Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

A SURVEY OF VARIOUS DATA SHARING METHODS IN SECURE COMMUNICATION IN CLOUD COMPUTING

Sudhakar Veledendi[1], Niranjan Polala[2], Tarasvi Lakum*[3]

[1] Department of Computer Science & Engineering, S.R.University, Ananthasagar,

[2,3*] Department of Computer Science & Engineering , Kakatiya Institute of Technology & Science, Warangal , Telangana, India.

Hanamakonda, Warangal, Telangana, India.

Abstract

The cloud is thoughtful application of security controls, creating a demand for best practices in the security program and governance regimes. Cloud Security and Privacy provides a guide to support those who are contend with building security in the cloud. In this survey paper, we discuss about security authentication between data accessing users and creating methods of parties to jointly compute a function of their inputs access while keeping those inputs private without knowing unauthorized party. To securely share the data onto others with the help of cloud storage and discussing with existing methods used for sharing the data onto secure communication.

Keywords- Secure multiparty authentication (SMA), Security, Renewal, Privacy, Communication.

1. INTRODUCTION

The next step in the advancement of the internet is cloud computing, which offers the means by which everything from computing resources, to computing technology, software and business processes can be offered as a service to you anywhere you need it. Cloud computing allow us to purchase, update, upload, download and safeguard all of our computing on the Internet as a feasible option, physical devices, operating systems and software otherwise are controlled. It does not entail a significant initial investment, so you are just "renting" what you need and what you need. Your PC is primarily used to run a Web browser for cloud storage. Remote servers (or virtual servers) and applications will spread across the internet, hence the term cloud, are responsible for physical computing and data computing.

The word "as a service" is freely used in cloud terms to mean the right to access anything over the Internet as appropriate. The terms software, operating systems and hardware are confusingly described as Cloud Software (or Software-as-a-Service), Cloud Platforms (or Platform-as-a-Service) and Cloud Infrastructure (Infrastructure-as-a-Service). The acronyms SaaS, PaaS and IaaS are often used to render matters lower.

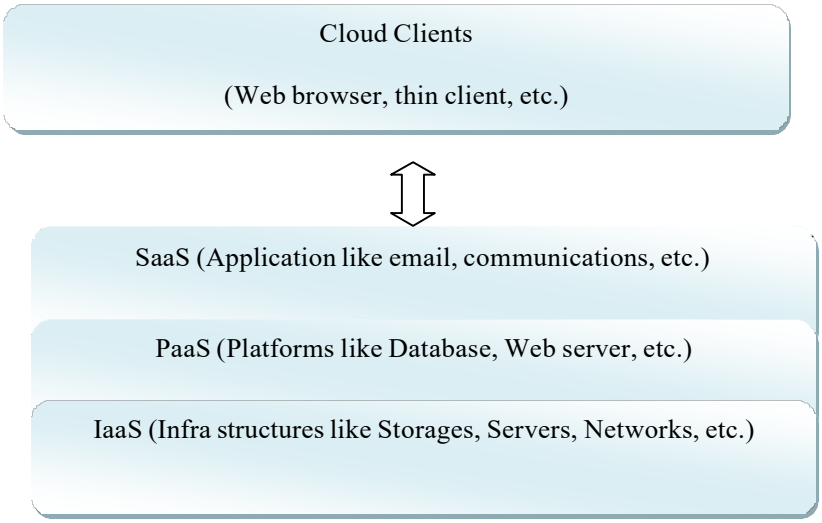

Figure1. Cloud Service Architecture

Cloud computing is meant to be part of our daily lives, but it isn't science. Software is not delivered over the Internet from a central computer. Cloud computing is a modern way of thought, and this is important if we are to be competitive and productive in the current economy. Here are just few drivers that demonstrate the importance of cloud computing:

• **Explosion of data**. Today, we sure are in the 'information age.' That means we depend more than ever on information in the past, but it also means a lot.

