Improved Cloud Data Security Using Source Key Policy Based Encryption

P Jayasree[1], Dr. V. Saravanan[2]
[1]Ph.D Research Scholar, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India
[2]Associate Professor, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India

Abstract-*Recently, the storage and retrieval of data in the cloud environment is an attractive research area. Because the cloud environment provides easy and reliable data access over internet. The service is provided over the various internet services by the companies such as Google, Microsoft, Yahoo, IBM, and Amazon. The Cloud Service Provider (CSP), data owner are the major components in cloud computing and the pool containing the resources. Remote data storage services are widely used by everyone. The security assurance for those stored data is very tedious when the data is accessed by multiple users. Attribute based encryption is an optimal way to control the data access over the cloud. To achieve high data security a novel policy based encryption scheme has been proposed. The proposed system developed a Source Key Policy Based Encryption (SKPBE) to provide high security data access in the cloud. The SKPBE improved with various parameters and deployed with the ELGammal encryption scheme. The result shows the proposed system achieved better security performance and decreases the encryption and decryption delay.*

Keywords-cloud computing, Data security, attribute based encryption, Cloud Service Provider, Key policy .

I. INTRODUCTION

Cloud computing is the pool of shared resources, which provides different types of services and allows the users to virtually access the computing resources [1]. It's an emerged new paradigm for remote data accessing and service utilization over the internet. Cloud computing technology offers different types of services which are categorized into different types such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS) [2]. The cloud also provides storage services widely with free of cost or pay-as-you go basis. The cloud computing has broad network access, high scalability, location independence, and provides the services on demand basis. Due to this advanced characteristics, the Cloud computing is more popular and widespread. Due to this reliable nature and wide popularity, the cloud has several security threats. Data protection and security is a critical task in the cloud computing environment. This needs a guarantee for the high level data security. In the traditional methods, the firewalls were used across the data centers to protect the sensitive information. The service providers are responsible for maintaining the data security and enterprises will rely on them. There are several challenges in the cloud relating to the security issues such as data availability, authentication, and data access control, legal issues, confidentiality and privacy maintenance, and service level agreement issues. In this paper, an attribute based encryption scheme is developed with key recovery and effective security mechanisms. The proposed SKPBE allows fast and secure data access verification and decryption in the multi user access clouds. This paper initially provides the outline about the threats and vulnerabilities in cloud computing and analyses the existing ABE schemes. Finally the paper gives the proposed system description with results.

Threats and Vulnerabilities

There are several vulnerabilities in the cloud such as Virtual Machine Attack, Malware Injection Attack, Session Riding and Hijacking, Vendor Lock-in, Resource Exhaustion, Denial of Service, XML Signature Element Wrapping and Sybil Attack [3].

Virtual Machine Attack: Virtualization is the important aspect of the cloud computing, where the software, operating system and all the components are combined together such that it is independent of the hardware. The client specific application has a virtual machine in the virtualized environment of the cloud. There are several virtual machines running in parallel for operating the system of the cloud provider. It is a tough task to manage the entire VMs, hence to recognize the type of vulnerability is a tedious task. In this type of attack, the attacker runs the code on the virtual machine and communicates directly with the hypervisor. The attacker accesses the host OS and all other VM'srunning on that particular host.

Denial of Service: The Denial of Service attack is that the website causes the unavailability of the content of the website to the users. Distributed Denial of Service attacks is the volume based attacks originating from a large number of computers. The workstations are usually the large workstations and are referred as the zombies. The zombies form a widely distributed attack network called a botnet.

Session riding and Hijacking attack: Session riding is the type of attack, which refers to the hackers sending the commands to a web on behalf of the targeted users. Session hijacking is the process of gaining an unauthorized access that is residing on a computer by using a valid session key. The session hijacking gives the chance to hackers to accomplish a wide variety of malicious activities.

