Journal of Theoretical and Applied Information Technology
15th May 2023. Vol.101. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPARATIVE ANALYSIS ON THE COMBINED MULTI LEVEL FUNCTIONALITY FRAMEWORK IN CLOUD ENVIRONMENT WITH ENHANCED DATA SECURITY LEVELS FOR PRIVACY PRESERVATION

K.SANTHI SRI[1], N. VEERANJANEYULU[2]

Department of CSE, Vignan's Foundation for Science Technology & Research, Vadlamudi, Guntur 522213, Andhra Pradesh, India
Department of IT, Vignan's Foundation for Science Technology & Research, Vadlamudi, Guntur 522213, Andhra Pradesh, India
E-mail: srisanthi@gmail.com[1]

ABSTRACT

Cloud Computing (CC) refers to a network of remote servers and user access via the Internet. Distributed data centers all around the globe are responsible for providing the infrastructure and hosting the servers that power cloud services. The dynamic user group handling and securing their sensitive information using cryptography model is a challenging task as the user groups are continuously increasing. Encryption is a better answer for these kinds of problems, but allowing access to users in the cloud has its own set of challenges. From the client's point of view, when the information is saved in the cloud, it should be crypted well to ensure that no other user can read it if they get access to it in any way. Using cloud storage comes with a number of potential drawbacks, including the lack of security for critical information. This study examines the considerations that should be made when choosing a cloud service provider, with a focus on the client's encryption needs and how, without them, the client runs the risk of either losing data or paying more than necessary to the cloud service provider. To enhance the privacy preservation and key management issues a combined framework that handles data encryption, key management and distribution, cloud user group management is analyzed in this research that enhance the data security levels using cryptography model and the key management and distribution process with the dynamic cloud user groups. This research performs a comparative analysis by comparing the combined framework with traditional models. The proposed model when compared with the existing methods exhibit better security levels.

Keywords: *Cloud Computing, Privacy Preservation, Cryptography, User Groups, Data Security, Encryption, Quality of Service.*

1. INTRODUCTION

As cloud computing is such a sizable and consequential topic, it has attracted the attention of many academicians and researchers from use in both the academic and industry sectors. Several issues surfaced after the introduction of cloud computing. Cloud computing faces a number of common and broad challenges, including interoperability [1], SLA-(service level agreement) [2], universal standards, a single approach for all cloud services, data portability among different clouds, a wide range of security issues, and, most importantly, privacy protection for users' secret and confidential information need to be considered into account for better quality of service [3]. Through the cloud's open design and interoperability with similar services, businesses of all stripes may meet their diverse set of needs with lightning speed and without sacrificing their customers' or clients' right to privacy [4]. The layers of the cloud work together to make things like sharing files and transferring information quickly and easily available [5].

The term cloud storage refers to the practise of storing data in the cloud and making it accessible to users in a variety of ways through traditional networks; this practise includes things like maintaining a brief description of cloud user information, business specifics, and backup information and making it globally available through the internet. Online data backup and archiving, data compliance standards [6], disaster

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

recovery, and compliance rules are some of the issues of cloud data storage. Data storage and transfer in the cloud can be accomplished in several ways, each of which is dependent on the SLAs and policies of the provider using the approach [7]. As the number of cloud storage providers proliferates, users have the option of porting their data from one service to another [8].

The onus of ensuring data privacy and resolving any difficulties that may arise during data retrieval falls on the service provider in this scenario [8]. In order to maintain their infrastructure and power supply, leading CSPs are shifting to a policy of sending client data to cloud recovery service providers. Some hypothetical criteria should be applied to define the maximum possible storage of information [9] in order to alleviate or increase user confidence in the security of their data. Assessing the privacy implications of off-site data replication and disaster recovery for service providers and end users may benefit from considering a variety of risk variables. Cloud storage has been included into a variety of administrative-level guiding principles to ensure that clients can be supplied on-demand across all settings while maintaining tight confidentiality [10].

One of the most frequent and productive methods of getting things done is by using a cloud data sharing solution that allows several people to see and modify the same collection of data. The proliferation of cloud-based file sharing has led to a new challenge: managing group keys [11]. Current approaches to managing group keys are overly prescriptive, limiting their applicability to a more general class of groups. As a result, various proposals for distributed protocols are made. Putting all of a user's data on the cloud is not a good idea because of security flaws and hacking risks [12]. In order to ensure that a newly joining user cannot decode past communications information in the newly joining group, and that a previously drawn back user cannot decode future communications data in the left group, compromises must be made on both reverse security and forward security. Therefore, it is recommended that large numbers of keys be rekeyed frequently to maintain safety. The generation, distribution, and upkeep of keys through group structure is a secure and reliable method [13].

Information technology has perpetually been preoccupied with the issue of data security. This is especially important to keep in mind when considering cloud computing, as data can be kept anywhere from a single server to across the globe. Users typically have concerns about the security and privacy of their data on the cloud. Though numerous techniques on the topics in cloud technology have been researched in both academic and industrial contexts, data security and privacy security are becoming increasingly vital for the future progress of cloud computing services in government [14], industry, and business. Maintaining the privacy and integrity of cloud-stored information requires the combined efforts of both hardware and software. The purpose of this analysis is to justify the security levels of the models used for securing the users data in cloud environment [15]. The models used for the key generation, user handling, key distribution is analyzed and the considered models are better in securing the users sensitive information [16].

