Cloud Computing Security: Challenges, Approaches and Solutions

AMGHAR Sara, TABAA Yassine, MEDOURI Abdellatif
New Technology Trends, Abdelmalek Essaadi University, Faculty of Sciences of Tetouan, Morocco

Abstract— Despite all the research that has been done in this area, the security in the cloud computing still one of the biggest problems that prevents customers to use the cloud service. In this work, we survey various research works on cloud computing related to security challenges and privacy issues. The main aim of this paper is to provide a better understanding of the security challenges of cloud computing and identify approaches and solutions which have been proposed by several researchers.

Index Terms— Cloud computing; Confidentiality challenges; Security challenges; Privacy; Data encryption.

1 Introduction

Cloud computing is a technology that has the potential to enhance collaboration, agility and availability, and provides the opportunities for cost reduction through optimized and efficient computing. So the cloud computing attracts the attention of many research community because it can provide tremendous benefits to the industry and the community.

As with any new technology, there are a lot of challenges and obstacles. Data confidentiality and security are among the main obstacles in adopting the cloud service both in the academic [1] area and at the enterprise level, because outsourcing data to a remote server and delegate data management to non-reliable cloud service provider may lead to loss of physical control over the data [2].

The Cloud computing is essentially a data storage solution. So the data is stored somewhere on servers in the cloud like the photos on Facebook, Skype conversations, and projects in Asana. But what happens if one of these services goes done and the data are erased [3].

In this paper we will review fundamental issues of the security and confidentiality of cloud computing systems, we describe the security problems surrounding cloud computing, and we present some existing approaches and solutions which have been proposed to solving these problems. Finally, we explore the possible prospects in order to provide a secure and a confidential cloud computing environment in the future.

2 Security and confidentiality challenges of Cloud Computing

Cloud computing is a computing model that provides services or applications online, accessible anywhere and anytime. It allows on-demand access via the network to a shared set of computing resources. In spite of all the advantages provided by the cloud the challenges are still numerous [4]. For example certain local agencies allow the security services to access the data held by individuals without informing users. These agencies can also listen and record telephone conversations that are hosted within their territory. The data hosted in the cloud are sensitive to this kind of situation. Therefore, it is necessary to take appropriate measures to make sure that the data shared in cloud remains private regardless of whether it is hosted in any territory or not.

2.1 Security challenges:

Despite all the advantages provided by the cloud services providers including some key security benefits, there are more security challenges that prevent customers from engaging in cloud computing strategy [5, 6]. The cloud environment raises various concerns of security:

1) Outsourcing data: Although the cloud offering tangible benefits to data owners, outsourcing data to a remote server and delegate data management to non-reliable cloud service provider, may lead to physical loss of control over the data.

Cloud computing provides access to data, but the problem is to ensure that only authorized persons can enter to this data. Appropriate mechanisms needed to prevent cloud providers from using customer's data in a way that has not been agreed upon in the past.

- ***Example:***

Back in 2008-2009, the Amazon Simple Storage Service (S3) experienced a spat of silent data corruption. Customers lost data permanently. Amazon reacted by enabling the user to run a MD5 checksum against data being sent to S3. Even now the Amazon admits warn against relying solely on the cloud for data storage and advise data backup procedures.

2) Virtualization: Virtualization is a technique which allows the use of same physical resources by multiple customers. We discuss the security issues related to virtualization below :

VM isolation: VMs (Virtual Machines) running on the same physical hardware need to be isolated from each other. A separate VM is instantiated for each user to ensure strong isolation between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host [7].

VM image sharing: A VM (Virtual Machine) image is used to instantiate VMs. The users can create their own VM image or can use an image from the shared image repository. Sharing of VM images in the image repositories is a common practice and can evolve as a serious threat if it is used in malicious manner. A malicious user can investigate the code of the image to look for probable attack point. On the other hand, a malicious user can upload an image that contains a malware. The VM instantiated through the infected VM image will become source of introducing malware in the cloud computing system. Moreover, an infected VM can be used to monitor the activities and data of other users resulting in privacy breach [8].

3) Multi-tenancy: Multi-tenancy or shared access is another feature unique to the clouds, where many consumers hosted their data in a shared public cloud infrastructure. Especially in public clouds, providers must account for issues such as access policies, application deployment, and data access to provide a secure, multi-tenant environment. Multi-tenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data shared in the cloud [9].

