Volume 6, Issue 3
June 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



# Combination of Cloud Computing Methods to Enhance Security and Privacy

**[1]Hashem Alvandi Kheradmand, [2]Anita Dashti ,[3]Mohammad Davarpanah Jazi**

[1]Department of Electrical Engineering, Graduate student of IT Engineering , Steel-of-Fooladshahr- Institute of Higher Education for postcode 8491663763

[2]Department of Electrical Engineering, Graduate student of Software Engineering , Steel-of-Fooladshahr- Institute of Higher Education for postcode 8491663763

[3]Department of Electrical Engineering, Assistant Professor, Department of Computer Engineering and Information Technology, Isfahan -Fooladshahr- Institute of Higher Education for steel - code 8491663763

E-mail: [1]Hashem313@Gmail.com, [2]Anita.Dashti2015@Gmail.com , [3]mdjazi@cc.ui.ac.ir

## ABSTRACT

Today security and privacy plays an important role in cloud computing technology. Users are concern about their data transferred to the cloud side. It is CSP's responsibility to take care of user's data. Security assurance in cloud computing has the highest priority because users need to store their sensitive data on cloud server resources provided by cloud service providers. In this paper the main focus is on privacy and security in cloud computing, the aim is to combine methods to get into a new way to have more privacy and security for user data. A review for security and privacy methods in cloud computing is provided then according to them increasing encryption is combined by virtualization to have an optimized method. This new method will be an important achievement in privacy and security of cloud computing and all other inherited technologies.

**Keywords:** privacy, cloud computing, data security, increasing cryptography, virtualization, mobile cloud computing.

## 2.INTRODUCTION

The main concern in cloud computing is data security and privacy. When data is transferred to cloud-side servers, users does not have any physical control to their data any more. So they are worried about the security and privacy of their sensitive data. Although using cloud computing resources brings some advantages for users like reducing costs and increasing agility, but because of wireless networks and misusing information by illegal access via internet, users are always worried about their data. Cloud service providers that belong to an organization or big companies can access to the users' data easily and without the need for owner's permission. So cloud service providers must cover security and privacy issues and reassure users that their data is all in peace. Cloud service providers should use strongest method for providing security and privacy, if not they would have a big failure.

Mobile cloud computing includes the concept of cloud computing, mobile computing and wireless networks and tries to provide cloud services for customers. Mobile devices supply from their battery, they have limited storage and computational resources and also security is not as appropriate as needed. These kind of limitations is always an obstacle for applications those who need more storage and computational resources in a mobile device. For overcoming these limitations there must be a cloud that can be accessed anywhere at anytime needed to perform storage and computational offloading to the cloud side. The single cloud environment has more security challenges and today most of the cloud service use multi-cloud services to reduce these kind of security and privacy challenges and increase user reliability. There has been many private and public cloud servers are started up.

Understanding the importance of having proper security and privacy and developing effective solutions is essential. Not only the strategies to prevent leakage and protect the confidentiality and privacy of user data is the main purpose in cloud service providers, but also increases their responsibilities. Moreover having comprehensive rules established by government and supervisor institution is essential to have proper implementation of regulation. There are different approaches for having better security and privacy in cloud computing. Privacy in cloud computing is collection, usage, publication, storage or destruction of private and sensitive information. The meaning of privacy and security is similar to traditional ones and the concept is the same in all stages of data life cycle, but it will be somehow special because of cloud's open and multi-tenant feature.

Volume 6, Issue 3
June 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



## 3. REVIEW OF METHODS TO HAVE PRIVACY IN CLOUD COMPUTING

According to researches available in cloud computing privacy, the authors decided to review four of the best methods proposed by different people. It would help to compare methods to have a better understanding of which is better and more reliable than other proposed methods. It is predicted that using a single cloud may cause regular disconnection and abusive people will perform some interruption so that the trend is into multi-cloud systems. Multi-cloud systems tend to be a new trade to grow rapidly in the future.

### 3.1 PROPOSED METHOD BY SADR-AL-SADATI

One of the secure sharing tools for data stored on cloud computing is encryption to protect confidentiality, privacy and integrity. This condition can be provided using increasing encryption or Homomorphic cryptography. Homomorphic cryptography is a kind of encryption that algebraic structure will be applied on data to produce cipher text. Multi users simultaneously can produce cipher text without collision and being aware of other user's data. Increasing encryption allows processing of encrypted end data according to initial encrypted data for making changes on unprocessed data. For sharing encrypted data, without having initial decryption, re-encryption will be performed. This re-encrypted data will be used only by legal users using authentication methods. During sharing process data will be showed in encrypted format, even if encryption might be done by different keys during different stages. Data will be decrypted only if the data owner gives the permission to CSP [1].