Having one person or team take care of all group communication in a centralized system that is the most effective way to get things done. Managing the production and dispersal of keys relies solely on this one variable. Logical Key Hierarchy is a technique that helps reduce the expenses associated with rekeying. Barriers to a unified approach include scalability costs, because achieving correspondence between participants relies on a certain focal element, rekeying becomes more of a hardship as a gathering's size increases [17]. The capacity cost is the number of private session keys that must be guarded. Upholding both forward and backward security as members of the organisation join and leave the cloud [18].

In most protocols for decentralized group key management, a large group is divided into several smaller ones, and a manager is assigned to each of these. The administrator manages the process of adding and removing users [19]. Each group's manager is the first to get a set of keys, and then those keys are passed out to the group's users. When a user in the cloud wants to join or leave a group, the session keys for that group must be updated. Thus, it benefits from the most attractive qualities of both centralised and decentralised models [20]. Using this method reduces the burden on key distribution center. In order to accomplish this, the large group is partitioned into multiple subgroups, each of which is overseen by a subgroup controller. This method

eliminates the risk of a failure at a central location. This protocol can be further subdivided into the time-driven and membership-driven categories [21]. Each time a user enters or exits a group, the session key associated with their account must be updated to reflect the new group membership protocol. The main distinction is that time driven procedure is applied at predetermined intervals. The general data storage model in cloud using basic cryptography model is shown in Figure 1.

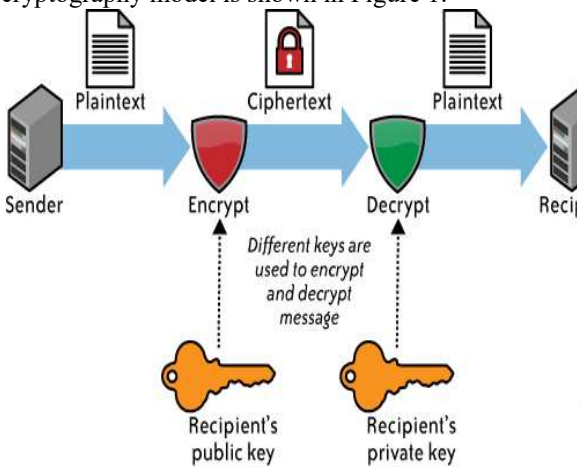


Figure 1: Basic Cryptography Model for Data Security

When a CSP only provides specific cloud services to one client, the result is known as a private cloud. In this setup, public and private cloud services have been combined. In a public cloud, users can access services from anywhere in the world. These tasks should be handled by the data owner and the CSP [22]. Google Cloud is one source that is easily accessible. Services can be provided on a free, per-client, or per-use basis to customers. Since the management of an open cloud is available to the public, other access to the data saved at the CSP's site. CSPs cannot be relied upon to safeguard the privacy of customers' sensitive information [23]. As a result, several companies avoid employing open cloud services because of security and privacy concerns. The data security process in cloud environment is shown in Figure 2.

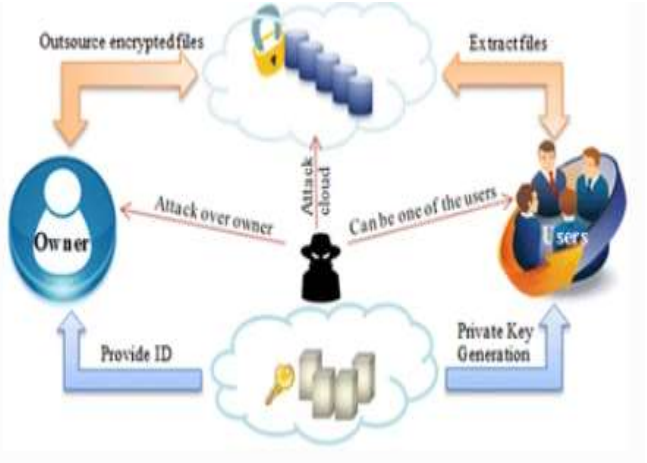


Figure 2: Data Security Process

The administrator must set up an entry-control system that protects the privacy of its customers while allowing for the swift and simple transmission of data to a sizable, publicly active group. For the purpose of archival storage in a public cloud that cannot be trusted, a system for granular access control using encryption is described [24]. Customers can see archives if they have been given permission to do so by the data controller. Accessibility to the cloud is granted or denied based on a number of factors, including the specific characteristics of each customer. Characteristics of the client are provided when they sign up for the service. The client's privacy is safeguarded alongside their data and records [25]. Report decryption is only granted to users whose features are a close match to those of the data owner using the proposed characteristics based access management model. Client anonymity ensures that data in the cloud is safe from attackers [26].

