International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A SURVEY ON SECURITY AND DATA SHARING ISSUES IN CLOUD ENVIRONMENT

Dr.P.Maragathvalli[1], G.Hemalatha[2]

[1,2]*Information Technology, Pondicherry Engineering college, (India)*

ABSTRACT

Cloud Computing is an emerging business trend. The cloud is porous in nature, and this makes it an attractive target by attackers and providing security has become more complex as the site. Cloud computing security protect critical information from theft, data leakage and deletion. Cloud data sharing allows people to store and synchronize documents, photos, videos and other files in the cloud and share among group of people.There is a need for both the enterprises and the cloud service providers to ensure security that they focus on the core elements of well secured cloud such as identity and access management, virtualisation security, content security, threat management and data privacy. Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location via the internet. This paper focuses on the security and data sharing issues in cloud environment.

Keywords- Cloud storage, cloud services, Data sharing, Data privacy, security issues.

I. INTRODUCTION

Cloud computing has become a popular buzzword and they have been widely used to refer to different technologies, services, and concepts. It is often associated with virtualized infrastructure or hardware on demand, utility computing, platform and software as a service, and many other things that now are the focus of the IT industry.

As cloud adoption continues to grow rapidly at the enterprise level, IT and security departments should provide for secure use of cloud storage and services. The benefits brought by cloud storage – from scalability and accessibility to decreased IT overhead – are driving rapid adoption at enterprises around the world, and there are steps that companies should take to improve cloud storage security and keep sensitive data safe and secure in the cloud.

A. THE NEED FOR CLOUD STORAGE SECURITY - The rise of Internet of Things (IoT) technology and the connected office has also made enterprises more reliant on cloud technology, albeit while driving security risks. Even smart printers have been found vulnerable to data leakage, and as more corporate devices become internet-connected, the potential for compromise or unintended leakage increases.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

B. CLOUD STORAGE SECURITY CONCEPTS - Cloud storage providers and enterprises share responsibility for cloud storage security. Cloud storage providers implement baseline protections for their platforms and the data they process, such authentication, access control, and encryption. From there, most enterprises supplement these protections with added security measures of their own to bolster cloud data protection and tighten access to sensitive information in the cloud.

C. CLOUD STORAGE SECURITY CHALLENGES One of the biggest challenges with cloud storage security is that employees use free file sharing and cloud storage services that are not approved by the organization and may not meet minimum security standards. Knowingly or not, employees can putcompany data at risk by using these services, particularly without the IT department's knowledge or approval.

Cloud-based data sharing is used as an alternative to backup solutions or by small and medium-sized businesses (SMBs) that want to give employees flexibility in their file accessibility, it's clear the technology is gaining traction as a business tool. Dozens of vendors have cropped up with cloud-based document sharing or file sharing in the cloud products designed toward customers ranging from individuals to organizations.

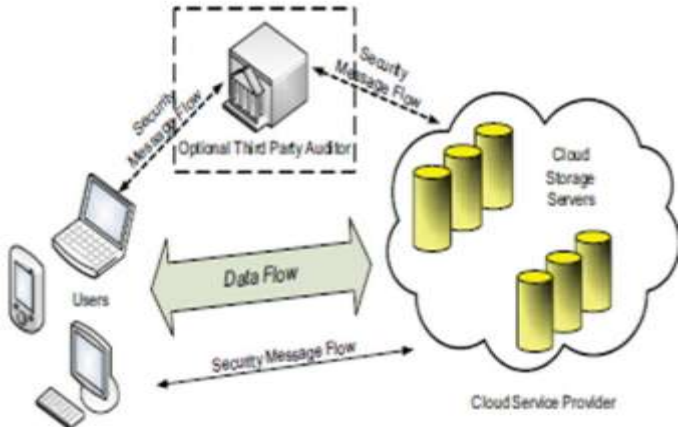

Fig.1 Cloud storage architecture

D. WAYS TO SHARE FILES WITH CLOUD STORAGE

- **Email Sharing** - Share files using email addresses. When a recipient gets the email, they can open the link to a secure area where they can download the files. Some cloud providers require the recipients have an account.

- **Social Network Sharing** - Posts a link on your social network's profile that directs people back to the shared file. It relies on your social network's privacy settings to be set to what you want and is shared to friends/followers that you have already approved.

- **Public URL Sharing -** Creates a URL that links directly to your shared files. Anyone with the link can access these files, which means it's up to the user to send out the URL responsibly.

• **Pre-registered User Sharing** - Requires that everyone is registered under a network of accounts, usually for business accounts. Teams can collaborate using the providers interface and makes it easy to share files between connected users. Privacy and permissions can be set within the cloud software.

