ISSN: 2096-3246
Volume 53, Issue 02, June, 2021

A ES

https://doi.org/10.5281/zenodo.12707057

A DATA EXCHANGE PROTOCOL TO REDUCE CLOUD STORAGE DATAPROTECTION RISKS IN THE BIG DATA ERA

VIJAYA BHASKAR MADGULA, DIGALA RAGHAVA RAJU, K BALAJI SUNIL CHANDRA

Assistant Professor [1,2,3]

vijaya.bhaskar2010@gmail.com, raghava.digala@gmail.com, hod.cse@svitatp.ac.in
Department of Computer Science and Engineering, Sri Venkateswara Institute of Technology, N.H 44,
Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:
Efficient data sharing, Security, SSGK, and cloud providers.

ABSTRACT

By using a cloud storage system, the data sharing service ensures the secure transmission of information to reliable users. Conventional methods store shared information in data centres that are under the control of the data owner and the data provider. On the other hand, cloud providers store this information in data centres that aren't necessarily under the same level of trust as the data owner. The possible breach of data confidentiality is brought about by this. Using a secret sharing groups key management protocol (SSGK), this article explains how to protect conversations and shared data against unauthorised access. In contrast to other attempts, SSGK uses a secret sharing approach to disseminate its group key, which is secure using a group key. By using our protocol, which aids our customers in maintaining the confidentiality of their data while utilising cloud storage, we were able to reduce storage space requirements by 12%.

Introduction

In the realm of corporate systems, cutting-edge big data technologies like cloud computing, BI, data mining, IoT, and industrial information integration engineering all point to a bright future. Distributed computer resources are pooled together as one in cloud computing, a new paradigm in computing. Different applications and services may be given these resources on the fly. Companies may take advantage of modern task execution technology's incredible scalability, adaptability, and efficiency while spending a fraction of the original budget. Businesses may gain more efficiency by using cloud computing services. they spend on smart application supercomputing and grid computing. Regardless of these advantages, storing personal information on such a cloud poses a serious problem [7] [8]. This proposal raises compliance issues since it will transfer sensitive data from a federation domain to a dispersed domain-like structure. Prior to gaining any benefit from big data technologies, it is essential to address the security and privacy concerns mentioned in [9] and [10].
It is not easy to build a system that ensures the security of cloud storage. A solution to the issue of shared data in the cloud might be to make it possible for authorised users to access the data quickly. Good access control is already challenging enough without adding the increasing number of businesses, devices, and applications that rely on the cloud. It is possible to target a larger number of access points. Lastly, there's always the risk of the cloud provider or network hackers erasing or corrupting shared data stored in the cloud. Protecting shared data against tampering, deletion, or falsification is a challenging task.
There are two opposing approaches to guaranteeing the security of a shared system that have existed historically. One way, called network access [11], ensures that no one other than those already listed in the access control table may see any shared files. Group keys [12]_[16] are another option for protecting shared information. Access control systems may assist prevent users from gaining unauthorised access to data, but they won't be able to thwart assaults launched by cloud service providers. The group key is often held in the possession of a third party in classic group major systems. If you want to use these methods, you have to believe that the third party has been reliable from the start. Within the context of cloud storage, however, this assumption is incorrect.
In order to facilitate data sharing in the cloud, the article presents a secret sharing group key management system. This protocol employs many safeguards to detect and prevent fraud. The first stage includes to ensure that allowed users may access the shared data whenever they need it by using symmetric encryption [17] methods. The owner distributes the encryption keys to all authorised users after data sharing is decided upon. The second point is that the person in possession of the decryption key has complete control over the sharing authorities. The interactive communication is encrypted using cryptographic methods [18] that use asymmetric encryption. This means that only authorised participants have the capacity to decode the key. In the case that unauthorised individuals find shared content, the protocol's secret sharing feature may assign a key among permitted participants. By taking precautions to safeguard data stored inside the cloud, we achieve a security-conscious cloud. Given the essential nature of the company scenario, any cloud deployment may go forward quickly thanks to the built-in security features of the cloud storage.