Malware Injection Attacks: In the cloud computing environment, the request from the client is executed based on the authentication and the authorization. There is a great possibility of exchanging messages between the web browser and the web server. During the swap of the data, the attacker benefits in attacking the data. If the attacker is successful in these types of attacks, then the cloud service suffers from the deadlocks, which forces a valid user to wait for the job to be completed. These types of attacks are also called as the meta-data spoofing attack.

XML Signature Element Wrapping: The XML is the fundamental markup language used for providing the client-server communication. These types of attacks are the well-known attacks on the web applications. In this type of server, the SOAP message is generated.

Vendor Lock-in: The vendor lock-in is the type of vulnerability, which is found in the cloud. These types of vulnerability arise in the undeveloped vendors. Lock-in will make a client depend on a cloud service provider. Since, several cloud providers have many principles and policies the clients are not able to easily transfer from one provider to another.

Resource Exhaustion: Resource exhaustion vulnerability is the process of resource consumption in an unnecessary way. This cause the bad design of resources on the service side, and it cause the leakage of the resources. In the resource leakage, the resources are not released from the memory after use. Hence, the identification of the cause is difficult to observe and identify unless closely monitored.

Sybil attacks: In this type of attack, the malicious user acquires the multiple identities and pretends to be the distinct users and creates the relationship with the honest users. The cloud storage is usually used in the public networking such as the Facebook, Orkut, Bebo, etc. The users store their files, such as the credentials, photos, videos, etc. on the public networking. The relationship between the malicious user and the truthful user is called as the attack that is used for social networking.

II. LITERATURE SURVEY

2.1 Vulnerabilities in Cloud Computing

In paper [4] authors Grobauer, et al. (2011) studied various vulnerabilities in cloud computing. There were two problems regarding the security issues in cloud computing. The risks were often used as the basic vocabulary for the threats and the vulnerability. The vocabulary for the risks, threats and the vulnerability was interchangeable. The issues raised specifically to the cloud computing and analyzed the vulnerabilities and the threats. The cloud computing made the well-understood vulnerabilities and introduce a security-specific cloud reference architecture.

In paper [5] authors Khorshed, et al. (2012) surveyed the gaps and challenges for the proactive attack detection in cloud computing environment. The long-term potential benefits of the cloud computing environment were the reduction of costs and the improvement of the business outcomes. To make the cloud computing more remarkable, the user needs to address the variety of security risks. In this survey, the extensive review on the cloud computing was focused. The top security threats were also studied, which were found in the cloud computing environment and their solutions were also defined.

2.2 Cryptographic Solutions in Cloud

Nowadays, the sequential changes in system architecture and the large computerized data availability in the data sharing networks motivated the data confidentiality and privacy concerns [6]. The utilization of internet by the Government agencies permits the data dissemination, user transactions for business dealings between the organizational and affiliation units. The e-commerce and e-government are the internet oriented technologies attributed by the impact of data sharing. The reason behind the use of data sharing in e-commerce is that the provision of better transactions between the users.

In paper [7] authors Sarathy and Muralidhar (2006) discussed the substantial problems in data sharing necessary to complete the whole transaction and analyzed with the development of new scenario referred as Operations Research/ Management Science (OR/ MS). The study of opportunities of OR/MS raised the potential risks to preserve the privacy and confidentiality in data sharing process. Hence, the secure data sharing is the promising solution to potential risks. There are two major categories in secure data sharing namely, sharing the data without considering the security or prevent the data transfer in an

insecurity platform. OR / MS approach declared the trade-off between the categories. The investigation of the significant impact of internet on data sharing in two ways namely, internet enabling and disclosure risk increase referred the "dual personality" that lead to an attractive research area. The declaration of OR / MS assured the usefulness and security of data sharing. The developed framework has the capability to perform following processes.