New cryptographic components and other proposals for protecting cloud data services from potential threats have recently been developed. These can be broken down into four main categories: cloud services that provide confidentiality, cloud services that allow for owner-controlled data exchange, cloud services that guarantee data integrity, and cloud services that safeguard users' right to privacy. In particular, searchable encryption and elliptic curve cryptographic algorithms are used to enforce secure data search and secure data processing, introduced preferential encryption and attribute-based cryptographic methods to achieve authorised access and secure data sharing, present provable information assets and proof-of-retrievability methodologies to guarantee data integrity and

retrieval, and enable privacy preserving to safeguard data across multi-party contexts [27]. Although some data confidentiality methods may also provide privacy protection, it is vital to note that privacy protection is handled independently from data confidentiality protection [28]. Instead than focusing on broad data security, privacy protection measures are considered.

2. METHODOLOGIES

Given the exponential growth in data volume in the cloud computing environment, data owners are increasingly likely to store their data there. While there may be financial benefits to outsourcing data processing and storage, the original data owners face new privacy and security challenges as a result. Improved search functionality and efficiency are great, but access control and formal security analysis are still problematic with the current state of the art in ranked keyword search [29]. A public auditing system that ensures the integrity of data saved in the cloud is crucial to the widespread adoption of cloud computing [30]. There has been a lot of study and discourse in recent years around public auditing procedure. Public cloud storage auditing protocols based on regenerating codes were introduced and these protocols were secure within the context of the security model that was evaluated.

As a shorthand for the processes through which the veracity of data saved in the cloud for multiple users is evaluated, the phrase cloud storage auditing methods for shared data is commonly used. Since there are a number of reasons why a user's membership in a group might need to be changed, such schemes usually allow for the user's withdrawal from the group. In the past, the computational cost of revoking a user using such a mechanism was directly proportional to the amount number of file blocks controlled by the user. Despite this advantage, it is possible that managing all of users data in the cloud will become a cumbersome burden. To facilitate efficient cloud data audits, it is crucial to learn how to reduce the computational load presented by user revocations. This research considers a novel auditing system that facilitates effective user revocation, regardless of the total number of file blocks owned by the user being revoked in the cloud. A method to revoke a user's access by replacing their authenticators but not their private key is analyzed. Integrity assessments for a revoked user can be performed even if the authenticators aren't updated. However, the considered method employs standard cryptography, which eliminates the need for the time-consuming certificate maintenance of traditional Public Key Infrastructure (PKI).

Maintaining data integrity is a major concern for secure cloud storage. Therefore, it is essential that data be accurate before outsourcing. Protocols for auditing data that has been outsourced make it possible for a verifier to quickly and easily determine whether or not outsourced files are legitimate without having to download the entire file from the cloud, greatly reducing the communication load on both the cloud server and the verifier. Currently used protocols have a number of drawbacks, one of the most significant being their reliance on public key infrastructure or precise identification, both of which can be difficult to implement. By creating a unique attribute set and assigning an auditor set, users may confidently store files in the cloud while also ensuring the data is accurate. The security of considered protocol is shown by relying on the computation Diffie-Hellman premise and the discrete logarithm assumption.

3. COMPARATIVE ANALYSIS

This papers performs a comparative analysis by considering the data security model in cloud called group key management technique using Diffie-Hellman and elliptic curve cryptograph with decentralized key management scheme using alternating multilinear forms for cloud data sharing with dynamic multiprivileged groups for privacy preservation of cloud data. The considered model is compared with the traditional Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage (CPIC-GSD) Model, Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud (SDGS-DA-TC) model and Dynamic Group-Oriented Provable Data Possession in the Cloud (DGOPDP) model.

At first, the considered model for user group handling is effective since it requires the cloud user to obtain the data owner's permission before users may access the data. For this reason, the considered solution employs the Elliptic Curve Diffie-Hellman method for both adding new members to the approved list and handling the case when an existing member of the authorised list requests to be removed. Not every authorised user is granted access to the same set of resources; instead, access is granted to users according on

their individual needs. The authorized users in the cloud will be granted with the permissions like Read-only; Write; Read-Write; Read-Write and Download. By submitting requests to the data owner, authorised group members will be granted with these permissions.

Cloud users and data owners can communicate safely with a computation process based on elliptic curve cryptography and the Diffie-Hellman key exchange. Initially, the proposed solution is useful when a cloud user requests access to data from a data owner. The owner of the data must give requested user with permission to use it. The considered approach makes use of the Elliptic Curve Diffie-Hellman method for both adding new members to the authorised list and dealing with the case where an existing member of the authorised group decides to leave the group.

To facilitate cloud data sharing across dynamic multiprivileged groups, a decentralised key management approach based on alternating multilinear forms is considered for analysis. This model is intended to ease pressure on Key Distribution Center (KDC). In this model, a large group is broken up into smaller ones, and each smaller group has a manager in charge of handling membership changes and group switching. Group Managers are given access to the session keys, and then they can share those keys with the members of their groups.

The particular keys are changed whenever a cloud user joins, leaves, or switches services, enabling them to communicate with members of other cloud user groups. Two independent entities are under the cloud user's command. With this strategy, users need not to worry about a weak spot. When a user in the cloud decides to join, leave, or move groups, a membership-driven rekeying to ensure that their session keys are always up-to-date is performed that is secure.