LITERATURE SURVEY

1. "Efficient and secure identity-based encryption scheme with equality test in cloud computing," According to Xinyi Huang et al. (2015) Removing the need to verify certificates is the goal of an identity-based ring signature (ID-based). An ID-based circle signature method was made available, which increased the ring signature's security level. If a user's account is still active after having their secret key hacked, this method can detect it by using previously generated signatures. Successive data owners are unable to re-access compromised medical records when confirm the accuracy of the data. It is especially important for any system that exchanges data on a

big scale, as it is both very effective and doesn't need any combination methods. Because the key update technique requires an exponentiation, while the user secret key is just an integer. This approach is useful, but it needs authentication and, more specifically, user privacy.

2. "A scalable attributed-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing," In 2015, Huang Qinlong and colleagues [2] Presented a cloud computing approach to secure information sharing based on attributes called Efficient Revocation Security (EABDS). The proposed system encrypts data using a symmetrical encryption approach and subsequent encoding of the Data encryption key (DEK) using Ciphertext policy attribute-based encryption (CP-ABE). To solve the key escrow problem, homomorphic encryption may be used with attribute authorities that provide key servers to generate keys only for key attributes. By limiting attribute authority to the creation of secret key attributes, homomorphic encryption technology safeguards data from unauthorised access. By swiftly revoking the qualities, the EABDS system guarantees both forward and backward security and cutting down on user computation expenses. This method yields better results with less mess.

3. "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation," In order to address issues with privacy in cloud storage, Hong Liu et.al. (2015) proposed a SAPA (Shared Authority-based Authentication Protocol) privacy statement. This protocol may be used with several cloud services. Authentication is the mainstay of existing security systems. Shared access permission is achieved using SAPA's anonymous requester matching mechanism. Users may rely on Ciphertext attribute-based access control to access their own data fields. Proxy re-encryption allows data sharing across numerous users. In order to prove that the SAPA is well-designed, the UC model is created. An individual's privacy might be jeopardised if a client has difficulties when using a cloud server and is compelled to request access from other users in order to exchange information. This system safeguards the patient's private information while they are online by controlling who may access it, allowing for the sharing of login credentials, and preserving their privacy. Without sacrificing client privacy, the SAPA protocol ensures authentication and authorization.
4. "Public auditing that protects user privacy in the cloud," In a 2014 study by Xin Dong et al., An effective, flexible, and extensible semantic security data policy was suggested. Two Ciphertex (CP-ABE) tools were employed by them. methods based on Identity Encryption (IBE) provide a safe and dependable way to share data in the cloud and provide dynamic access to that data. Fast and secure dynamic operations, such as file creation, user revocation, or input by the user updates, are provided by their system, which also ensures robust data sharing and defends cloud users' privacy. In addition to reverse secrecy and very effective access control, this system is impenetrable to collusion. Cloud computing may be economical for businesses and consumers alike, but it doesn't protect users' personal information. The proposed approach provides semantic security for data exchange in the cloud by using the generic Bilinear group model in conjunction with access and secrecy confidentially. There is very little overhead when comparing this system's overall performance to existing solutions.
5. The authors of the paper "Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-based Sign encryption" (Qiang Tang et.al., 2014) suggested that MPSE be implemented for multi-party data encryption. By using this feature, users may selectively decrypt their data. In the event of a catastrophe or average situation, an alternative security paradigm is suggested. scenario collusion owing to the dynamics of the individual consumer. He suggested a new system with proven safety. A MPSE security model offers a better safety assurance than that. Authorisation is approved inside the MPSE formulation just at index level; for each of its indexes Alice is able to decide whether or not Bob is able to search for, that means when allkeywords attempt to use authorised Bob, Alice is enabled to allow Bob to search for just a subset of keywords on its indexes and Bob's colluded cloud server is able to recover the keyword for any and all Alice queries. In this MPSE wording Alice is supposedto discover a single trapdoor searching issue for all indexes that she has approved. The drawbacks of this formula include If Alice has several key index pairs and uses them with different peers, it exposes some unneeded information. By contrast, the row - column structure cannot confront this kind of issue.