4) User authentication: The data hosted in the cloud needs to be accessible only by authorized users, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. So, the protection of user credentials and account details of the cloud service provider and others malicious users must be assured.
In order to ensure the confidentiality and the security of user authentication, the organizations need to be able to view data access logs and audit trails to ensure that only authorized users can access the data.

- **Example:**

Back in 2008, the society Dropbox experienced a great problem when the hackers stole account password of an employee Dropbox and retrieving information about a confidential project.

5) Contingency Planning: The emergency planning are very important because the data owners need to have a way which allows them to handle their data shared in the cloud in the case of an emergency. So, the data owners should know if their data can be easily retrieved and migrated to a new service provider or to a non-cloud strategy when the cloud providers failed or bankrupt, and what happens to the data and the ability to access this data if the cloud providers gets acquired by another company.

2.2 Confidentiality challenges

Confidentiality is a core issue in all the challenges we've discussed so far, including the need to protect identity information, policy components during integration, and transaction histories. Many organizations aren't comfortable storing their data and applications on systems that reside outside of their on-premise datacenters because the data in the cloud can be accessed by cloud providers which could be the greatest fear of cloud customers [10].
There are also two important characteristics that impose challenges to the development of data protection:

• A cloud service can be provided through a chain of service providers. This means that the primary provider uses the resources of other providers. This makes the outsourced files more venerable to attacks.
• Some possible changes to the indirect providers involved in a cloud service need to be considered also. For example: a participating provider may need to transfer its operations together with users' data to someone else because of the sale of company, a merger, seizure by the government, etc. This means that the user's files may remain on several inactive hard drives even after user's request for deletion or close of account.

1) Integrity: Integrity is a data security key aspect which means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, updating or creation. By preventing unauthorized access to the data, data owners can attain greater confidence in data and system integrity [11].

- **Example**:

In 2007, the European Centre for Nuclear Research has published a paper describing the problem of silent data corruption. Then in 2008, they found that about 38 000 files were corrupted in 15,000 terabytes of data they have generated. With the encrypted storage, even small data corruption can result in files that will simply not open or backups that cannot restore your data!

2) Availability: Data availability concern is a critical issue which prevents organizations from moving to the cloud. It is the key decision factor when deciding among public, private or hybrid cloud providers as well as in the delivery models [12].
Availability refers to the property of a system to be accessible and usable at anytime by an authorized user. System availability includes a system ability to carry on operations even when some authorities misbehave.
Authors in [12, 13] give examples of attacks which could have a negative effect on data availability such Distributed Denial of Service attack in which a legitimate customers are deprived of the services and resources they would normally expect to have access to by absorbing all available bandwidth.

3 Security in the Cloud: present and future

All surveys show that security is one of the biggest obstacles that hamper the widespread adoption of cloud computing [14]. There are many questions such as:

- What confidence can we have in the storage of the data outside the company?
- What are the risks associated with the use of shared services?

Researchers are interesting to find technological solutions which ensure the confidentiality and the security of the data shared in the cloud. In this section, we discuss various approaches proposed to counter the security issues discussed in the previous section.

3.1 Data encryption

The data owners must ensure that their sensitive data are protected both at transit and in rest, so some researchers in [15] have proposed to encrypt the data before sending it to the cloud. Data encryption is an essential and a most secure methodology which the main aim is to protect data confidentiality. Recently, several encryption schemes have been described in the literature, these encryption schemes were classified into two types as described in [16]: symmetric key encryption and public key encryption.

The symmetric key encryption scheme allows a data owner to outsource its data symmetrically encrypted to an entrusted server, and it used a single key to encrypt and decrypt the data. This is named a secret key. There are several symmetric algorithms like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [17].

Authors in [18] developed a Bloom filter based per-file index scheme to reduce a workload for each search request proportional to the number of files in the collection.

The public key encryption is used in a similar scenario with two keys: one key is for encryption and another for decryption. In [19] authors proposed a secure and privacy preserving keyword searching scheme using ElGamal public-key encryption. It allows the cloud providers to participate in the decipherment, and return the encrypted files containing certain keywords without knowing any information.