In paper [8] authors Wang, et al.(2013) proposed a secure cloud storage system that supports public auditing for preserving the privacy of the users data. An external auditor was enabled to audit the outsourced data of the user without learning the data content. The TPA was enabled to perform simultaneous auditing of the multiple users in an efficient manner. The Homomorphic Linear Authenticator (HLA) and random masking were used to guarantee that the TPA does not learn any knowledge about the data stored on the cloud server during the auditing process. Thus, the burden of the cloud user from the tedious and expensive auditing task was reduced and leakage of the outsourced data was prevented. The security and performance analysis have shown that the proposed schemes were highly secure and efficient. The computation time and cost required for the auditing task were reduced efficiently by using the batch auditing scheme.

In paper [9] authors Yang, et al(2013) proposed a secure and efficient Data Access Control Scheme for Multi authority Cloud Storage (DAC-MACS). A novel multi-authority CP-ABE scheme with efficient decryption was constructed, and an efficient attribute revocation method was designed to achieve both forward security and backward security.

In paper [10] authors Graf, et al. (2012) proposed a graph-based key management approach to enable scaling and flexibility in key management within a heterogeneous cloud environment. Access rights were represented as graphs to distinguish between the keys used for encrypting hierarchical data. Commonly shared data was utilized by disjunct clients using hierarchically organized access rights in the form of Directed Acyclic Graph (DAG). Encryption Key (EK) and Classic Key were combined to ensure scalability within the updates. Each client had a subgraph, which consists of its CK and the descendants. A global key graph was used to manage join/leave the operations of nodes as well as insert/remove operations edges. Versa key was used to encrypt the new key material of the updated descendants by using the keys stored in the adjacent nodes, which stays valid for modification. The shadow key has been implemented as an extension to key graph for accessing only the most recent version of the data.

In paper [11] authors Li, et al. (2014) proposed Dekey construction, to provide reliable convergent key management through convergent key duplication and sharing with the support of both file-level and block-level deduplication. Dekey was implemented using Ramp secret sharing to distribute the convergent key securely across multiple servers without the need for key management by the users on their own. The system model consists of three entities: user, Storage-Cloud Service Provider (S-CSP) and Key Management Cloud Service Provider (K-CSP). S-CSP was used to provide data outsourcing, and data redundancy was eliminated via deduplication, thereby reducing the storage cost. KM-CSP was used to maintain convergent keys for users and to provide them with minimal storage cost and computation service. File-level deduplication eliminated the storage of any redundant files, whereas block-level deduplication divided a file into smaller fixed size and eliminated the storage of any redundant blocks. Single point of failure and storage overhead in key management were the two issues of baseline approach. The storage overhead has been reduced in Dekey approach by sharing the same block if multiple users access the same convergent key.

III. ATTRIBUTE BASED ENCRYPTION SCHEMES

3.1 Attribute Based Encryption (ABE)

In Attribute Based Encryption (ABE), the user can decide the person to decrypt a cipher text based on the attributes and policies of the message. A central authority creates the secret keys for each user by using the attributes and policies. Moreover, this scheme contains various encryption standards such as, Key Policy Attributed Based Encryption (KP-ABE), Cipher text Policy Attribute Based Encryption (CP-ABE) with non-monotonic access structure; Hierarchical Attribute Based Encryption (HABE) and Multi Authorities Attribute Based Encryption (MAABE) are also analyzed. Generally, the Attribute Based Encryption (ABE) makes the user and data attributes as the major components for generating the keys while the data is encrypted. The attributes are mainly used to describe the encrypted data and build the policies into user's keys. The ABE scheme has the following advantages:

- It reduces the communication overhead of the internet
- It provides a fine-grained access control

3.2 Key Policy Attribute Based Encryption (KP-ABE)

It is the modified form of classification ABE model, where the users are assigned with an access tree structure over the data attributes. In this model, the threshold gates used are defined as the nodes of the access tree and the attributes are associated with the leaf nodes. The secret key of the user is defined to reflect the access tree structure, and the cipher-text is labeled with the sets of attributes. Moreover, the private keys are associated with the monotonic access structures that are able to decrypt the user's cipher text.