IMPLEMENTATION

Existing System

- Rao proposed a secure sharing schemes of personal health records in cloud computing based onciphertextpolicy attributed-based(CP-ABE) signcryption. It focus on restricting unauthorized users on access to the confidential data.
- Liu et al. proposed an access control policy based on CP-ABE for personal records in cloud computing as well.
- Huang et al. introduced a novel publickey encryption with authorized equality warrants on all of its ciphertext or a specified ciphertext

Disadvantages

Keep in mind that the project we are doing does not really have an admission control system based on groups.

by anybody in possession of the t-shares. The secret sharing concept became verifiable (VSS) when Chor et al. [32] improved it. The accuracy of shareholders' holdings may be verified.

Advantages

□ Therefore, the data will remain secure due to the fact that the data owner is entirely reliable and unchangeable.

The system's security is severely lacking due to the absence of strong encryption mechanisms. New Approach By using the effective strategy proposed in SSGK, data stored on cloud storage here may be made more secure independently of any third party. An asymmetric algorithm and a secret sharing method were used to increase the difficulty that unauthorised individuals might get the keys that could be utilised to decipher the shared data. In 1979, two researchers, Blakley [30] and Shamir [31], developed secret sharing systems whose only purpose was to safeguard cryptographic keys. Individuals entrusted with a secret might be given a portion of it via a secret sharing arrangement. This mystery might be solved An additional layer of security is provided by the secret sharing mechanism, which distributes a group key. Each team member has the opportunity to uncover and gather several types of sub-secret shares that can be combined to form a group key. Findings and Analysis Consider a distributed storage information imparting framework to various parts; Figure.2 depicts the information sharing paradigm. Cloud provider, data owner, and collecting persons are the three types of components that make up the convention model. Data owners have access to a public platform provided by the cloud provider where they may store and exchange encrypted data. Owners are not able to guide the information access control process with the cloud provider. Any client may freely download the encrypted data. Conventional model of the proposed

ISSN: 2096-3246
Volume 53, Issue 02, June, 2021

A ES
https://doi.org/10.5281/zenodo.12707057

- SSGK for information. The data owner is defined by the entrance strategy and scrambles its information with a symmetric encryption calculation utilizing a gathering key. The gathering individuals who fulfilled the entrance strategy establish a sharing gathering. At that point mystery sharing plan is utilized by the proprietor to disseminate the encryption key to the sharing gathering. Gathering individuals: each gathering part including the information proprietor is appointed with anovel and a couple of keys. The bunch individuals can uninhibitedly get anyintrigued scrambled information from the public cloud. Anyway the client canunscramble the information if and just on the off chance that it get the information decoding key from the information proprietor. In SSGK, we have the accompanying suppositions: The information proprietor is completelytrusted and will never be undermined by any foes. Cloud supplier is semi-trusted,it effectively executes the undertaking appointed to them for benefits, in any case, they would attempt to discover as much mystery data as conceivabledependent on the information proprietors transferred information. We presently portray the security model of SSGK by posting potential assaults. The gatheringkey is dispersed by running the mystery sharing conspire. Portions of the gathering individuals can assemble their subsecret offers to reproduce thegathering key. In addition, the correspondence channel of our convention is characterized as: Every pair of members have a highlight point channel to send messages.

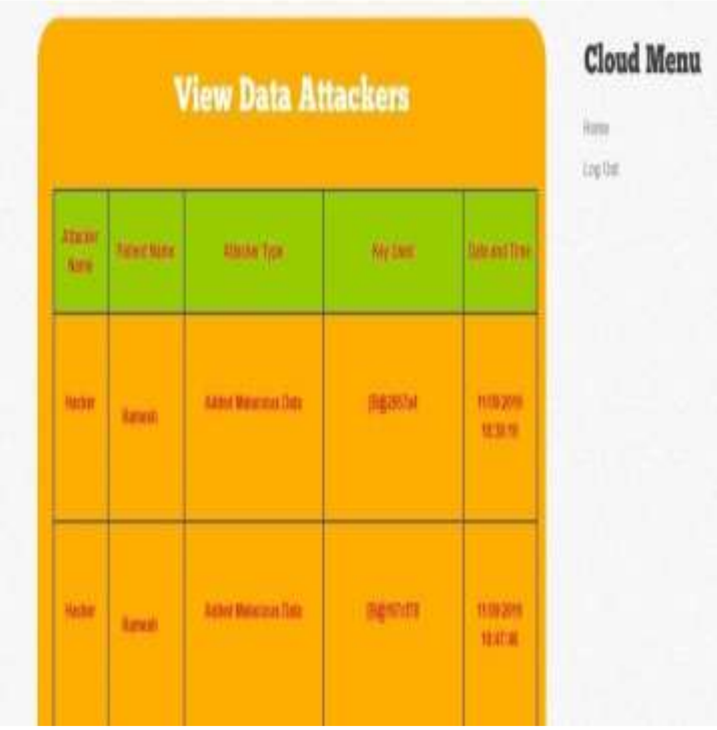
EXPERIMENTAL RESULTS:

[illegible]	[illegible]	Attacker Type	Date and Time	Attacker Name
[illegible]	[illegible]	Key Attacker	[illegible]	[illegible]
[illegible]	[illegible]	Key Attacker	[illegible]	[illegible]

Fig :View Key Attackers

ISSN: 2096-3246
Volume 53, Issue 02, June, 2021

https://doi.org/10.5281/zenodo.12707057



View Data Attackers

Attacker Name	Patient Name	Attacker Type	Key Used	Date and Time
Hacker	Ramesh	Added Malicious Data	[B@2957a4	11/09/2019 18:38:19
Hacker	Ramesh	Added Malicious Data	[B@1671f78	11/09/2019 18:47:46

Fig :View Data Attackers

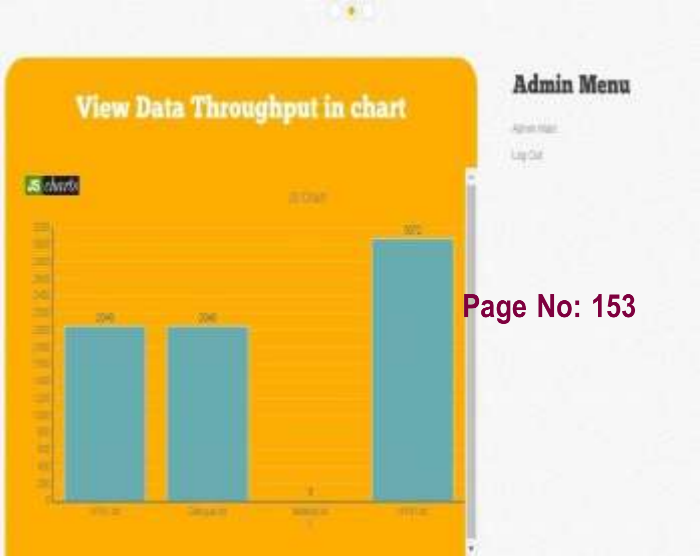


Fig:View Data Throughput inchart

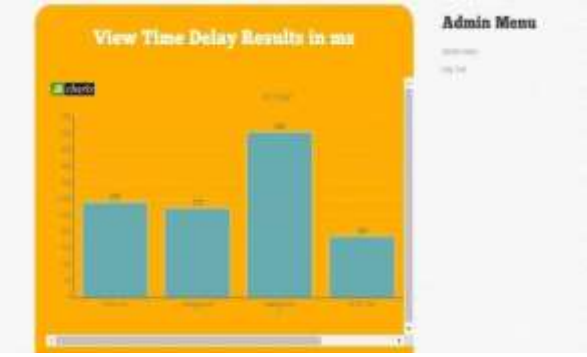


Fig : View Time Delay ResultsCONCLUSIONS

In this article we present a new group key management protocol enabling cloud data sharing. In SSGK, we utilise RSA withvalidated private keys to allow the data owner to have a thorough control of the external data without depending on just about any 3rd person. We also provide thorough analysis of potential assaults and appropriate responses, which shows that GKMP is safe against weaker assumptions.We also show that our protocol has reduced storage and computer complexity. This scheme's security approach ensuresgrid private information in cloud storage. Cryptography ensures public channel transfer; the validated security system makes the grid data available only to authorised parties. Better data and computing performance makes our approach more feasible.

The issue including forward and reversesecurity regarding group key management may need certain modifications to their protocol. The efficient and scalable group members method remains the future work.