3.2 Data classification

Data security is a great concern for any organization when moving towards the cloud. To achieve a higher level of data security, classifying data based on security level criteria becoming point of interest by several organizations that use or provide cloud services. Several researches have already been done in this area witch classifies the data in social network or other applications. A three dimensional view for data taxonomy is proposed in [20]. It classifies data as per visibility, Granularity and purpose. Several levels are defined along these dimensions to ensure the data privacy. The authors in [21] presented the taxonomy of social data, it classifies the data based on the way it is generated in the social network, and as a result the privacy and access rights should be applied. Data classification in various stages of social network generated data is presented by authors in [22]. It classifies data throw security and confidentiality parameter confidentiality. The data disclosure in a network, it applies this classification in various phases of data like processing, collection, invasion and dissemination.

Authors in [23] have proposed a new classification technique that ensures the security of the data hosted in the cloud which is data classification which is based on the various aspects. It classifies the data on three types of characteristics that are access control, content, and storage. Some authors classify the data according to the risk associated with the disclosure. They are confidential, internal, public, or top secret. Some classify the data based on the way it is created, user personal data, their usage patterns etc.

Figure 1 indicates the three types of characteristics on which data has to be classified in [23].

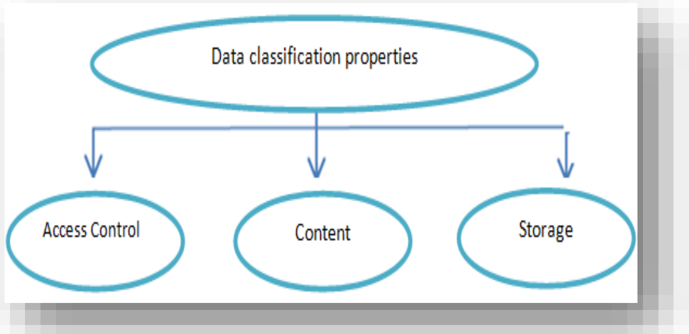

Figure 1: Data Classification in Cloud computing.

3.3 Virtualization

Virtual Machine VM images are entities that require high security and integrity because it indicates the initial state of the VM.

Wie et al. [24] proposed Mirage, an image management system for the cloud environment. The Mirage provides a fourfold security to the VM images. The publishing and retrieval of the VM images is regulated by an access control framework. The filters are applied to the images both at publishing at retrieval time to detect and remove the unwanted information. A tracking mechanism is utilized to keep track of an image both in terms of auditability of actions and derivation. Moreover, maintenance of repository is also provided by the Mirage. The access control is provided at check-in and checkout times. The filters remove any leftover private information, malware, and pirated software from the image.

In [25], the authors proposed encrypted virtual disk images in cloud (EVDIC) that exploits encryption to secure the VM images on the disk. The image encryption module encrypts an image whenever a VM is terminated. The EVDIC uses advanced encryption standard (AES) with a key size of 256 bits. The key is generated by key management server (a third party that is not a part of the cloud) through the password of the user. The encrypted image is then stored on the disk. During retrieval, the image decrypt module interacts with the key management server to retrieve the decryption key and decrypts the image for loading into a VM. The EVDIC also stores integrity information for the VM images. Therefore, it provides confidentiality and integrity services to the VM images. Moreover, any sensitive data loaded into the image is also protected by the proposed scheme.

3.4 Data storage security

The data storage is one of the most used cloud service, when the users can outsource any amount of data to cloud servers to benefit virtually from unlimited hardware or software resources.

To ensure the quality of the cloud storage, integrity and availability of data shared in the cloud, authors in [26] proposed efficient methodology that supports on-demand data correctness verification. The proposed methodology conducts the verification_of the cloud data correctness without explicit knowledge of the whole data. The erasure correcting code and homomorphic tokens are used for the aforesaid purpose. The homomorphic token are pre-computed by the user and data is fragmented and stored redundantly across the cloud servers. To verify data correctness, a challenge containing random data blocks indices is transmitted to the cloud. The cloud computes the response and sends back to the user where decision is made based on the comparison of received result with the pre-computed tokens. Additionally, the proposed scheme performs error localization by detecting the misbehaving server. The proposed scheme secures the cloud storage against integrity attacks and server colluding attacks.

