International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 927-936 June - Dec 2018 www.csjournals.com

Security in Cloud Computing: A Review

Nirmal[1], Sanjeev Kumar[2]
[1,2]Department of CSE, Guru Jambheshwar University of Science & Technology, Hisar, INDIA

Abstract: In recent years, Cloud Computing has been a growing technological field. It is used to store and access data and programs via the Internet rather than through a computer. This feature motivates the move from local infrastructure to off-site data centers accessible via the Internet and managed by cloud hosting providers. For its benefits, moving to this computational paradigm creates security problems that lead to a new dimension of cloud security. This article reviews work on cloud security issues and develops a general literature review.

1. Introduction

Cloud computing is a recently introduced innovation. Used for processing on the Internet. A cloud computing service consisting of highly optimized virtual servers. These virtual machines offer numerous software, hardware and data resources that can be easily used. Organizations can connect directly to the cloud and use these services in pay-per-use facilities. This helps companies avoid capital expenditure on additional local infrastructure resources and immediately increase or decrease as required [6]. Cloud computing separated the application from the operating system and hardware via middleware. Therefore, for cloud computing, if the operating system or hardware does not work, the application services do not stop. There is no doubt that cloud computing has many advantages that an organization can use. There are some basic features of cloud computing, such as virtualization, on-demand services, fast flexibility, broad network access, resource group, measured service. All types of services are divided into three areas: IaaS (Infrastructure as a service), PaaS (Platform as a service) and SaaS (Software as a service) [7]. All these services are provided and used in real time over the Internet. IaaS includes services that provide consumers with infrastructure such as hardware, network, connectivity and storage, while PaaS provides the waiting environment as a service to manage, develop and test applications. SaaS refers to the category of services where the software is provided over the Internet. Therefore, there is no need to install software or pay for software and purchase licenses. All services, such as water or electricity, are used as public services. There are three types of clouds in the cloud delivery model. It includes public, private (local) and hybrid clouds. The public cloud corresponds to the Internet according to the standard cloud computing model. The service provider uses the Internet to provide all services to the user. Services can be free or paid. An organization has private or local clouds. It offers all the advantages of the public cloud, such as: B. Flexibility, monitoring, automation and administrative support. It offers more security in the cloud, since it is implemented in the firewall. The public and private hybrid is a hybrid cloud. Both are mixed to use both and create more value [8]. Although the cloud has many advantages, but it is an evolving technology, there are still many problems and challenges in the area of cloud computing.

Cloud Computing SecurityIssues: There are many issue related to privacy, security in cloud computing.The security issues are concerned in cloud computing because in cloud at any time the data can outbreak the service provider and the information is deleted deliberately. Fig. 1 shows organization of data security and privacy in cloud computing environment.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 927-936 June - Dec 2018 www.csjournals.com

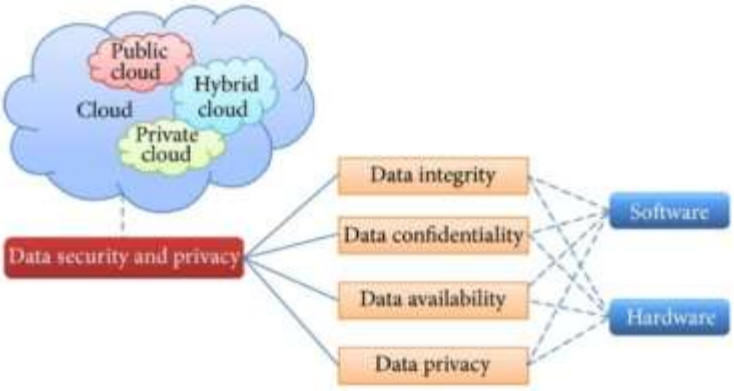

Fig 1 : Data security and privacy in cloud computing

The cloud is expected to offer features such as encryption strategies to ensure a secure data storage environment, rigorous access control, secure and stable backup of user data. However, the cloud allows users to reach computing power that exceeds their physical domain. This leads to many security problems. The main security concerns are:

Identification and Authentication: Multiple access to the cloud allows access to one instance of the software for more than one user [3]. This will create an identification and authentication problem because different users use different tokens and protocols, which can cause interpretation problems.

Access control: illegal access to confidential data can be obtained due to moderate access control. If the appropriate security mechanisms are not used, there may be unauthorized access. Since data has been in the cloud for a long time, the risk of illegal access is greater [3].