3.3 Cipher-Text Policy Attribute Based Encryption (CP-ABE)

The CP-ABE is another modified form of ABE, where every cipher-text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher-text only if the set of attributes are associated with the user's private key. It works in the reverse way of KP-ABE and the access structure of this scheme inherits the same method that is used in KP-ABE to build. If the user's key with attribute satisfies the access structure of the encrypted data, it recovers the data. This concept is similar to the traditional access control schemes. The encryption specifies the threshold access structure for his interested attributes while encrypting a message. It supports the access control in the real environment, where a set of attributes are combined to satisfy the access structure in the encrypted data. The major disadvantages of the existing CP-ABE are,

- It does not fulfill the requirements of access control
- It requires considerable flexibility and efficiency
- It needs to specify the policies and to manage the user attributes

In this scheme, the decryption keys support only the user attributes that are logically as a single set, so the users can use all the possible combinations of attributes in a single set. This scheme organizes the user attributes into a recursive set based on the structure and improves dynamic constraints on how these attributes are combined to satisfy a policy.

Table 1.0 Attribute based encryption comparative analysis

Techniques/ Parameter	Fine grained access control	Efficiency	Computational overhead	Collision resistant
ABE	Low	Average	High	Average
KP-ABE	Low, High if there is re-encryption technique	Average, high for broadcast type system	High computational overheads	Good
CP-ABE	Average realization of complex access control	Average, not efficient for modern enterprise environments	Average computational overheads	Good
HABE	Good access control	Flexible	Some of overhead	Good
MA-ABE	Better access control	Scalable	Average	High collusion resistant

3.4 Attribute Based Encryption Scheme with Non-Monotonic Access Structures

The problem with attribute based encryption scheme with non- monotonic structure is that there are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but there are useless for decrypting the encrypted data. The major drawbacks of this scheme are,

- It is inefficient and complex
- Here, each cipher-text needs to be encrypted with n number of attributes.

3.5 Hierarchical Attribute Based Encryption (HABE)

This model contains a Root Master (RM) corresponds to the Third Trusted Party (TTP) and multiple Domain Masters (DMs) in which the top level DM is correspond to multiple enterprise users and numerous users. It used the property of hierarchical generation of keys in HIBE scheme for generating the keys.

The overall comparison between all these ABE schemes are shown in Table 1.0, which includes, the comparison based on collision resistant, efficiency, computation overhead, and access control. From the above comparison made in table 1.0, the proposed system has been developed.

IV. PROPOSED SYSTEM

Cloud environment provides various types of services for all type of applications. Providing data security in such application is more important. In the traditional cloud data security schemes allows data security in different terms, such as firewall and intrusion detection based, the existing system used key generation process, firewall rule settings and the network centric approaches for data security. However, the existing data protection solutions lack the data integrity, robust key generation process, computational overhead, collision in the encryption key, and data crashing by the data owner in the cloud server. To address all these issues, a new attribute based encryption named as "Source Key Policy Based Encryption (SKPBE)" is proposed along with the ElGamal encryption standard. The proposed methodology focuses on the security of the key for the data that is been outsourced in the cloud servers.

- Further, it provides secured access control mechanism, and data access policies for improving the data security in cloud.
- The usage of the SKPBE enhances the data security in cloud computing environment.
- To prove the effectiveness of the proposed SKPBE, it is compared with the existing subset cover for the security performance metric.
- The encryption time of the proposed SKPBE is compared with the existing role based access control.
- The variation of the encryption time with respect to the file size is analyzed.
- The analysis of the decryption time with respect to the number of attributes is analyzed for the existing Attribute Based Encryption (ABE), and the proposed SKPBE methods.
- Further, the encryption/ decryption time, and encryption speed for the existing KP-ABE, CP-ABE, CP-ABE-WP methods are compared with the proposed SKPBE.