• **Renewed focus on collaboration**. Information is normally of better benefit if it is exchanged strategically, not only within a business, but also with partners, vendors, outsourcers and other parties involved around the world.

• **Economic necessity**. Companies are continually faced with the need to reduce costs, especially during the worst economic downturn since the 1930. But global competitiveness and other trends have led businesses, amid the crisis, to pursue

significant cost saving measures. This ensures that all new strategies are applied and the workers are eliminated.

• **Entrepreneurial activity**. The economic crisis has a positive effect on entrepreneurship. As a result, smaller enterprises today are more than ever, and small firms require low cost access to capital. Cloud computing provides these small enterprises with access to the resources they need to thrive.

• **Outsourcing**. Cloud computing and outsourcing go hand in hand. The outsourcing movement is motivated by the economic need mentioned above and it thrives from two viewpoints because of the high degree of entrepreneurship we see. Most of the small businesspersons who today start their enterprises are contracting suppliers. In addition, the need for outsourcing is motivated further by the demand by larger existing corporations for cost savings. The basis for outsourcing to occur is cloud computing.

• **Teleworking and telecommuting**. Yes, people are working at home, and companies are allowing it, in part out of the effort to keep costs in check. Cloud computing has provided the framework to allow a new era of working at home to become reality.

In today's world, security is highly critical. Cyber criminals and other kinds of individuals with black hats try to hack into the network and to make personal profits, and cyber attack casualties are enormous every year. With firewalls, anti-virus and anti-malware software, physics security, including locked data centers, and complicated authentication and authorization methods, we are taking great strides to secure our personal information and network. When laptops are misplaced, severe economic signs and computer protection concerns can occur; but, because all is saved on the cloud, data may also be retrieved regardless of what happens on the system because data is not saved physically on the system.

Since cloud infrastructure is a modern computing paradigm, a lot of confusion exists about how security can be accomplished at all levels (e.g. network, host, service, and data levels). This complexity often prompted information managers to suggest safety is their main concern for cloud computing.

The model is used when accessing data into a multi-partner community to protect authentication and provide cloud storage support. Encryption helps to avoid unauthorized

access to files. Data sharing is an important functionality in cloud storage. For example, blogs can encourage their friends to see a subset of their private photos; a company can provide its staff with access to any confidential data. The complicated challenge is how to exchange encrypted data efficiently.

Users can of course extract encrypted data from the storage, decrypt it, and transfer it to others, but the importance of cloud storage is being lost.

In order to have direct access to these data from the server, users can assign access rights to the share data to others. However, it is important to find an effective and safe way to share data in cloud storage.

2. SURVEY FOR EXISTING TECHNIQUE

The methods of data sharing in the Cloud are secure as well as effective with assured multi-party distribution. The two major challenges in cloud computing are security and reliability. Other users can access the data of the customer via the cloud. Security concerns emerge regarding consumer records. There are too many methods and algorithms accessible to ensure cloud data protection. Some of these are:

- Encryption - A method that uses complicated algorithms to hide the original information using the encryption key.
- Authentication processes - which, create a user name and password for data access.
- Authorization practices - Provide users who can use cloud-specified data with authorization.

Encryption

The following are discussed and summarized certain encryption methods, used in the existing system

Xuefeng Liu et al [1] presented Sharing data in Multi owner manner still preserving identity and data privacy due to frequent change of membership. The authors in this paper recommended that multi-owner data sharing be carried out for complex communities. Group signature and dynamic encryption broadcast technologies was used to exchange data in one group with other members. Without updating the secret key of the residual individual, revocation can be quickly accomplished by way of revocation lists and gives individual

verified entry. New granted user decrypts data file directly without the data owner being informed. Calculation cost for encryption, overhead storage is irrespective of users that have been revoked.

Boyang Wang et.al [1] has envisioned that data can be easily shared by group. The revoked user data block resigned by existing user, when the user is revoked from the group. A new public monitoring system has been proposed in this paper on the integrity of the data exchanged with successful user revocation.