3.5 Multi-factor authentification

Authentication is the first step that ensures the privacy and security of the data sharing in cloud. In order to ensure a higher security than the static passwords, researchers in [27, 28] proposed using one-time password technology (also called dynamic passwords) which is an automatically generated numeric or alphanumeric that authenticates the user for a single transaction or session. The user doesn't have to remember one-time passwords because it's often generated by the token and presented to the user if he needs to authenticate.

The author in [29] proposed to combine one-time passwords generated by a token with static passwords to achieve two factor authentications. Token is something the user has; static password is something the user knows. If the attacker learns the static password of the user, he cannot impersonate him, because he doesn't control the user's token. Two-factor authentication may not be infallible, but it is an important step in securing the data stored in the cloud from threats such as cyber attacks.

The authors in [30] proposed a new approach named Multi-factor bio-metric Fingerprint Authentication (MFA) that provides a convenient and a high-secure identity verification process to validate the legitimacy of the remote users using random strings. The multi-factors as the password and the user ID, biometric fingerprint and random strings are used as key parameters in the process of authentication. In this approach, user credentials are not stocked in the cloud servers however allow the servers to perform authentication on hashed credentials. Moreover, it prevents the cloud service providers to learn and access the user credentials.

3.6 Identity Management and access control

When we talk about access control we mean the way how users can access to the data outsourced in the cloud. To provide fine grained access control in cloud, attribute based encryption (ABE) has been suggested in [31]. This technology contains two types CP-ABE (cipher-text policy) and KP-ABE (Key Policy). In CP-ABE, access policy is given in cipher text with each file and each user is issued a secret key associated with its attributes. Furthermore, in PK-ABE, access policy is defined in private key that is assigned to users and can decrypt only those files whose attributes match with this policy [32]. Several researchers have proposed scheme which is based on the ABE technology. For example, the authors in [33] proposed an efficient approach for authentication and controlling access to the cloud. This proposed scheme makes use of Attribute Based Encryption (ABE) and the Attribute Based Signature (ABS) for access control and anonymous authentication, respectively. The anonymous authentication enables the user authentication without revealing the identity of the user. The signature is verified based on the attributes that eliminates the requirement of identity for authentication. The Key Distribution Center (KDC) issues the encryption, decryption, and signing keys. The user encrypts the data and the signature and transmits it to the cloud. The cloud verifies the signature that is attributing based and stores the data in case of valid user.

In order to achieve a higher access control security the Attribute-based broadcast encryption (ABBE) was first proposed by the authors in [34], in which broadcasters can encrypt data with access policy and a list of the users who can access to this data, only the receiver is in this list and satisfies the access policy that can decrypt ciphertext. The authors in [35] proposed a new efficient methodology named EP-ABBE Based on CP-ABE and BE. The EP-ABBE reduces the decryption computation of user, and protects user privacy by obfuscating the access policy of ciphertext and user's attributes.

The authors in [36] proposed Role Based Multi-tenancy Access Control (RB-MTAC) scheme that combines identity management and role based access control. The scheme requires the users to register with the cloud to obtain unique ID. The user sets the password during registration process. To enter the cloud, a user has to pass through identity management module that identifies the user on the basis of registered identity credentials. The users can access to all resources through the RB-MTAC module that maintains the access control lists for resources.

3.7 SeDaSC methodology

In [37], the authors proposed a new methodology named secure data sharing in cloud (SeDaSC) which can be used to secure the data sharing among the group by using the symmetric encryption. This methodology provides confidentiality and integrity of the data shared in the cloud, access control for malicious insiders, and forward and backward access control. The SeDaSC methodology is based upon 3 entities which are the users, a cryptographic server (CS), and the cloud. The user sends to the CS the data, the list of the users, and parameters required to generate an access control list. The cryptographic server (CS) is responsible for key management, encryption and decryption of data, and the management of access control list. The CS generates the symmetric key and encrypts the data with the generated key. Thereafter, for each user, the CS divides the key into two parts so that a single part alone cannot regenerate the key. One part of the key is transmitted to the corresponding user in the group, and the other part is maintained by the CS within the ACL related to the data file. The encrypted data is then sent to the cloud for storage.