The overall flow of the proposed ELGammal based Source Key Policy Based Encryption is depicted in the figure 1.0.

The proposed method includes has three important components such as process of key setup process, source key policy generation, policy and key verification. The detailed description about each component is illustrated in the following sections.

4.1 SKPBE:

To address the security issues of the cloud such as complexity of the system, shared multi-tenant environment, and control loss, the cryptographic technique is exploited. The security model of the proposed system includes three processes such as, source key and policy generation, encryption and decryption.

4.1.1 Key Setup process:The SKPBE is used for one-to-many encryption. By exploiting the attributes, the public key for encrypting the data is generated. In SKPBE, there exist three main factors such as authority, data owner, and data user. The data owner maintains the data for sharing. The data owner initially registers their data in the cloud server, and obtains their access by authorizing the credential information from the cloud server. The data owners can process or create the data file. Further, they can generate the data repository for deriving the data owner attributes. The role of the data user is to decrypt the encrypted data using the private key received from the authority. While decrypting the data, the attributes in the private key of the data user, and the attributes in the encrypted data should be matched. If there exists a match, the data is decrypted else the data user is not allowed to decrypt the data. In this phase of the research, the ABE exploits the attributes of the data, and the data owner for encrypting, and decrypting the messages. The information related to the data owner are preserved, managed, and backed up in the cloud repository. The data owners access the cloud repository through the internet. Subsequently, the key evaluation mechanism is analyzed for the security purpose. After analyzing the key evaluation mechanism, the attributes of the data, and the data owner are obtained.

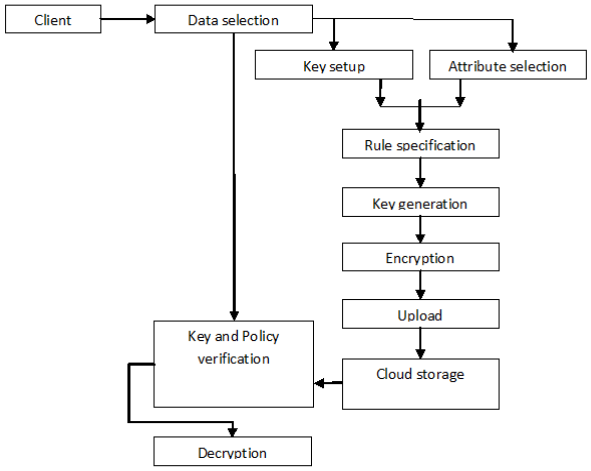

Figure 1.0 proposed SKPBE architecture

4.1.2 Encryption: The encryption is the process of converting the plain text into the cipher text that could not be understood

by anyone except the authorized person. The data is often encrypted using the encryption algorithm, and an encryption key. The encryption process creates the cipher text that could be viewed in the original form if decrypted using the correct key. The encryption process can be executed by anyone who wants to encrypt the data.

4.1.3 Decryption: The decryption is the process of converting the cipher text into the plain text. The data is often decrypted using the decryption algorithm, and the decryption key. The decryption process is executed by the delegate who received the aggregate key that was generated by the extract process. In order to decrypt the cipher text on the receiver end.

- Aggregate key
- An index that represents the class of the cipher text
- Cipher text

V. RESULTS AND ANALYSIS

The proposed system has successfully implemented and the results are compared with the existing schemes. The analysis is made in terms of time, and security performance for proposed SKPBE. Besides, the comparative analysis between SKPBE and existing methodologies such as conventional ABE, KP-ABE, CP-ABE, and HABE and MA-ABE also discussed to assure the effectiveness in cloud security model creation.