Where P is a prime number, the groups are denoted as CG1, CG2, CG3,..., CGn, Let CCG1 and CCG2 be constrained cyclic groups with the same prime request P, and let G be a generator of CG1. Assuming L is large enough, all group managers will share the same F-multilinear map and the same hash function H(CG). Additionally, a secret S[L.P] is selected at random. Trough, the group manager obtains the system parameters, its public and private keys (K_{pu},K_{pr}), and the keys of the other group managers. A session key is differentiated from an older version of itself by S_k. The considered model combined framework is shown in Figure 3.

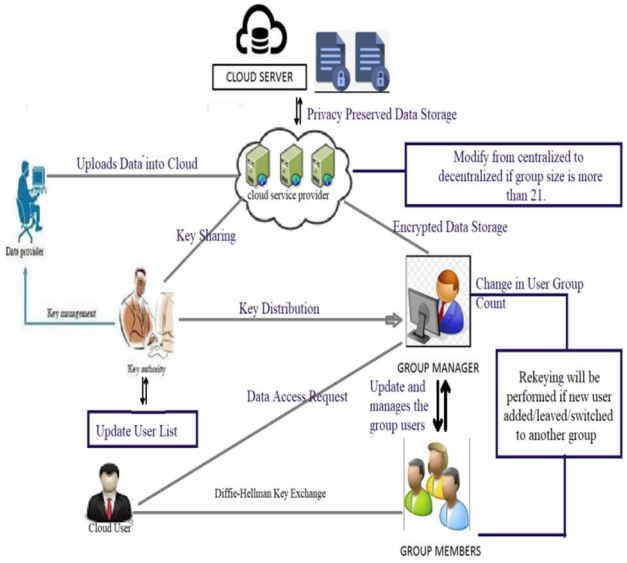


Figure 3: Considered Model Integrated Framework

The considered model takes into account four parties that make up a Cloud data sharing system: the data owner, the cloud service group, the group manager, and the cloud users. When a user in the cloud decides to quit the group, the manager creates a new key and the group management is responsible for sending it out to the group's remaining members. Signature Key is also communicated to the opposite group manager to convey this information. After verifying the signature, users in group should determine whether key version has been updated. Overcompensated service groups use alternating multilinear forms of a uniform rekeying material to update session keys securely and efficiently. Managers can participate in the rekeying material transaction if they have access to the mutual session keys. It only takes one pass to arrange a rekeying material, as opposed to several inflated session keys. As a result of the cloud's multiprivilege group communication capabilities, users can adjust their permissions to suit their needs.

To switch from one group to another in the cloud, the user must first leave the previous group and then join the new group. The key thing here is that the user access privileges have not changed, hence the shared SKs between SGn and SGm do not need to be altered. Leaving the group is analogous to going from SGn to SGm, and vice

versa. In order to facilitate the sharing of cloud data amongst shifting, multi-privileged groups, a decentralized key management technique based on alternating multilinear forms is considered. Neither centralized nor decentralized group protocols are required. In considered system, a huge group is broken up into several smaller groups, each of which is led by a individual manager. The administrator of a group is responsible for handling requests to join, leave, or swap groups. The group can contain a maximum of 21 users and if it exceeds, the model becomes decentralized. If any cloud user needs to join or leave the group and change their privileges, the associated session keys must be reset. Users that join and leave the group frequently will often trade the perks they received upon joining one group for those of another. According to the considered methods, each leaving or switching task requires only a single cycle of planning. Using this method also helps to reinforce the ever-changing nature of cloud benefit user groups.

The considered model accepts user requests for cloud resource accessing and then forms as groups. The groups will be monitored by the group manager. The group manager will generate the individual keys for all the users using key authority and the individual keys and group key is shared to all the group members. The group members will access the cloud resources using the group key and own keys. The key distribution is performed using Diffie-Hellman and data security is provided using elliptical curve cryptography as the data is converted into a point on elliptical curve and then shared to the cloud. The group members can enter or leave or switch the groups as per their requirement. If any group member leaves the group, the manager will perform rekeying and a new group key is calculated and shared to all. This allows the group to maintain data security and avoid unauthorized access.

The cloud users who maintain a group of a maximum of 21 users will be monitored by the group manager which is a centralized model. If more number of users enters the group, the decentralized mode is activated and the cloud service provider will handle the users as per the requests. Two independent groups are under the cloud user's command. With this strategy, users won't have to worry about a weak spot. When a user in the cloud decides to join, leave, or move groups, membership-driven rekeying is performed to ensure that their session keys are always up-to-date. Since the servers and managers of service groups typically have powerful computing resources, it is not concerned for them to be in charge of generating session keys. Key distribution for the purpose of rekeying is unnecessary in considered approach. In leaving/entering/switching operations, only rekeying material is distributed instead of numerous keys. That is why considered approach is so effective at cutting down on communication expenses. The key size and the key session is also dynamic so that the security levels in the considered approach is high.

When a cloud user asks access to data from a data owner, the approach under consideration works as intended, at least in its current version. In the model under consideration, the Elliptic Curve Diffie-Hellman technique is utilised to both expand the pool of authorised users and respond to the exceedingly unlikely scenario in which one of those users decides they no longer want to be on the approved list. Due to security concerns, not every authorised user is given access to all of the available resources; rather, access is allowed on a case-by-case basis. Attribute-based cloud data can round out the procedure for trustworthy outsourced storage that protects users' privacy and facilitates effective multi-keyword ranked searches in real time, which greatly simplifies cloud-based identity management. The answer to scaling problems is identity-based encryption transformation, which employs multi-factor authentication and lightweight cryptography for sharing data on the public cloud.