This approach was used to re-sign proxy data strategy, which helps the user to resign the revoked user block and does not need to retrieve server data in order to checks the integrity of data exchanged and to protect the integrity of the data. Shamir's secret sharing has been applied to a multi-proxy model to decrease the probability of violence. Further development focus on collusion resistant proxy re-signature. It does not accept the investigation of the public.

Yuqing Zhang proposed "MODS" (Multiple Owner Data Sharing) method presents the design of the secure data sharing mechanism for dynamic groups in an insecure cloud, including group signature integration and broadcast encryption techniques [1]. This way dynamic community supports i.e. without upgrading the remaining users, users can quickly be revoked by revocation list and new users can decrypt data files without consulting the dataset holders. The scale and calculated costs of encryption thus depend on the number of users revoked. This device established certain performance and safety drawbacks. Even in the revocation list, after expire users cannot access the data for each user until the Community Admin changes and gives it to the cloud the time allocated to each user.

Cong Wang et al [3] are the first to consider that, Secure cloud storage system supports privacy-preserving public auditing. Users can retrieve TPA and check the integrity of cloud-based data stored. It consists of four algorithms, namely key generation, signature generation, proof generation, and proof verification. The MAC based approach provides the consumer with extra management and HLA expenses and does not support privacy preserving. The drawback of this scheme is auditing a specific file is restricted and a secret key must have a fixed priority. In this paper public key based Homomorphic linear authenticator and HLA with random masking technique is suggested. It consists of two levels, including setup and auditing. In order to protect the user's identity, TPA will check data integrity without knowing original information.

Wang proposed scalable and fine-grained data access-control scheme by defining access polices based on data attributes and KP-ABE technique [2]. The combination of ABE and proxy re-encryption and lazy re-encryption allows the database owner to allocate the device to insecure servers without disclosing the necessary data information. Data files are encrypted by data owner using a random key.

The random key is further encrypted with a collection of attributes via key policy attribute-based encryption (KP-ABE). Then an access structure and the linked secret key by group admin are allocated to approve members. Only the user with data file characteristics that meet the access structure can thus decrypt a cipher text. This system has some drawbacks, as this system does not support multiple-owners such that certain individual owner's embodiments make it less versatile, as group admin alone is responsible for altering the shared data file.

Authentication processes

Chow et al. [4] proposed an authentication platform for cloud based policies. This system is simple and scalable to deal with the problem of client application authentication. The framework suggested uses the Trusted Cube to control the authentication infrastructure and authenticate the user actions. Implicit authentication is called behavioral authentication. Behavioral authentication uses habits to authenticate users instead of text data or biometrics. Customer devices are given probability authentication ratings depending on the actions they detect using a statistical model. This authentication system contrasts threshold values with a user authentication score to see if it is the correct user's hand. However, it is up to the authentication provider to recognize a valid customer. As the user increases, the efficiency declines with third party authentication.

Yu et al. [5] proposed a new cryptographic method to secure data access control and data outsourcing in semi-untrusted Cloud servers using the Key Policy-Attribute-Based Encryption (KP-ABE) scheme. The author also applied re-encryption scheme in revocation phase to reduce the data cost. Due to the frequent node reversals, the ABE-based approach cannot be efficient in a dynamic mobile cloud. The disadvantage of the ABE method is that data shareholders should be known before encryption.

Prachi Soni, et al., [6] proposed a multi-factor authentication framework for implementing the data security in cloud environment. During the service provision of the

user, the developed multifactor system examines various features such as confidentiality, integrity, privacy, and authentication. The author establishes security through the zero-skill protocol that successfully encrypts the cloud service provider's user information. The system's efficiency is assessed by the experimental results. On the basis of the above claims, the multi-factor authentication process is used to create cloud security. This paper presents the homomorphic encryption algorithm based on the cipher-text policy attribute, which ensures security by three steps. The author uses the digital signature and image captcha to identify successful security in the cloud environment during the encryption process.