In the enterprise, cloud data sharing can present security risks and compliance concerns if company data is stored on third-party providers without the IT department's knowledge. Popular third-party providers for cloud data sharing include Box, Dropbox, Egnyte and Syncplicity.

Cloud encryption is the transformation of a cloud service customer's data into cipher text. It is almost identical to in-house encryption with one important difference - the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. It is capabilities of the service provider need to match the level of sensitivity of the data being hosted.

II. CRYPTOGRAPHIC TECHNIQUES

Cryptographic techniques have become essential for security in cloud. A key is used for data encryption and decryption. This helps in protecting confidentiality and integrity of data. It ensures security of data being shared in cloud and also allows data to be stored securely.

Cryptography refers to the science of designing ciphers. Encryption refers to the method of converting plain text to secret text (cipher text) which can only be read by owner of secret key. At present various cryptographic algorithms are there which belong to two major categories

I.Symmetric algorithms such as DES, AES, Triple DES

II. Asymmetric or public-key encryption algorithms such as RSA, Diffie-Hellman, ECC, etc.

The difference is in the way the keys are used. In symmetric key encryption, the person who is sending the data and the person who is receiving the data share a key which is kept secret. This is then used to encrypt and decrypt the messages. In asymmetric key encryption, two keys are involved wherein one is used for encryption (this is publicly available) and the other is used for decryption (this is kept secret).

- **Identity-based encryption (IBE),** is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). It allows any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. This kind of encryption reduces the complexity of the encryption process for both users and administrators.

- **Attribute based encryption [2]** - It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). A user can encrypt a message under a public key and a policy. Decryption will only work if the attributes associated with the decryption key match the policy used to encrypt the message.

- **Fully Homomorphic Encryption** - Homomorphic encryption ensures privacy of data in communication, storage or in use with tools similar to conventional cryptography, but with extra features of computing over encrypted data, searching an encrypted data, etc. Search and manipulation of cipher text was difficult with traditional encryption techniques.
- **Proxy re-encryption**-Proxy re-encryption is a form of public-key encryption that allows a user Alice to "delegate" her decryption rights to another user Bob. Alternative solutions to this problem typically require Alice to divulge her secret key to Bob, or to enroll in some sort of key escrow system. This may be undesirable for a variety of reasons. In a proxy re-encryption scheme, Alice delegates a semi-trusted proxy to translate cipher texts encrypted under her key into cipher texts encrypted under Bob's key. Once delegated, the proxy operates independently of Alice. The proxy is considered "semi-trusted" because it does not see the content of the messages being translated, nor can it re-encrypt Alice's messages to users for whom Alice has not granted decryption rights.

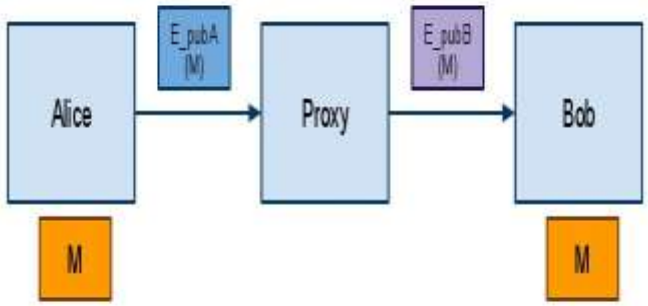

Fig.2 Example for proxy re-encryption

- **Key-aggregate searchable encryption(KASE)** method of data sharing it consists of two types of users: Data owner and Data user. Data owner is uploading n numbers of documents to cloud server which are shared with the data user. Generally, here documents are encrypted by a key pair, this obtained key pair is changed into single aggregate key by using data owner public key and master secret key. The single aggregate key produced is send to the data user via a secure communication channel. Data user can perform searching over the shared documents by generating single aggregate trapdoor. For each searched word, it can generate an aggregate trapdoor. If a match is obtained, the shared documents are unlocked and returned to respective authorized data user. units may be used as secondary units.

- **Cipher text-policy attribute-based encryption**

In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext.

Policies may be defined over attributes using conjunctions, disjunctions and (k,n)-threshold gates, i.e., k out of nattributes have to be present.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice features are; that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