Data interception: the company providing the services may violate the law. There is a risk of data interception by foreign government institutions.

Encryption/ Decryption: There is an issue of the Encryption/ Decryption key that are provided. The keys must be provided by the customer itself.

Policy Integration: different servers in the cloud can use different tools to ensure the security of customer data. That is why integration policy is one of the main security problems.

Accessibility: accessibility is the main problem in cloud computing. During virtualization of customer data, customers have no control over physical data [3]. If the data or service is not available in the cloud, it is difficult to obtain the data.

Secure Data Management: because data is an important element of cloud computing in aspects of the secure cloud. In particular, security concerns, ranging from how to effectively store data on foreign computers, to queries about encrypted data, because a large part of the data in the cloud can be encrypted, is a key challenge in the implementation of security schemes in Cloud Computing [8].

Resource Allocation: in the cloud model, we lose control over physical security. In the public cloud, we share computer resources with other companies. In the shared group outside the company, we have no knowledge or control over where the resources are executed. Disclosing our data in an environment shared with other companies may give the government a "reasonable cause" to confiscate its assets because another company has broken the law. Simply because we share the cloud environment, you can put your data at risk of confiscation. Storage services provided by a cloud service provider may not be compatible with another provider's services if they choose to switch from one provider to another. Therefore, highly encrypted systems are required to protect resources in the cloud.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 927-936 June - Dec 2018 www.csjournals.com

2. Existing Algorithms for Cryptographic Security

The encryption is used in cryptography to obtain confidentiality, integrity, availability and authentication of data. There are two main categories of encryption algorithms. These categories are symmetric and asymmetric encryption algorithms. Figure 1 shows the further classification of these algorithms[6].

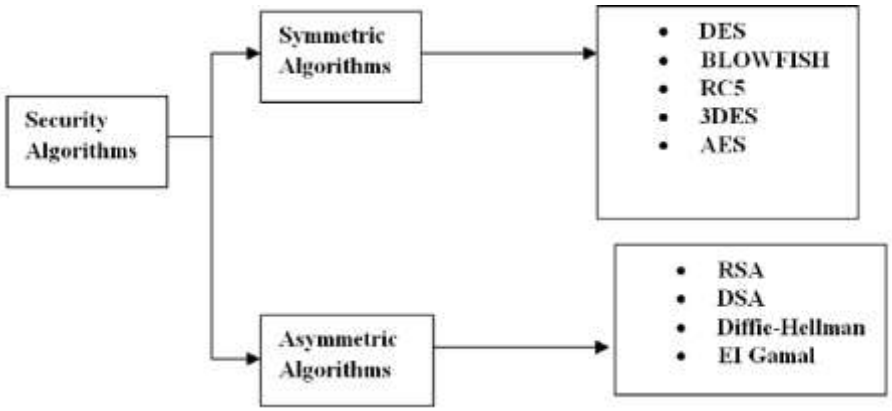

Figure 1: Cryptographic Security Algorithms

Symmetric Algorithms:

In Symmetric key encryption, only single key is used for encrypt the data and same key is used to decrypt the data. SomeSymmetric encryption algorithms are discussed here.

- **Data Encryption Standard (DES):** DES[6] is a block cipher that uses shared secret key for encrypt and decrypt. The DES cryptography approach is defined by Davis R. Obtain a fixed-length string that is transformed by a series of complicated operations on the bit of the encrypted text string.In the case of DES, the entire block size is 64 bits. DES uses a 56-bit key for encryption, so that the decryption procedure can only be performed by someone who knows the key used to encrypt the information.The broad level phase in DES is as follows: 1) In the first phase, 64-bit plain text data is transferred to an IP function. 2) The IP is achieving on plain text. 3) The IP produces two different halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT). 4RPT and LPT pass through the 16 round coding process. 5) RPT and LPT are rejoined and a final permutation (FP) is obtained in the combined block. 6) The results of this procedure produce 64-bit encrypted text. Rounds: All of the 16 stages, in turn, consist of the broad level steps.