Guo, M.; Liaw, H.; Hsiao, L.; Huang, C.; and Yen, C. proposed a method in which Tenants are also authenticate dusing graphical passwords. The algorithm operates when the tenant selects one image from many images and then draws a correct pattern for authentication [7]. This algorithm is vulnerable to attacks by surfers. Another concern is that the images are saved locally, meaning that authentication is not feasible if the system crashes.

Reference No.	**Algorithm/Technique**	**Advantage**	**Disadvantage**
3	privacy-preserving public auditing	User can resort TPA and verify integrity of stored data in cloud storage	Auditing a specific file is limited and secret key must be of fixed priority
2	novel public auditing mechanism	integrity of the shared data with efficient user revocation was proposed	Not support public auditing.
1	secure multi owner data sharing for dynamic groups	User revocation can be easily achieved through revocation list without updating secret key of the remaining user and also provides control access to the users.	Encryption computation cost, storage overhead of the proposed scheme is independent of the revoked users
4	policy based cloud authentication platform	authentication platform in which behavioural authentication is used based on client personal data	passing the personal information of the client to cloud can affect the user privacy

5	novel cryptographic approach using Key Policy-Attribute Based Encryption (KP-ABE) scheme	re-encryption scheme in revocation phase to reduce the data cost	ABE as method is the attributes of the data sharers that should be known before encryption
6	cipher text policy attribute based homomorphic encryption algorithm	the digital signature along with image captcha for establishing the efficient security in the cloud environment	The system may not work well when enterprise users outsource their data for sharing on cloud servers
7	Authenticate dusing graphical passwords	then tenant draws a correct pattern to get authenticated	the images are stored local ly so if the device crashes, authentication would not be possible

Table shows the existing methods

3. PROBLEM DEFINITION

- Cloud provides the service for the user to utilize on-demand cloud applications without considering the local infrastructure limitations.
- During a data sharing in group user's privative data cannot be illegally accessed, but neglect a restrained privacy issue during a user demanding the cloud server to request other users for data sharing.
- In case of data accessing, many of the users may be in a collaborative relationship and thus data sharing /forwarding becomes significant to achieve the productive benefits.
- Security parameters in cloud environment, an on-demand cloud application for a group is difficult to maintain and sustain.
- Time consumption for data sharing and accessing is high during group communication.
- In the multi group cloud, anonymous modify the shared access request. So that requester and provider cannot able to access the original data.
- Then, there are demands for some applications to move their data in the Cloud and centralize executive for data center, services and applications are designed to achieve cost savings and operational efficiencies.
- Multi user data from dynamic cloud pose serious challenges for cyber operations because an ever growing number of applications in the cloud and the amount of

complex monitoring data collected from critical cloud environment require scalable methods to capture, store, manage, and process the big data.

4. COMPARISON OF EXISTING WORK

The comparison of existing work under various file sizes while sharing the data in multi-party group. First, the paper output for various file sizes is built on the basis of user sharing. Then the time is evolved for cryptographic operations.

This paper can only be done by having random download times on every volume of file. The key control of encryption methods is the essential part of how data are encrypted. The failure of the picture is dependent on the encryption ratio. The symmetrical algorithm uses a longer variable key length. The key control in the encryption process is also a significant feature. Computational speed it is critical in many real-time applications that encryption and decryption algorithms fulfill real-time requirements as soon as possible.

Algorithm	**Data confidenti -ality**	**Ciphertext size**	**Scalability**	**User revocation**	**User Account —ability**	**Executio n time**
CP-ABE	Medium	Larger	High	Yes	Less	Slow
MODS	Moderate	Larger	Medium	Yes	High	Slow
KP-ABE	moderate	Larger	Medium	Yes	Less	slow
Group signature and dynamic broadcast encryption	Moderate	Larger	High	no	High	fast

Table 1 shows the techniques comparison

Encryption and decryption Ratio: The encryption ratio is the calculation of the number of data to encrypt. Encryption ratio should be minimized to reduce the complexity on computation. User Revocation is carried out by the manager of the group.