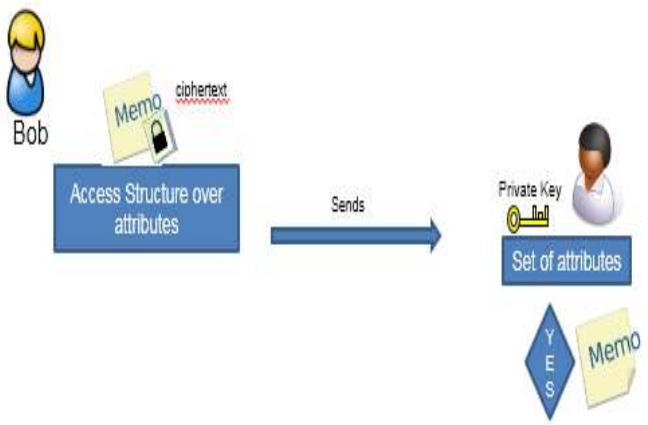

Fig.2 Cipher text-policy attribute-based encryption

- **Key-policy attribute-based encryption**

KP-ABE is the dual to CP-ABE in the sense that an access policy is encoded into the user's secret key. Encrypted data is described by a set of attributes, and access rule contained in the user's private key. If a set of attributes of data matches the structure of access to the user's private key, the data can be decrypted. Attributes of encrypted data correspond to the structure of the access user's private key, so the user can decrypt the data. The encryption algorithm is different from the original version of the ABE generating the private key and accordingly decrypt: the user's private key is generated by according to the structure of the necessary access. By separating secret for the vertices from the root to the top of each end x selected polynomial q_x such that $q_x(0)=q_{parent(x)}(index(x))$, where $parent(x)$ is node relative to the parent x, and $index(x)$is number tops x among the peaks belonging to the same parent. In this way, $q_r(0)$ corresponds to master key y, which is distributed on the leaves of the tree, the corresponding components of the private key. e.g., (A∧C) ∨D, and a ciphertext is computed with respect to a set of attributes, e.g., {A, B}. In this example the user would not be able to decrypt the ciphertext but would for instance be able to decrypt a ciphertext with respect to {A, C}.

III.LITERATURE SURVEY

Comparative analysis of the several encryption techniques utilized in providing security to the cloud are given in the following table.

SL.NO	AUTHORS	PAPER TITLE	MONTH & YEAR	PROBLEM	TECHNIQUES	ADVANTAGES
1	Guofeng Lin, Hanshu Hong, and Zhixin Sun	A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing[1]	May 2017	To solve key escrow problem, key exposure and reduce client decryption overhead.	Collaborative key management protocol in CP-ABE	Enhance both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system.
2	Rohit Ahuja, Sraban Kumar Mohanty, Kouichisakurai	A Traceable Signcryption Scheme for Secure Sharing of Data in Cloud Storage[3]	December 2016	To trace the traitors, who intentionally leaked their data access privileges for personal gain	Traceable cipher text policy attribute-based signcryption	It allow users to modify data on cloud servers and device computationally efficient traceable signcryption scheme for mobile devices.
3	Linmei Jiang, and DonghuiGuo,	Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud	August 2015	To protect data from being disclosed, Since CSP is a semi-trusted party in cloud storage.	Conditional Proxy Broadcast Re-Encryption for Data Sharing	Size of user set is not limited. Users taking part in and quitting the sharing group dynamically and freely

		Storage[4]				
4	Kaitai Liang and Willy Susilo	Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage[5]	2015	Secure share and search for the outsourced data is a formidable task, which may easily incur the leakage of sensitive personal information	Attribute-Based Proxy Re-Encryption	Chosen Cipher Text Attack integrate searchable attribute-based encryption with attribute-based proxy re-encryption, which is applicable to many real-world applications.
5	Baojiang Cui, Zheli Liu and Lingyu Wang	Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage[6]	2014	Sharing encrypted data with different users via public cloud storage may concerns that data leaks in the cloud storage	Key-aggregate searchable encryption	Owner only needs to distribute a single key to a user and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner.
6	Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage[7]	2013	To share data with others in cloud storage by secure, efficient, and flexible manner	Key-aggregate encryption	Key-aggregate cryptosystem is more flexible than hierarchical key assignment which can only save spaces The delegate can always get an aggregate key of constant size.

TABLE 1.COMPARATIVE STUDY ON EXISTING WORKS

IV.SECURITY ISSUES IN CLOUD COMPUTING

The most important classes of cloud-specific risks are:

1. **Loss of governance:** In using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues that may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences. This also includes compliance risks, because investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud:

- If the CP cannot provide evidence of their own compliance with the relevant requirements
- If the CP does not permit audit by the cloud customer (CC). In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS).

2. **Lock-in:** There still is little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

3. **Isolation failure:** Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and reputation between different tenants (e.g., so-called guest-hopping attacks). However, it should be considered that attacks on resource isolation mechanisms (e.g., against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

4. **Management interface compromise:** customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

5. **Data protection:** Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification

summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

6. **Insecure or incomplete data deletion:** When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

7. **Malicious insider:** While usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

8. **Customers' security expectations:** The perception of Security levels by Customers might differentiate from the actual security (and availability) offered by the CP, or the actual temptation of the CP to reduce costs further by sacrificing on some security aspects.

9. **Availability Chain:** Reliance on Internet Connectivity at Customer's end creates a Single point of failure in many cases.