The considered model is implemented in eclipse and developed in java. The cloud users are created and the groups are maintained. The encryption and decryption is performed using elliptical cryptography and the keys are distributed among the users using diffie hellman key exchange model. The considered approach when contrasted with the existing models exhibit better performance. The comparative analysis is performed and the results are clearly shown.

Cloud users will send a request for CSP for accessing the cloud resources. The CSP will validate the cloud users and assign the keys and allot in a group so that the cloud users can access the cloud resources. The time for validating the cloud users and adding them to a user group is calculated that is less when contrasted to the existing models. The Figure 4 shows the time for adding the cloud users to groups of the considered integrated model and traditional models.

Journal of Theoretical and Applied Information Technology
15th May 2023. Vol.101. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

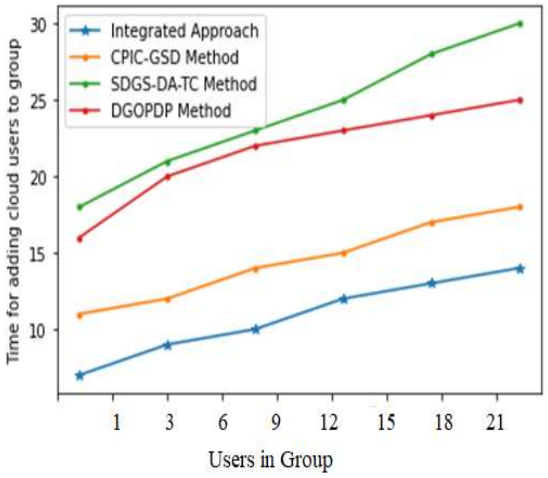


Figure 4: Time for adding cloud users to group

The group in the considered model holds a limited number of users. The maximum number of cloud user group is 21. The group generation time levels with maximum users in the group is considered and the comparison levels are shown in Figure. Only the considered integrated model considers the maximum group size as 21. However, the traditional models considered less group members size. The group generation time levels are shown in Figure 5.

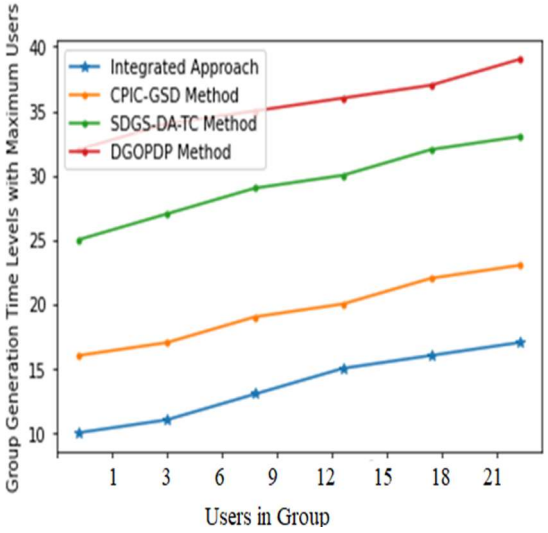


Figure 5: Group Generation Time Levels with Maximum Users

Generation of cryptographic keys is known as key generation. No matter what kind of information is being encrypted or decrypted, the key is used to do both. The public and private keys are used in the integrated approach for encryption and decryption. The time levels for the individual key generation and group key generation is shown in Figure 6.

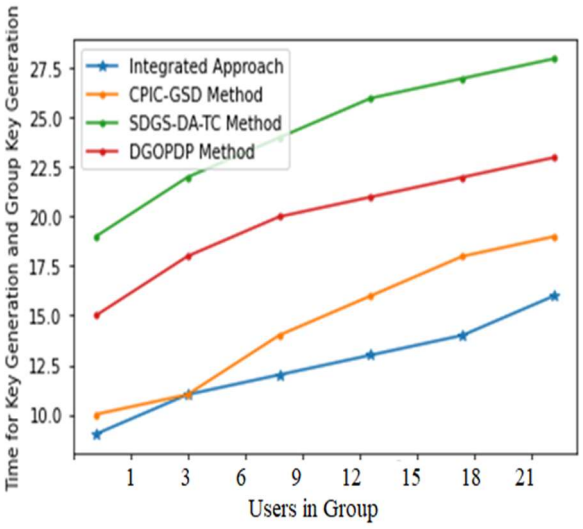
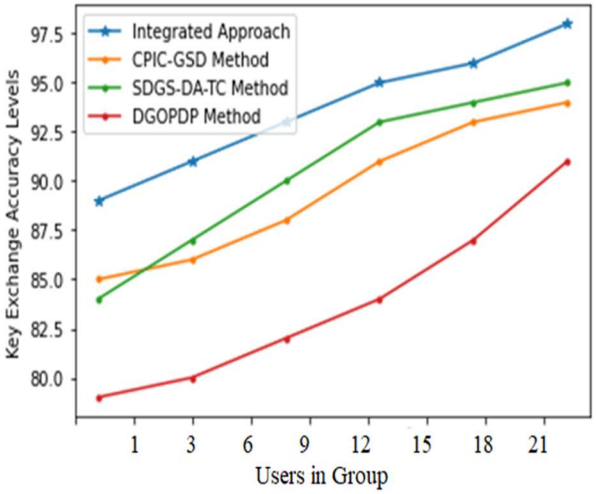


Figure 6: Time for Key Generation and Group Key Generation

In cryptography, a key exchange refers to the process by which two parties share secret information in order to apply a cryptographic algorithm. Both the sender and the recipient must have the ability to encrypt and decrypt messages for the exchange of encrypted communications to take place. The key exchange accuracy levels of the proposed and existing models are shown in Figure 7.