4 Discussion and comparison

While several research works concerning security and confidentiality on cloud computing continue to be conducted. There still various issues that need to be addressed in order to provide a secure cloud environment. Indeed, data shared throw the cloud are the target of several network attacks, which aim to interrupt and modify information. To deal with these problems, various approaches are proposed by diver's researchers in order to solve them. Some of these solutions are presented in previous section of this paper. Indeed, data encryption is seen as a normal solution to ensure the confidentiality of shared data in the cloud. However, until recently, the encryption is not a silver bullet to ensure data confidentiality. In fact, the peculiarity of the cloud model means that is hard to readily apply traditional cryptographic methods for privacy protection.

There are many kinds of access control model specified for Information system but they still not satisfying cloud computing needs. Each model proposed in this area presents its weakness. As an example, comparing The ABBE and the EP-ABBE, the user storage overhead and decryption computation of user is much lower in EP-ABBE than in ABBE. Moreover, EP-ABBE can protect user privacy by obfuscating access policy of ciphertext and the attributes of user.

Despite all the solutions that are already proposed by various security researchers, the data shared in the cloud are not yet secured. So, the need to find new methods and solutions is urgent.

5 PERSPECTIVESS

Cloud computing security concerns all the aspects of making cloud computing secure. Despite of intensive research efforts by different researchers, several issues remain unsolved and should be fixed in order to provide a most secure cloud environment.

First, cloud community need to find a global comprehensive security solution that includes the most of security requirements in the cloud which allows to achieving confidentiality and security from the cloud providers. Multi-tenancy is one of the essential characteristics of cloud computing that raises various security concerns, which make it one of the big challenge for the cloud computing. Unfortunately the research topics in this area to find the solutions for multi tenancy security issues are very rare. The customers due to many reasons may want to migrate their data or applications to another cloud. However, migration to a different cloud is difficult. Indeed, there is a need of standardized formats and protocols that can help the customers to migrate their data to a different cloud easily.

Identification of indicators for insider attacks in the cloud is a wide area of research that can enhance security throw cloud providers. The differentiation between a normal and malicious user within the cloud is another area of research which can resolve a lot of security problems.

In our future work, we tend to provide an efficient and a new encryption scheme designed for cloud environment that allows cloud customers and providers to have a fine grained and flexible access control system to improve security when sharing data over cloud computing.

6. Conclusion

The cloud computing has provided research opportunities in all aspects surrounding this technological revolution especially in topics such as security and privacy in cloud computing.

Security in the cloud computing is one of the major preoccupations of organizations in the adoption of cloud technologies process. Despite all the efforts and research works that have been conducted in this area, there still remain various challenges that prevent customers from engaging in the cloud computing strategy.

In this paper we described the security problems that surround Cloud computing environment and we cited some approaches to achieving security and confidentiality from the cloud provider.

This space is fast moving, and we can expect to see plenty of solutions in the coming years.

References

[1] Y. Tabaa, and A. Medouri, "Towards a next generation of scientific computing in the Cloud," IJCSI International Journal of Computer Science Issues, vol. 9, no. 3, 2012.

[2] Mehdi Sookhak , Abdullah Gani , Muhammad Khurram Khan ,Rajkumar Buyya , "Dynamic remote data auditing for securing big data storage in cloud computing," Information Sciences (2015), doi: 10.1016/j.ins.2015.09.004.

[3] http://www.cloudcomputingnews.net/news/2015/jan/26/what-happens-when-data-gets-lost-cloud/.

[4] Cloud security alliance, "security guidance for critical areas of focus in cloud computing v3.0".

[5] L. FB Soares, D. AB Fernandes, J.V. Gomes, M.M. Freire, P. RM Inácio, "Cloud security: state of the art, in: Security, Privacy and Trust in Cloud Systems, " Springer, Berlin, Heidelberg, 2014, pp. 3–44.

[6] Takabi, H., Joshi, J., Ahn, G.J, "Secure cloud: Towards a comprehensive security framework for cloud computing environments", Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual. 2010, p. 393–398. doi:10.1109/COMPSACW.2010.74.

[7] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.

[8] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, "An analysis of security issues for cloud computing, ", J. Internet Services Appl. 4 (1) (2013) 1–13.