5.*1 Performance Measures*

The performance criteria of proposed SKPBE are measured by using the time required for both encryption and decryption. The description of each performance metric is illustrated as follows:

*Encryption Time:*The time required by the algorithm to covert the plain text into cipher text refers encryption time. The variation in file sizes and the number of key attributes causes the maximum encryption time. The algorithm is referred better only if the encryption time is minimum with increase of file sizes and key attributes

Table 2.0 Attribute based encryption comparative analysis

Size in KB	Existing (time in seconds)	Proposed
1	49	22
10	61	39
100	73	40

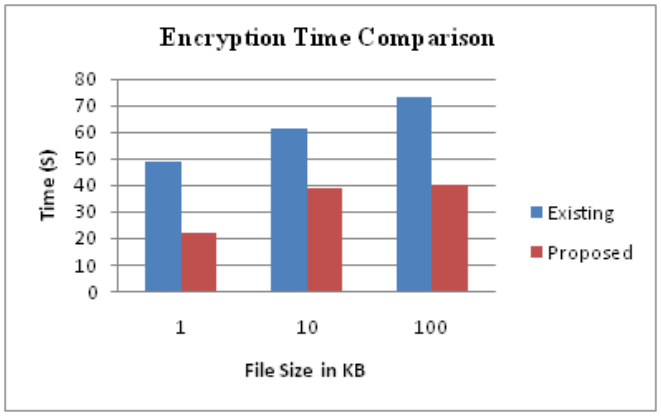

Figure 2.0 Encryption time comparisons

The analysis of encryption time with varying file size and the comparison between the proposed SKPBE and role based access control. The increase in file size gradually increases the encryption time.

Decryption Time: The time required by the algorithm to covert from the cipher text into the plain text refers decryption time. The variation in file sizes and the number of key attributes causes the maximum decryption time. The algorithm is referred better only if the decryption time is minimum with increase of file sizes and key attributes.

Table 3.0 Attribute based encryption comparative analysis

No.of attributes	ABE	SKPBE
1	0.123	0.052
10	0.147	0.056
20	0.15	0.1
30	0.172	0.12
40	0.2	0.14
50	0.226	0.152

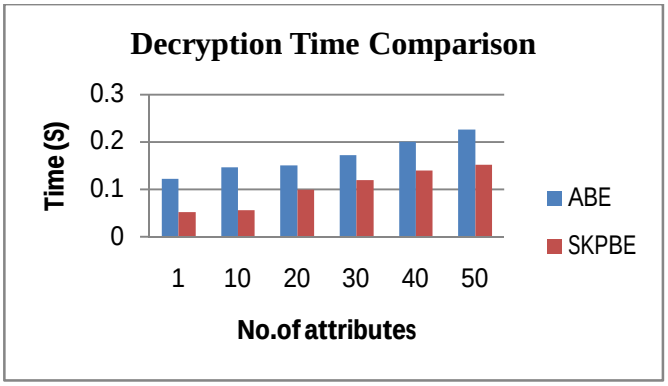

Figure 3.0 Decryption time comparisons

From the figure 3.0, the conventional ABE schemes extended with the inclusion of verification of outsourcing description. The variation of number of attributes from low to high value leads to increase of decryption time. The comparative analysis between the proposed SKPBE and existing ABE with the outsource verification for decryption time conveyed that the proposed optimal key derivative policies provided the less time consumption

Security Performance: The security analysis of proposed Derivative Key Policies (SKPBE) and the high level access control vector based group key management with subset cover optimization for number of key attributes involved. For each number of key attribute, the security performance is estimated as a percentage value.