V.CHALLENGES IN CLOUD DATA SHARING

1. **Data leakage** - Most of the businesses that have held back from adopting the cloud have done so in the fear of having their data leaked. This feat stems from the fact that the cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. It is only human nature to doubt the capabilities of a third-party, which seems like an even bigger risk when it comes to businesses and sensitive business data.

2. **No control over data-** The problem here is that when using third-party file sharing services, the data is typically taken outside of the company's IT environment, and that means that the data's privacy settings are beyond the control of the enterprise. And because most cloud services are designed to encourage users to back up their data in real-time, a lot of data that wasn't meant to be shared can end up being viewed by unauthorized personnel as well. The best way to avoid such a risk is by ensuring you're your provider encrypts your files during storage, as well as transit, within a range of 128 to 256-bit.

3. **Bring Your Own Device (BYOD)** -Another emerging security risk of using cloud storage and FSS is that they have given employees the ability to work on a Bring Your Own Device (BYOD) basis. And this trend is set

to increase as more employees prefer to use their own devices at work, either because they're more used to their interfaces or have higher specs than company-provided devices. Overall, BYOD has the potential to be a win-win situation for employees and employers, saving employers the expense of having to buy IT equipment for employees while giving employees more flexibility.

4. **Snooping** -Files in the cloud are among the most susceptible to being hacked without security measures in place. The fact that they are stored and transmitted over the internet is also a major risk factor. And even if the cloud service provides encryption for files, data can still be intercepted on route to its destination. The best form of security against this threat would be to ensure that the data is encrypted and transmitted over a secure connection, as this will prevent outsiders from accessing the cloud's metadata as well.

5. **Key Management** - The management of cryptographic keys has always been a security risk for enterprises, but its effects have been magnified after the introduction of the cloud, which is why key management needs to be performed effectively. This can only be done by securing the key management process from the start and by being inconspicuous, automated, and active. This is the only way to ensure that sensitive data isn't vulnerable when it is going to the cloud.

6. **Cloud Credentials** - The basic value proposition of the cloud is that it offers near-unlimited storage for everyone. This means that even an enterprise's data is usually stored along with other customers' data, leading to potential data breaches via third parties. This is mitigated - in theory - by the fact that cloud access is restricted based on user credentials; however, those credentials are also stored on the cloud and can vary significantly in security strength based on individual users' password habits, meaning that even the credentials are subject to compromise. While a credential compromise may not give attackers access to the data within your files, it could allow them to perform other tasks such as making copies or deleting them.

VI.CONCLUSION

Cloud computing is affordable, efficient, and scalable, and still the best solution for most businesses.While the cloud may be flexible and cost-efficient, a lack of data safeguards and compliance standards makes security the largest hurdle to leap.Cloud Storage is a service where data is remotely maintained, managed, and backed up, but it is not easily usable and accessible. To overcome this issues Conditional proxy broadcast re-encryption for data sharing, Attribute-based proxy re-encryption, Key-aggregate searchable encryption and Key-aggregate encryption techniques are used. Still these techniques do not rectify all the issues but minimize the damage of the data.

REFERENCES

[1.] Guofeng Lin, Hanshu Hong, and Zhixin Sun, *"A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing"* IEEE Access,2017

[2.] Mazhar Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li and Albert Y. Zomaya, *"SeDaSc: Secure Data Sharing in Clouds",* IEEE Systems Journal, *Vol 11, No. 2, June 2017, pp. 1-10.*

[3.] Rohit Ahuja, Sraban Kumar Mohanty, Kouichisakurai, *"A Traceable Signcryption Scheme for Secure Sharing of Data in Cloud Storage",* IEEE International Conference on Computer and Information Technology,2016.

[4.] Linmei Jiang, and _DonghuiGuo, *"Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-encryption for Cloud Storage",* Journal of latex class files, Vol. 14, No. 8, August 2015.

[5.] Kaitai Liang and Willy Susilo, *"Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage",* IEEE Transactions on Information Forensics and Security, 2015.

[6.] Baojiang Cui, Zheli Liu and Lingyu Wang, *"Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing Via Cloud Storage",* IEEE Transactions on computers, *Vol. 6, No. 1, January 2014.*

[7.] Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, *"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage",* IEEE Transactions on Parallel and Distributed Systems, 2013.

[8.] J. Shao; G. Wei; Y. Ling; M. Xie *"Identity-Based Conditional Proxy Re-Encryption"* Proceedings of IEEE International Conference on Communications, 2011.

[9.] G. Ateniese, K. Fu, M. Green, S. Hohenberger *"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage"*. ACM Transactions on Information and System Security (TISSEC), Volume 9, Issue 1, 2006.

[10.] Jissy Ann George, Dr.M.Hemalatha , "*Cryptographic Techniques, Threats and Privacy Challenges in Cloud Computing",* International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015.