- **BLOWFISH:** It is one of the most common public algorithms. It is developed by Bruce Schneierin 1993. Blowfish has a variable length key, 64-bit block cipher.It is not known that any attack wins against this.The survey showed the superiority of the Blowfish algorithm compared to other algorithms in terms of computation time. Blowfish was designed with the followings goals in mind: a) Encryption rate is fastb) Blowfish uses only simple operations. These operations are addition, XOR and table search. These operation makes its design and implementation are simple. c) Secure-Blowfish is secured due to its variable key length, which is up to maximum of 448-bit.d) Blowfish is suitable for applications where the key does not change for a long time (for example, communication link encryption), instead of the application where

the key frequently changed(for example, Packet Switching). Blowfish is superior to other algorithms in terms of performance and energy consumption [8].

- **3DES:** This was enhancement of DES[7] and developed in 1998.This 3DESEncryption technique issame as original DES butit always usesthe threekeys to increase the encryption level.Encryption is done by first key and Decryption is done by second key.Third key again used for encryption. But 3DES is bit slower than other block cipher methods. Because of its triple phase encryptionit requires moretime than DES.

- **AES: (**Advanced Encryption Standard)[10], The most popular and most widely used symmetric encryption algorithm that will probably be found today is the Advanced Encryption Standard (AES). It is at least six times faster than triple DES. DES had to be replaced because the key size was too small. Due to the increasing computing power, it was considered vulnerable in the face of a comprehensive key search attack. Triple DES was designed to overcome this inconvenience but proved to be slow. The AES is Symmetric key symmetric block cipher. It is Stronger and faster than Triple-DES. AES is an iterative code instead of Feistel. It is based on a "substitution and permutation network". It includes a number of related operations, some of which involve replacing the input data with specific output data (exchanges) and others with bit shuffling (permutations). It is worth noting that AES performs all calculations in bytes instead of bits. Therefore, AES considers 128 bits of a plain text block to be 16 bytes. These 16 bytes are arranged in four columns and four rows to process them as an array. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, calculated from the original AES key. AES can be implemented on various platforms especially in small devices.Therefore, now one day AES is widely used for security in the cloud. The implementation proposal states that first of all the user decides to use cloud services and will migrate their data to the cloud. The user then submits his service requirements to the cloud service provider (CSP) and selects the best specific services offered by the provider. When data is migrated to the selected cryptographic service provider, and in the future each time the application loads data to the cloud, the data will be first encrypted with the AES algorithm and then sent to the provider. After encryption, the data is sent to the cloud, any request to read data will appear after being decrypted by the user, and therefore readable data can be read by the user. The plain text data is never written anywhere on cloud. This includes all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications.

Asymmetric Algorithms:

Two keys are used in AsymmetricEncryption. One key is public key which used forencryption and other key is private key which used for decryption.SomeAsymmetric encryption algorithms are discussed here.

- **RSA ALGORITHM**:Its named after the creators Rivest, Shamir and Adleman (RSA)[7]. In RSA, the public key is distributed to everyone, through which the message can be encrypted, and the private key used for decryption is kept secret and not shared with everyone. The way in which RSA works in the cloud computing is elucidated as follows: We have encrypted our data in the RSA algorithm to ensure security. The goal of data security is to access them only to interested and authorized users. After encryption, the data is stored in the cloud. So you can contact your cloud service provider if necessary. The cloud service provider authenticates the user and provides data to the user. Because RSA is a block code where each message is assigned to an integer. The public key is known to everyone, while the private key is known only to the user who originally owned the data. In this way, the cloud service provider performs the encryption and the user or consumer in the cloud decrypts it. Once encrypted with a public key, the data will be decrypted.

- **Diffie-Hellman Key Exchange (D-H)**: It is a method of exchanging cryptographic keys [8] by establishing a common secret key that will be used for communication between them and not for encryption or decryption. This key exchange process ensures that both parties do not have prior knowledge about the joint establishment of a secret key shared on aunsecure Internet. The key transformations are exchanged and both end with the same session key that looks like a secret key. This allows anyone to calculate the key for the third session, which cannot easily be obtained from an attacker who knows both values. This key encrypts subsequent communications with a symmetric key code, but is vulnerable to a Man-in-the-Middle (MITM) attack.

3. Security Solutions in Literature

Yibin Li, Kekegai et al. [1] description of how many applications in the cloud have been limited due to critical problems related to data security and privacy, and one of them is that sensitive data is reachable to the cloud operators. Therefore, in the proposed smart approach for cryptography, due to the compilation of partial data not available to cloud service operators. In this proposed approach, distributed cloud servers are used to store data after dividing the data file, and the approach used is the SA-EDS model (security-efficient distributed storage).Jiaqi Zhaoet al.[2]proposed a security framework for G-Hadoop which provides security solutions such as SSL protocol.This security model simplified the user's authentications. This security framework provides the protection of traditional attacks to the G-Hadoop system.