On the basis of these, Delta Revocation List is open to the public and members of the party are permitted to encrypt and depend on the revoked users. The users who are revoked

shall be kept in the user list and freely accessible in the cloud. In the case of its authenticity, Delta RL shall be bound by signature. Once the Group Member has submitted the application for resignation, the Group Member is classified as revoked.

The cloud itself performs the resigning; this scheme improves the efficiency of user revocation thereby reducing the communication and computational overhead**.**

Data confidentiality The data owner stores their data into the cloud and shares them with the members of the group. Anyone who uploads the data has the right to modify and delete its cloud data.

Algorithm	**Encryption ratio for 100KB (milliseconds)**	**Decryption ratio 100KB (milliseconds)**	**Buffer size**
CP-ABE	8	83	157
MODS	7	64	100
KP-ABE	5	78	178
Group signature and dynamic broadcast encryption	8	50	192

Table 2 for encryption, decryption ratio comparison techniques

5. CONCLUSION

In this paper we provide the survey of authentication between the users while share the data in the multi-party group. Security authentication is given to the data, which can be accessed by the user, and methods are developed for parties who are interested in measuring the user accessed input feature that is kept secret from unauthorized party. Policy renewal data accessing can be renew key is added to the file. If the user wishes to renew the file he / she can download and change all renew keys directly and then upload, the new renew keys to the files in the cloud. Existing Techniques are compared with each other also find some drawbacks. In order to overcome the drawbacks of existing system is enhanced with privacy which expects to obtain more efficiency and guaranteed output delivery.

References:

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "MODS: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions On Parallel and Distributed Systems, Vol.24, No. 6, June 2013.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534- 542, 2010.

[3] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245

[4] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi and Z. Song," Authentication in the clouds: a framework and its application to mobile users," in Proceeding ACM Cloud Computing Security Workshop, CCSW '10, Chicago, USA,Oct. 2010

[5] C. Wang, S. Yu, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing", In Proc. of INFOCOM, IEEE, 2011, pp.534–54.

[6] Prachi Soni, MonaliSahoo, "Multi-factor Authentication Security Framework in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, volume 5,issue 1,2015

[7]Guo, M.; Liaw,H.; Hsiao, L.; Huang,C.; and Yen, C.,"Authentication using graphical pass word in cloud", Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , pp.177-181, 24-27 Sept. 2012.

[8] U. Padmavathi, C.Mohammad Gulzar "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" ,SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 2 issue 6 June 2015.

[9] Melissa Chase and Sherman S.M. Chow "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", IEEE, 2010.

[10] Sonia Jahid, Prateek Mittal and Nikita Borisov"EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation", IEEE, 2011.

[11] S.Ramamoorthy and R.Saravanan "sharing secure data in the cloud For the multiuser group" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Volume 3, Issue 1, January – February 2014.

[12] M.Kavya and M.V. Jagannatha Reddy,"Privacy Preserving Data Sharing in Multi Groups", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014, 6926-6928.

[13] M. Kavitha Margret, "Secure Policy Based Data Sharing for Dynamic Groups in the Cloud" International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 6, June 2013.

[14] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu," Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, 2014.

[15] Taware Sangram, Zargad Ameya, Waghmare Raju, Ghodke Omkar, Prof.A.A. Chavan, "Secure Data Access in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2016.

[16] Hong Liu, Huansheng Ning, Qingxu Xiong, and Laurence T. Yang," Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems,2013.

[17] R. Ranjith, D. Kayathri Devi, "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.

[18] S.Senthil Kumar, Christo Paul.E, Nilutpal Bose, " Secure Data Sharing For Dynamic Groups in the Cloud Using Broadcasting Encryption Techniques" International Journal of scientific research and management (IJSRM), ISSN (e): 2321-3418 Vol. 2, Issue 4, pp 719-723, 2014.

[19] R. Lu, X. Lin, X. Liang, and X. Shen, ―Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing, Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[20] S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing Proc. IEEE INFOCOM, pp. 534-542, 2010.