[9] Ahmed Albugmi; Madini O Alassafi; Robert Walters; Gary Wills, "Data Security in Cloud Computing," Fifth Int. Conference FGCT IEEE, vol. 2, no. 1, pp. 1–169, 2016.

[10] Elsevier B.V. "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions".

[11] Gartner. Assessing the security risks of cloud computing, Gartner, 2008.

[12] Zibouh, Ouadia,et.al., "Cloud Computing Security Through Parallelizing Fully Homomorphic Encryption Applied To Multi-Cloud Aproach", Journal of Theoretical and Applied Information Technology 87.2,May 2016,Volume-87, pp. 300-307.

[13] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", Procedia Computer Science, vol. 37, 2014, pp. 357–362.

[14] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, "Security issues in cloud environments: a survey", Int. J. Inform. Sec. 13 (2) (2014).

[15] Bethencourt, J., Sahai, A., Waters, B., 2007. “Ciphertext-policy attribute-based encryption“.

[16] Syam Kumar Pasupuleti, Rajkumar Buyya, Subramanian Ramalingam, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing, 2015.

[17] Vishal R. Pancholi and Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," International Journal for Innovative Research in Science and Technology, vol. 2, no. 9, pp. 18-21, 2016.

[18] Goh E-J. Secure indexes, Technical Report 2003/216, Cryptology, ePrint Archive; 2003 (http://eprint.iacr.org).

[19] Liu Q, Wang G, Wu J. Secure and efficient privacy preserving keyword searching for cloud services. J Netw Comput Appl, 35. Elsevier.

[20] Ken Barker, Mina Askari, Mishtu Banerjee, Kambiz Ghazinour, Brenan Mackas, Maryam Majedi, Sampson Pun, and Adepele Williams, “A Data Privacy Taxonomy”, Advanced Database Systems and Applications Laboratory, Canada, 2009.

[21] Bruce Schneier, “A Taxonomy of Social Networking Data, The IEEE Computer And Reliability Societies”, August 2010.

[22] Sergio Donizetti Zorzo, Rodrigo Pereira Botelho, Paulo Muniz de Ávila, “Taxonomy for Privacy Policies of Social Networks Sites”, Published Online, Social Networking, 2013, 2, 157-164 October 2013.

[23] Elsevier B.V, “Data Classification for achieving Security in cloud computing“, 2015.

[24] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, “Managing security of virtual machine images in a cloud environment“, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 2009, pp. 91–96.

[25] M. Kazim, R. Masood, M.A. Shibli, “Securing the virtual machine images in cloud computing“, in: Proceedings of the ACM 6th International Conference on Security of Info and Networks, 2013.

[26] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, “Toward secure and dependable storage services in cloud computing“, IEEE Trans.

[27] Vimmi Pandey, Vishal Paranjape, “An Improved Authentication Technique with OTP in Cloud Computing“, 2013.

[28] Ali A. Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou, “Cloud Authentication Based on Anonymous One-Time Password“, 2013.

[29] http://resources.infosecinstitute.com/one-time-passwords-with-token//.

[30] http://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-015-0046-4.

[31] Chunhua Li(✉), Ronglei Wei, Zebang Wu, Ke Zhou, Cheng Lei, and Hao Jin, “Adopting Multi-mode Access Control for Secure Data Sharing in Cloud“, Springer International Publishing Switzerland 2015.

[32] Lee, C.-C., Chung, P.-S., Hwang, “A survey on attribute-based encryption schemes of access control in cloud environments“, IJ Netw. Secur. 15(4), 231–240 (2013)

[33] S. Ruj, M. Stojmenovic, A. Nayak, “Decentralized access control with anonymous authentication of data stored in clouds“, IEEE Trans. Parallel Distrib.

[34] Lubicz D, Sirvent T, “Attribute-based broadcast encryption scheme made efficient. Advances in Cryptology“.

[35] FU Jing-yi, HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, “Secure personal data sharing in cloud computing using attribute-based broadcast encryption“, 2014.

[36] S. Yang, P. Lai, J. Lin, “Design role-based multi-tenancy access control scheme for cloud services“, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013,

[37] Mazhar Ali, Student Member, IEEE, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Senior Member, IEEE, Athanasios V. Vasilakos, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE, “SeDaSC: Secure data sharing in clouds”.