Manogaran, Gunasekaranet al.[3] proposed a Big Data protection by MetaCloudDataStorage Architecture in Cloud Computing Environment. The number of the user who logged in to the cloud data center was found using the Map Reduce platform and the various data elements assigned to the suppliers are protected using the proposed platform, which is the

MetaCloudDataStorage interface. This proposed approach requires many implementation efforts that provide valuable insight into the cloud computing environment.

In [4] a big structure is bringing forth by analysis on cloud authenticator-based data integrity verification techniques.A simple aspect of the search problem is being analyzed. First, the motivations and research methodologies were summarized to illustrate the research problem. Second, the representative addresses several current results, which are summarized and compared. Finally, future changes have been made to visualize the possibilities.

Ramachandran, Muthu et al.[5] gaves general evaluation of the cloud and data security literature. The data security and security design is provided as a service which is explained in the use of Business Process Modeling Notations (BPMN).In this paper two cloud service providers and their security design are analyzed. The BPMN can be used to identifiedthe attack on the security service section, in case of any security breach. For more resilient and reliable security service in business, integrating CCAF version 2 with BPMN.

JoonsangBaeket al.[6] proposed a secure cloud computing based framework which is called as Smart Frame. The hierarchical structure of cloud computing centers is built within it, which provides several cloud services for information management and analysis of large data sets. When solving critical security problems within the proposed framework, a security solution based on identity-based encryption, signature and proxy re-encryption is provided.

Mehdi Sookhaket al.[7] proposed an effective Remote Data Audit (RDA) technique for the cloud storage system, which is based on algebraic signature properties that cause minimal processing and communication costs. The Divide and Conquer (DCT) table also presents a new data structure that can efficiently support the structure of dynamic data such as adding, inserting, editing and deleting. Compared to other latest generation RDA techniques and their proposed approach, it shows that their approach is very efficient and safe, which helps to reduce communication and calculation costs on the server and auditor.

KekeGai et al. [8] focuses on problems with large data sets, and their practical implementation is being considered in the cloud. To maximize the performance of privacy protection, a dynamic data encryption (D2ES) approach was developed. The DED algorithm mainly supports the D2ES model developed for the encryption of dynamically alternative data packets with different time constraints. The main objective of this approach is to maximize privacy protection through selective encryption strategies with specific runtime requirements.

Syam Kumar et al. [9] proposed an efficient and secure approach to protecting privacy, which is used to outsource data on mobile devices with limited resources in the cloud and to encrypt data, the probabilistic public key cryptography algorithm. To recover files from the cloud by encrypting the data, an implicit keyword search is activated. The goal of this approach is to achieve an efficient data encryption system without sacrificing data privacy.

Sandeep K. Sood [10] proposed specialized procedures and various techniques as part of the work in which the data is effectively protected from beginning to end, that is, from the owner to the cloud, and then to the user. Three cryptographic parameters presented by the user based on the beginning of the data classification, for example, Confidentiality (C), Availability (A) and Integrity (I). It also applies to a data protection strategy that uses a variety of measures, such as 128-bit SSL (secure sockets layer) encryption, and can be increased to 256-bit encryption if necessary, to verify the integrity of the data. data through MAC (Message Authentication Code), encrypted with the ability to search and divide data in the cloud into three sections in the cloud.The supplementary protection is rendered by the data division into three sections and data simple access.

Shaikh Rizwana et al. [11] describes the active area of experiments and research in the field of data security and cloud privacy. Organizations that move to the cloud, privacy protection and data loss are paramount. There are different types of data and the level of protection

required for each type of data varies. A classification technique is proposed in which the parameters are determined on the basis of different dimensions. At a basic level, data security is guaranteed, where protection is required, and depending on the classification of data sets in storage security provisions, it is applied based on their size. The proposed classification scheme, in which a series of sample data was collected, on the basis of which its performance was analyzed.

Yibin Li et al. [12] proposed an approach to secure financial services in the cloud computing of large multimedia datasets according to which semantic-based control (SBAC) is an innovative approach. The proposed approach is the IntercroSsed Secure Big Multimedia Model (2SBM). This approach is essentially designed to securely access various media through multiple cloud-based platforms. The proposed model is compatible with the main algorithms, which include the OBAR algorithm (access recognition based on ontology) and the semantic information matching algorithm (SIM).