Table 4.0 Attribute based encryption comparative analysis

Number of key attributes-Security Performance (%)	Existing	Proposed
1	21	39
2	42	50
3	58	61
4	62	80
5	78	80

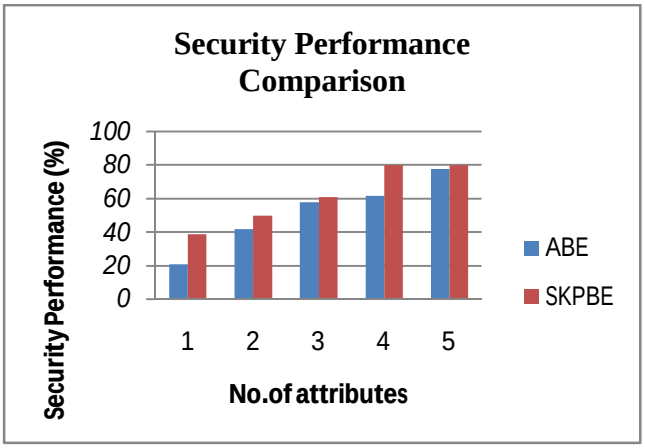

Figure 4.0 security performance comparisons

The performance analysis results show that the proposed SKPBE provides less encryption time in regard of file size. Further, it provides optimal encryption speed than the existing methods. When the number of requests rises, the SKPBE will fail by restriction of the attributes. Hence, in the next chapter, the proposed SKPBE integrates the attributes in the attribute-based encryption with the several numbers of requests. The major problems in traditional approaches are more encryption time, computational cost with less processing speed. But, in the SKPBE the results are improved on the basis of ELGammal encryption. The better solutions provided by the proposed SKPBE assures the confidentiality and integrity with the improved security level.

VI. CONCLUSION

The paper addressed the secure data access issues in the cloud. The paper has summarized various attribute based encryption scheme and finally proposed a new policy based ABE scheme for secure data access, which overcomes different types of research challenges. This initially reduces the time for encryption, decryption and key generation time delay. This utilizes the Elgammal encryption scheme, which is an public key encryption system based on the differ hellman key exchange scheme. Using this scheme, the proposed system performs Source policy based encryption named as SKPBE. This scheme assures the data protection in the cloud. The knowledge about the security level and data access vulnerabilities is considered as the initial stage of encryption mechanisms. The application of encryption and decryption mechanisms assured the privacy protection of cloud deposited data. The analysis of existing ABE schemes is compared with the proposed system and proposed system provides high security and less computation time.

REFERENCES

[1] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al. "A view of cloud computing." Communications of the ACM 53, no. 4 (2010): 50-58.

[2] Luo, Jun-Zhou, Jia-Hui Jin, Ai-bo Song, and Fang Dong. "Cloud computing: architecture and key technologies." Journal of China Institute of Communications 32, no. 7 (2011): 3-21.

[3] Dahbur, Kamal, Bassil Mohammad, and Ahmad Bisher Tarakji. "A survey of risks, threats and vulnerabilities in cloud computing." In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications, p. 12. ACM, 2011.

[4] Grobauer, Bernd, Tobias Walloschek, and Elmar Stocker. "Understanding cloud computing vulnerabilities." IEEE Security & Privacy 9, no. 2 (2011): 50-57.

[5] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28, no. 6 (2012): 833-851.

[6] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In Computer Science and Electronics Engineering (ICCSEE), 2012

International Conference on, vol. 1, pp. 647-651. IEEE, 2012.

[7] Sarathy, Rathindra, and Krishnamurty Muralidhar. "Secure and useful data sharing." Decision Support Systems 42, no. 1 (2006): 204-220.

[8] Wang, Cong, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for secure cloud storage." IEEE transactions on computers 62, no. 2 (2013): 362-375.

[9] Yang, Kan, and Xiaohua Jia. "DAC-MACS: Effective data access control for multi-authority cloud storage systems." In Security for Cloud Storage Systems, pp. 59-83. Springer New York, 2014.

[10] Graf, Sebastian, Patrick Lang, Stefan A. Hohenadel, and Marcel Waldvogel. "Versatile key management for secure cloud storage." In Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on, pp. 469-474. IEEE, 2012.

[11] Li, Jin, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick PC Lee, and Wenjing Lou. "Secure deduplication with efficient and reliable convergent key management." IEEE transactions on parallel and distributed systems 25, no. 6 (2014): 1615-1625.