REFERENCES

[1] "On minimising energy cost in Internet-scale systems with dynamic data," published in 2017 by IEEE Access, is authored by P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin. [2] "A fuzzy preference tree-based recommender system for personalised business-to-business E-services," published in the IEEE Transactions on Fuzzy Systems, volume 23, issue 1, pages 29–43, in February 2015, by D. Wu, G. Zhang, and J. Lu. "Data mining with big data," in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97_107, Jan. 2014, by X. Wu, X. Zhu, G.-Q. Wu, and W. Ding. "Information ow in reverse logistics: An industrial information integration study," published in December 2012 in the journal Information Technology Management, was written by X. Shi, L. X. i, L. Yang, Z. Li, and J. Y. Choi. “SDN and virtualization solutions for the Internet of Things: A survey” by N. Bizanis and F. A. Kuipers was published in May 2016 in IEEE Access, volume 4, pages 5591–5606. "Integration of hybrid wireless networks in cloud services oriented enterprise information systems," published in November 2012 by Entre- prise Inf. Syst., was written by S. Li, L. Xu, X. Wang, and J. Wang. “Risk and safety programme performance evaluation and business process modeling” (K.-Y. Teng, S. A. Thekdi, and J. H. Lambert, 2012) was published in the IEEE Transactions on Systems, Man, Cybernetics, and Humans, volume 42, issue 6, pages 1504–1513. In the paper "Towards efficient content-aware search over encrypted outsourced data in cloud" published in the proceedings of the 35th Annual IEEE International Conference on Computer Communications (INFOCOM) in April 2016, the authors cite work by Z. Fu, X. Sun, S. Ji, and G. Xie. "Improving privacy and security in decentralised ciphertext-policy attribute-based encryption," published in the IEEE Transactions on Information Forensics Security in March 2015, was written by J. Han, W. Susio, Y. Mu, and J. Hou. [10] "Privacy preserving in cloud computing environment," by D. Zou, Y. Xiang, and G. Min, published in "Secur. Commun. Netw." in October 2016, volume 9, issue 15, pages 2752–2753. [11] "Secure overlay cloud storage with access control and assured deletion," published in the IEEE Transactions on Dependable and Secure Computing, by Y. Tang, P. P. C. Lee, John C. S. Lui, and R. Perlman in

November/December 2012, pages 903-916. The paper "Fine-grained data sharing in cloud computing for mobile devices" was presented at the 2015 IEEE Conference on Computing and Communications (INFOCOM) and was written by J. Shao, R. Lu, and X. Lin. [13] "Privacy preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362_375, Feb. 2013, by C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. [14] "Proposal for secure group communication using encryption technology," in Proceedings of the 9th International Conference on Mobile Computing and the Internet of Things, October 2016, pages 1–6, by S. Tanada, H. Suzuki, K. Naito, and A. Watanable. The article "Securing outsourced data in the multi-authority cloud with _ne-grained access control and efficient attribute revocation" was written by J. Zhou and colleagues in August 2017. It can be found in the Computer Journal, volume 60, issue 8, pages 1210-1222. [16]An extensible attribute-set-based access control system that supports both sharing and full-computational electrical engineering, volume 57, pages 241–256, January 2017, "edged delegation of access privileges in cloud computing." Citation: "AES and blow_sh: Symmetric key cryptography algorithms simulation based performance analysis" by J. Thakur and N. Kumar in the International Journal of Emerging Technology and Advanced Engineering, volume 1, issue 2, pages 6-12, December 2011. The article "Secure integration of asymmetric and symmetric encryption schemes" was published in January 2013 in the Journal of Cryptology and was authored by E. Fujisaki and T. Okamoto. In Feb. 2017, Y. S. Rao published an article titled "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing" in the journal Future Generation Computer Systems, volume 67, pages 133–151.

[20] "Attributed-based encryption schemes," published in 2011 in the Journal of Software, edited by S. Jin-Shu, C. Dan, W. Xiao-Feng, and S. Yi-Pin. In their 2015 November article titled "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," H. Liu, Y. Huang, and J. K. Liu discuss ciphertext-policy attribute-based encryption.

[22] "PKE-AET: Public key encryption with authorised equality test," published in October 2015 in the Computer Journal, by K. Huang et al. An "Ef_cient and secure identity based encryption scheme with equality test in cloud computing" was published in the August 2017 issue of Future Generation Computer Systems by L. Wu, Y. Zhang, K.-K. R. Choo, and D. He.