In this paper [13], financial customer privacy information is protected by a proposed algorithm called Proactive Dynamic Secure Data Scheme (P2DS) with attribute-based access control (ABAC), as well as a data self-determination scheme, and the its purpose is to provide privacy data was not unexpected by a third party. The proposed scheme is compatible with two main algorithms, which are the attribute-based semantic access control algorithm (A-SAC) and the proactive access determination algorithm (PDA). The main contribution of this document are three aspects: firstly, to limit access to data, a semantic approach is proposed. Second, a user-centered approach is proposed that prevents proactive execution of user data in unexpected operations on the cloud side and finally a high level of secure security is found in the proposed scheme because it refers to dynamic threats, including threats and future emergency situations.

ChandrasekaranBalaji et al. [14] described the IBE (Identity Based Encryption) scheme, in which identities are used as a chain. According to three theories, its principle of operation depends on bilinear coupling, quadratic waste and networks. The extended type of identity-based encryption is (attribute-based encryption), which uses a set of expressive attributes instead of identities. It is an effective access control mechanism to calculate encrypted text for a group of users based on the access structure. Very often, existing ABE schemes are based on double line coupling. The constructions of the new ABE scheme take place in square waste and assign a relationship based on a fundamental arithmetic theorem. In this approach, in a cloud environment, the most serious threat to large data sets is the access control of unauthorized users, which is avoided due to the lower number of instances of the user attribute set in the square value.

In Paper [15], a novel approach is proposed so as to place the data in the in cloud storage systems. First, a linear programming model as a data placement problem is formulated so as the data's total retrieval time is minimized and over storage nodes it is divided and distributed under the security constraint. The problem is solved by developing a heuristic algorithm for cloud storage Systems (SEDULOUS) that is Security-aware Data placement mechanism. And the proposed algorithm effectiveness is demonstrated through comprehensive simulations.

GaiKekeet al.[16] uses a decision tree technique to predict the potential risk of data exchange between financial services institutions. A targeted approach is to reduce the possibility of privacy leaks shared by many datasets. SEB-SIC (classification of secure information based on supervised learning) is a proposed model compatible with the proposed algorithm, which is the DTRP (risk prediction based on a decision tree) algorithm. The efficiency of the scheme used is good, as shown in the experimental marks on precision exams, but it creates an additional computational load. In this document, the topics on which it focuses and its proposed approach use a combination of supervised learning techniques to classify

information in order to avoid disclosure of harmful information to both financial service providers and customers.

Sam Adam Elnagdyet al.[17] described that there is a remarkable increase in the demands of mitigating losses for financial firms from cyber incidents and that has derived the rapid growth in the Cyber security Insurance (CI). In the current applications, there are some uncovered number of dimensions as still CI is at is stage of exploration and one of the critical issue in the CI is cyber-attack. The proposed framework is CA-HCIA (Cost-Aware Hierarchical Cyber Incident Analytics),in which the security cost is reduced without the security level lowering down.Victor Chang et al.[18] explained the overview on the CCAF rationale and components for protecting the data security, the system design of the CCAF is illustrated. The BPMN simulation use which allows the evaluation of the chosensecurity performances before the actual implementation. Demonstrating in this paper the CCAF multi-layered security for the data protection in real time.Jinguang Han et al. [19] proposed a decentralized ABE policy framework on privacy, in which each authority issues a secret key to the user independently. Therefore, if many permissions are corrupted, user attributes are not collected by GID tracking. In particular, the system requires assumptions of standard complexity and collaboration of several bodies is not required, unlike the previous comparable program, which requires assumptions of non-standard complexity (for example, q- Diffie-Hellman reversal decision) and interaction with many organs. Based on assumptions of standard complexity with privacy protection, this is ABE's first decentralized program.

In Paper[20], a novel patient-centric framework is proposed and for data access control as a mechanisms suite to PHRs. For PHRs file, fine-grained and scalable data access control is achieved and for encrypting each patient's PHR file leverage the attribute based encryption (ABE) techniques. This paper focused on the many data owner scenario and splits the PHR system user into multiple security domains which eases the key management complexity significantly for owners and users. Simultaneously, guaranteed the patient privacy of high degree by the exploitation of multi-authority ABE. The access policies or file attributes dynamic modification is also enabled in the scheme in which efficient on-demand user/attribute revocation is supported and also under emergency break-glass access is supported.