Journal of Theoretical and Applied Information Technology
15th May 2023. Vol.101. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 7: Key Exchange Accuracy Levels

The creation of security solutions to safeguard network activity relies on cryptographic methods. However, practical implementation of such methods is at risk due to the computational and energy limits of network devices. The suggested method's computational expenses by operation is very less, specifically, adding, removing, and switching cloud users. The Figure 8 shows the key computation cost levels of the considered and traditional models.

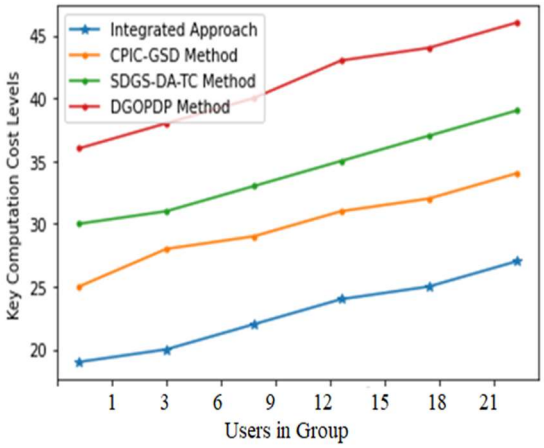


Figure 8: Key Computation Cost Levels

Rekeying is the method through which a new key is generated for the system. While the system's encryption must be turned on in order to generate new keys, rekeying can be performed regardless of whether or not the arrays themselves are encrypted. The rekeying is performed when a user from a group leaves or switches or a new user is added to the group. The Rekeying time levels are represented in Figure 9.

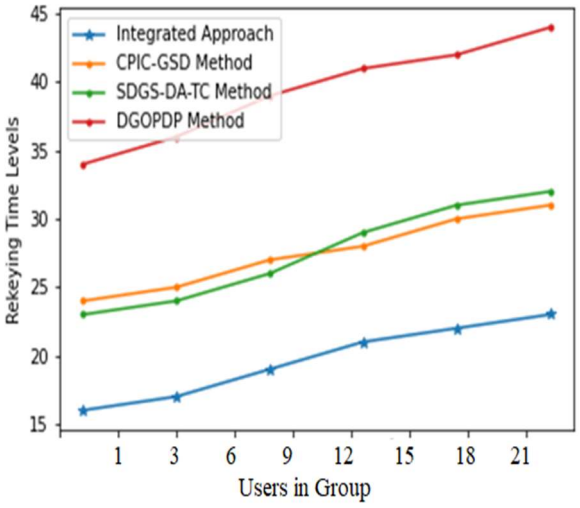


Figure 9: Rekeying Time Levels

Encryption is the procedure of encoding data in the field of cryptography. As a result of this operation, the plaintext representation of the data is transformed into the ciphertext form. In a perfect world, only authorised individuals would be able to convert ciphertext back into plaintext and gain access to the original data. The Figure 10 shows the encryption and decryption time levels of the considered approach and traditional models.

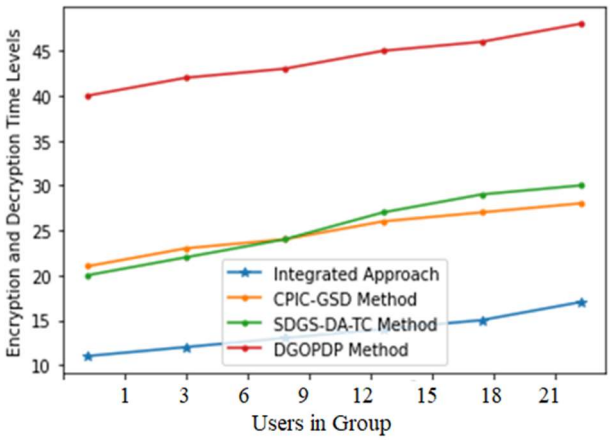


Figure 10: Encryption and Decryption Time Levels

Encryption is a process of transforming a message from its human-readable form into one that cannot be deciphered by anybody other than the intended recipient. To decrypt a message means to return it to its original, non-encrypted form. The accuracy levels in

performing encryption and decryption is shown in Figure 11.

