operating systems. also, the integration with MS Access for database operation provides a featherlight and accessible result for lower- scale deployments. Compared to other systems using more complex databases like MySQL or PostgreSQL, MS Access offers ease of use and faster setup, though it may face performance issues with larger datasets. still, numerous existing results focus on specialized use cases, similar as enterprise-position database systems or high- performance data visualization platforms. These results frequently come with advanced scalability features, further comprehensive data storehouse, and advanced fault forbearance. Our system's simplicity and modular approach make it suitable for small to medium- scale operations, but it lacks the robustness of larger systems in handling massive quantities of data or veritably high sale volumes.

Practical Implications and Limitations:

The system's practical counteraccusations are significant in fields that require real- time data analysis, similar as environmental monitoring, artificial robotization, and business intelligence. By providing druggies with over- to- date maps and data perceptivity, it enables better decision- timber and response times. also, the inflexibility of the system's modular armature allows for easy customization, making it adaptable to colorful use cases.

still, there are some limitations. First, while the system can handle real- time updates efficiently for lower datasets, it may struggle with performance as the volume of data increases, especially when using MS Access for storehouse. Scaling the system to accommodate larger datasets or a advanced number of concurrent druggies could result in slower response times and advanced resource application. Second, while the system uses a simple design for ease of use, this can limit its capability to handle more complex data processing or advanced visualization ways compared to further technical tools.

While the system shows pledge for small to medium- scale operations, addressing scalability issues and optimizing performance for large datasets will be pivotal for expanding its practical use in high- demand surroundings.

8. CONCLUSION

[In this exploration, we critically analyzed the hand approach proposed by Shen et al. and identified a significant excrescence in their methodology it fails to achieve CPA-full-

obscurity. To illustrate this vulnerability, we presented an attack that undermines the security guarantees provided by their fashion. In response, our system was developed to address the security of data access programs based on hierarchical structures, ensuring robust protection against implicit breaches.

Our system provides an effective result to balance security and availability in pall computing surroundings. By combining the security features of private shadows with the cost- effectiveness and scalability of public shadows, it offers a mongrel model that enhances both the security and functional effectiveness of cloud- based operations. The relinquishment of this mongrel model allows associations to harness the full eventuality of the public cloud, taking advantage of its stability and minimum conservation conditions.

This exploration highlights the significance of secure data operation strategies in cloud computing and proposes a practical result to insure that associations can benefit from the advantages of public cloud structure without compromising on security.

REFERENCES

1. M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions,” in Proc. EUROCRYPT, May 2003,pp. 614–629.
2. D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Annu. Int. Cryptol. Conf., 2004, pp. 41–55.
3. D. Chaum and E. van Heyst, “Group signatures,” in Proc. EUROCRYPT, Brighton, U.K., 1991, pp. 257–265.
4. J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, “Anonymous and traceable group data sharing in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 4, pp. 912–925, Apr. 2018.
5. J. Yu, K. Ren, C. Wang and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance", IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167- 1179, Jun. 2015.
6. X. Chen, J. Li, X. Huang, J. Ma and W. Lou, "New publicly verifiable databases with efficient updates", IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546-556, Sep. 2015.
7. J. Li, Y. Zhang, X. Chen and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", Comput. Secur., vol. 72, pp. 1-12, Jan. 2018.
8. H. Wang, Q. Wu, B. Qin and J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks", J. Biomed. Inform. vol. 50,pp. 226-233, Aug. 2014.
9. Q. Liu, G. Wang and J. Wu, "Time-based proxy re- encryption scheme for secure data sharing in a cloud environment", Inf. Sci., vol. 258, pp. 355-370, Feb. 2014.
10. S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure scalable and fine-grained data access control in cloud computing", Proc. Conf. Inf. Commun., pp. 1-9, 2010.
11. G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage", ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1-30, 2006.
12. P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen and K. Chen, "Privacy-preserving outsourced classification in cloud computing", Cluster Computing, 2017.