Conclusions

The publicity of cloud computing model is pushing the IT industry in the direction of a long-envisioned era. Nowadays it is theutility, likewater, electricity, gas and telephony.The basic product of on-demand services is a realistic result for many small and medium-sized enterprises, which mainly reduces the overall infrastructure costs. With this new technology, clouds are still subject to improvements, namely concerningsecurityHistory has shown that security should be a top priority, which is why analyzing the literature in this paper clearly indicates how to address cloud security issues. This review draws strong will and momentum to design secure cloud, informational intentions for academic and industry environments. As this field matures, solid complementary methods should be provided to meet the stringent requirements of cloud environments. Although cloud computing is now a normal technology and is still evolving, its conversion should provide more optimized solutions.

REFERENCE

[1] Yibin Li, Kekegai, LongfieQiu, Hui Zhao"Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences 2016.
[2] Jiaqi Zhao, Lizhe Wang, Jie Tao, DimitriosGeorgakopoulos "A security framework in G-Hadoop for big data computing across distributed Cloud data centers," Journal of Computer and System Sciences 80.5, 994-1007, 2014.
[3] Manogaran, Gunasekaran, ChanduThota, and M. Vijay Kumar "MetaCloudDataStorage architecture for Big Data security in cloud computing," Procedia Computer Science 87, 128-133, 2016.
[4] Chang Liu, Chi Yang, Xuyun Zhang and Jinjun"External integrity verification for outsourced big data in cloud and IoT: A big picture," Future Generation Computer Systems 49, 58-67, 2015.
[5] Ramachandran, Muthu and Victor Chang "Towards performance evaluation of cloud service providers for cloud data security," International Journal of Information Management 36.4, 618-625, 2016.
[6] JoonsangBaek, QuangHieu Vu, Joseph K. Liu and Yang Xiang"A secure cloud computing based framework for big data information management of smart grid," IEEE transactions on cloud computing 3.2, 233-244, 2015.
[7] Mehdi Sookhak and Abdullah Gani "Dynamic remote data auditing for securing big data storage in cloud computing," Information Sciences 380, 101-116, 2017.
[8] KekeGai, MeikangQiu, Hui Zhao and JianXiong "Privacy-aware adaptive data encryption strategy of big data in cloud computing," Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on. IEEE, 2016.
[9] Pasupuleti, Syam Kumar, SubramanianRamalingam, and RajkumarBuyya "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," Journal of Network and Computer Applications 64, 12-22, 2016.
[10] Sandeep K.Sood "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications 35.6, 1831-1838, 2012.
[11] ShaikhRizwana and M. Sasikumar"Data classification for achieving security in cloud computing,"Procedia computer science 45, 493-498, 2015.
[12] Yibin Li, KekeGai, Zhong Ming and MeikangQiu "Intercrossed Access Controls for Secure Financial Services on Multimedia Big Data in Cloud Systems," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 12.4s 67, 2016.
[13] MeikangQiu, Kekegai, BhavaniThuraisingham and Hui Zhao "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry," Future Generation Computer Systems2016.
[14] ChandrasekaranBalaji and RamadossBalakrishnan "Attribute Based Encryption Using Quadratic Residue for the Big Data in Cloud Environment," Proceedings of the International Conference on Informatics and Analytics. ACM, 2016.
[15] Seungmin Kang, BharadwajVeeravalli and KhinMiMiAung"A Security-Aware Data Placement Mechanism for Big Data Cloud Storage Systems," Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016.
[16] GaiKeke, MeikangQiu and Sam Adam Elnagdy"Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data," Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE

International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016.

[17] GaiKeke, MeikangQiu and Sam Adam Elnagdy "A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance," Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016.

[18] Victor Chang and MuthuRamachandran "Towards achieving data security with the cloud computing adoption framework," IEEE Transactions on Services Computing 9.1,138-151,2016.

[19] Jinguang Han, Willy Susilo, Yi Mu and Jun Yan "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems 23.11,2150-2162, 2012.

[20] Ming Li, Shucheng Yu, Yao Zheng, HuiRen and Wenjing Lou "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE transactions on parallel and distributed systems 24.1, 131-143, 2013.