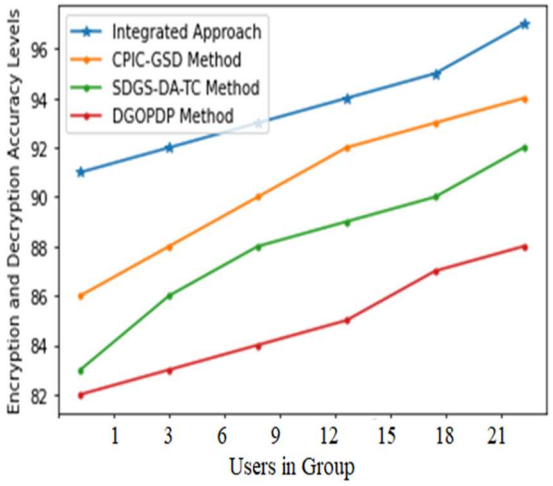


Figure 11: Encryption and Decryption Accuracy Levels

When it comes to digital information, data security is the process of preventing its loss, misuse, or alteration at any point in time. Information security as a whole is covered by this idea, from the physical safeguarding of servers and storage devices to the management of user access and the logical protection of programmes. The policies and procedures of the company are included as well. The data security levels of the considered approach and the traditional models are represented in Figure 12.

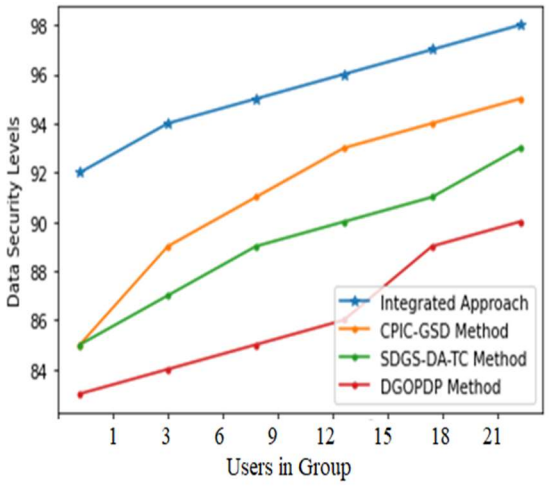


Figure 12: Data Security Levels

4. CONCLUSION

Data security and privacy concerns are the primary roadblocks to the widespread adoption of cloud computing. Every business must find ways to keep data stored and processed for as little as possible, while analysis of data and information remains a top priority across all industries. Businesses won't feel safe entrusting data and information to cloud service providers unless there is mutual trust between them. Researchers have proposed a variety of strategies for keeping data safe and ensuring the highest level of security for data kept in the cloud. However, many of the remaining knowledge gaps can be closed with better implementation of these methods. This study gives a comparative analysis on the considered encryption and user handling model with the old approaches, which is a significant step towards developing mutual confidence between service providers and their consumers in cloud computing environments. If both cloud providers and cloud requestors/end-users ensure all there own data has its own privacy policy, even if they consented to choose distinct cloud providers to contain or exchange data, as per adaptability and interoperability of privacy law and pertain its issues, then researchers can have faith that this proposal will prove to be a useful base for solving their issues on privacy for data centre in all stipulated areas. The cloud may store some sensitive data. Users' trust in cloud service providers declines and they become more susceptible to privacy invasions whenever sensitive data is exposed or stolen. The method under consideration is initially helpful when a cloud user makes a request to a data owner. The owner of the data must give him permission to use it. The considered approach makes use of the Elliptic Curve Diffie-Hellman method for both adding new members to the authorised list and dealing with the case where an existing member of the authorised group decides to leave. The outcomes demonstrate that the suggested method outperforms the other traditional models, in terms of group user management. In order to facilitate the sharing of cloud data amongst shifting, multi-privileged groups, this research considered a decentralised key management technique based on alternating multilinear forms. Neither centralised nor decentralised group protocols are required. In the considered model, a huge group is broken up into smaller ones, and each of those gets its own manager. The administrator of a group is responsible for handling requests to join, leave, or swap groups. If any cloud user needs to join or leave the group and change their privileges, the

associated session keys must be reset. Users that join and leave the group frequently will often trade the perks they received upon joining one group for those of another. According to the considered method, each leaving or switching task requires only a single cycle of planning. The proposed model security level increases as the key size is dynamic and the key generation depends on the number of users in the group. The key distribution is also performed in a technical way as the user in a group leaves the cloud, the information is distributed to all users in cloud for avoiding unauthorized access and rekeying is performed immediately to secure the data. Centralized and distributed key management systems both have problems, but the considered model eliminates both of them. When compared to already-existing techniques, the considered method's analysis is both secure and computationally efficient.

REFERENCES:

[1] J. Li, H. Yan and Y. Zhang, "Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage," in IEEE Transactions on Services Computing, vol. 14, no. 1, pp. 71-81, 1 Jan.-Feb. 2021, doi: 10.1109/TSC.2018.2789893.

[2] Q. Huang, Y. Yang and J. Fu, "Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud," in IEEE Transactions on Services Computing, vol. 14, no. 4, pp. 1013-1025, 1 July-Aug. 2021, doi: 10.1109/TSC.2018.2850344.

[3] K. He, J. Chen, Q. Yuan, S. Ji, D. He and R. Du, "Dynamic Group-Oriented Provable Data Possession in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1394-1408, 1 May-June 2021, doi: 10.1109/TDSC.2019.2925800.

[4] J. Li, J. Ma, Y. Miao, R. Yang, X. Liu and K. -K. R. Choo, "Practical Multi-Keyword Ranked Search With Access Control Over Encrypted Cloud Data," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 2005-2019, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3024226.

[5] J. Zhang, R. Lu, B. Wang and X. A. Wang, "Comments on “Privacy-Preserving Public Auditing Protocol for Regenerating-Code-Based Cloud Storage”," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1288-1289, 2021, doi: 10.1109/TIFS.2020.3032283.

[6] H. Yan and W. Gui, "Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving," in IEEE Access, vol. 9, pp. 45822-45831, 2021, doi: 10.1109/ACCESS.2021.3066497.

[7] Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling Efficient User Revocation in Identity-Based Cloud Storage Auditing for Shared Big Data," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 608-619, 1 May-June 2020, doi: 10.1109/TDSC.2018.2829880.

[8] Y. Yu, Y. Li, B. Yang, W. Susilo, G. Yang and J. Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage," in IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 377-390, 1 April-June 2020, doi: 10.1109/TETC.2017.2759329.

[9] H. Deng et al., "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3168-3180, 2020, doi: 10.1109/TIFS.2020.2985532.

[10] S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

[11] Y. Yang, Y. Chen, F. Chen and J. Chen, "An Efficient Identity-Based Provable Data Possession Protocol With Compressed Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1359-1371, 2022, doi: 10.1109/TIFS.2022.3159152.

[12] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu and J. Ma, "Data Integrity Auditing without Private Key Storage for Secure Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1408-1421, 1 Oct.-Dec. 2021, doi: 10.1109/TCC.2019.2921553.

[13] X. Yang, M. Wang, X. Wang, G. Chen and C. Wang, "Stateless Cloud Auditing Scheme for Non-Manager Dynamic Group Data With Privacy Preservation," in IEEE Access, vol. 8, pp. 212888-212903, 2020, doi: 10.1109/ACCESS.2020.3039981.

[14] Y. Li and F. Zhang, "An Efficient Certificate-Based Data Integrity Auditing Protocol for Cloud-Assisted WBANs," in IEEE Internet of Things Journal, vol. 9, no. 13, pp. 11513-11523, 1 July1, 2022, doi: 10.1109/JIOT.2021.3130291.

[15] Yang, J. Xu, J. Weng, J. Zhou and D. S. Wong, "Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 212-225, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2851256.

[16] A.Jin, J. Park and H. Mun, "A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment", *Wireless Pers. Commun.*, vol. 105, no. 2, pp. 599-618, 2019.

[17] H. C. Chen, "Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application", *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 839-852, 2019.

[18] L. Zhou, X. Li, K.-H. Yeh, C. Su and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance", *Future Gener. Comput. Syst.*, vol. 91, pp. 244-251, Feb. 2019.

[19] G. Sharma and S. Kalra, "Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications", *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 1771-1794, Feb. 2019.

[20] G. Xu, H. Li, Y. Dai, K. Yang and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data", *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 870-885, Apr. 2019.

[21] X. Li, Y. Zhu, J. Wang and J. Zhang, "Efficient and secure multi-dimensional geometric range query over encrypted data in cloud", *J. Parallel Distrib. Comput.*, vol. 131, pp. 44-54, 2019.

[22] Z. Guan et al., "Cross-lingual multi-keyword rank search with semantic extension over encrypted data", *Inf. Sci.*, vol. 514, pp. 523-540, 2020.

[23] H. Dai, X. Dai, X. Yi, G. Yang and H. Huang, "Semantic-aware multi-keyword ranked search scheme over encrypted cloud data", *J. Netw. Comput. Appl.*, vol. 147, 2019.

[24] H. Wang, D. He and S. Tang, "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud", *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1165-1176, Jun. 2016.

[25] H. Wang, D. He, J. Yu and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession", *IEEE Trans. Serv. Comput.*, Nov. 2016.

[26] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni and K. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems", *IEEE Trans. Dependable Secure Comput.*, Feb. 2017.

[27] T. Jiang, X. Chen and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation", *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2363-2373, Aug. 2016.

[28] Y. Tseng, T. Tsai, S. Huang and C. Huang, "Identity-based encryption with cloud revocation authority and its applications", *IEEE Trans. Cloud Comput.*, Mar. 2016.

[29] J. Wei, W. Liu and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption", *IEEE Trans. Cloud Comput.*, vol. 6, no. 4, pp. 1136-1148, Oct. 2018.

[30] D. He, N. Kumar, H. Wang, L. Wang, K.-K.-R. Choo and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network", *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 633-645, Jul. 2018.

[31] Z. Cao, H. Wang and Y. Zhao, "AP-PRE: Autonomous path proxy re-encryption and its applications", *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 5, pp. 833-842, Sep. 2019.

[32] C. Ge, W. Susilo, L. Fang, J. Wang and Y. Shi, "A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system", *Designs Codes Cryptography*, vol. 86, no. 11, pp. 2587-2603, Nov. 2018.

[33] P. Jiang, J. Ning, K. Liang, C. Dong, J. Chen and Z. Cao, "Encryption switching service: Securely switch your encrypted data to another format", *IEEE Trans. Services Comput.*, Oct. 2018.