### 3.2 PROPOSED METHOD BY WEICHAO WANG

The smallest part of data is block. Data owner can encrypt blocks and send them to the cloud. End user can send request for accessing the data to data owner. Data owner refers to access control matrix then sends the data access certificate to the end user via a secure channel. After that the end user send the received certificate to cloud service provider, thus the cloud service provider checks the certificate and if it is verified, encrypted data blocks will be sent to the end user. At last the end user can decrypt the encrypted data blocks via received cipher key from the data owner [2].

### 3.3 PROPOSED METHOD BY MOHAMMADI

In this proposed method not only data privacy but also access control is provided for data owners. This proposed method has four identity including data owner, inductor, cloud service provider and user. Data owner and CSP can get into agreement via SLA. According to the agreement, N data centers will be considered for storing data of the owner. According to the number of agreed data centers, the owner will divide the file into N blocks which each block consists of two parts with verified label. Both parts will be stored on the cloud server. Verified label consists of some information that according to them blocks can be controlled by the data owner and the inductor. Content of the verified label can be seen only by the data owner and the inductor can access the label via owner's permission. The data owner will define a distinctive key for encrypting of the first block. Although the number of blocks can be much, so the number of encryption key increases. Managing and maintaining these encryption keys is difficult for the owner, so the proposed method decided to use hierarchical structure to extract the key. After sending the block to the inductor, encrypted blocks will be sent to pre-scheduled data centers by the inductor according to received data from the owner. The inductor can control the data just by random or verified label, also can make sure whether the data exists on pre-scheduled data centers. The user can request to have decryption key just by the inductor, and from the owner [3].

### 3.4 PROPOSED METHOD BY GANJI

This method can detect outliers using Rough collection theory. The main purpose of analyzing Rough collection is to obtain approximate concepts through acquired data. This theory is a powerful mathematical tools for reasoning ambiguous things. It also provides omitting and reducing the irrelevant knowledge or additional requirements from the database. The main responsibility of this system is omitting additional data without losing fundamental data on database. After reducing the data, a set of summarized and meaningful data will be gained so decision makers' work get much easier. In fact, Rough collection by reducing data space and choosing important terms will map raw data space and term to meaningful space [4].

Volume 6, Issue 3
June 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



## 3.5 COMPARISON OF PROPOSED METHODS IN CLOUD COMPUTING PRIVACY

| Parameter Reference | Mechanism | Tools used for encrypting/decrypting | Encryption time | Accessibility |
|---|---|---|---|---|
| Sadr-Al-Sadati | Increasing Cryptography | Algebraic structure | Before sending to cloud | Legal users after authentication |
| Weichao Wang | Block | ---- | Before sending to cloud | Access control matrix |
| Mohammadi | SLA | block | Before sending to cloud | Legal users after authentication |
| Ganji | outliers | Graph set theory | ----- | Legal users |

## 4. REVIEW OF METHODS TO HAVE SECURITY IN CLOUD COMPUTING

According to methods proposed in cloud computing security, the authors decided to review four of the best methods. By comparing these methods it would be possible to have a better understanding of which one is more reliable than other proposed methods.

## 4.1 PROPOSED METHOD BY BORSE

### 4.1.1 MULTI-CLOUD STRUCTURE

In multi-cloud environment using SIC architecture, there is a CSP that plays the role of the central and the main server. The SCP stores all existing big data in the system. Clients and users do not know where their data is stored. Data will be stored on a server that could be located anywhere. The CSP will consider the capacity of each server and will evaluate the size of the data, so it can decide which server to store it. The decision process will be performed as a result of load balancing algorithms. The CSP also specifies the storage path on each server. The cloud servers will store only the user's data and don't store anything about the user's personality and identity. For example the central system or the CSP knows all the password and the cipher key to decode encrypted data. This way the CSP must always be kept secured. The CSP acts like an efficient bridge between the users and the cloud servers. As the users have their own data on cloud servers, so that they need these cloud servers for processing it [5].

### 4.1.2 Using data encryption

For having more security on cloud environments, it would be better to perform cryptography. If data is distributed on multi-cloud environment, using better security method instead of encoding is essential. When the user sends data to the cloud, it will be first encrypted and then it will be stored on a cloud server. This way double security level will be provided. For storing data on multi-cloud environment, a symmetric key and a secret key algorithm will be the best choice. A secret key is known as coding. Coding is a hidden technique that the sender and the receiver use the same key for encoding. This technique can be used in multi-cloud storage environment, so that the data can be accessed more easily. A secret key algorithm uses the same key for encoding and decoding. In this technique the secret key must be kept secured because whoever reaches to the secret key, can access the data. The secret key algorithm and the symmetric key algorithm use the same key for encoding and decoding. The difference between these two algorithms is that the secret key algorithm is faster than the other, and is more efficient in transferring huge flood of data in comparison with public key algorithm [5].

## 4.2 PROPOSED METHOD BY PARVEEN

Manipulating big data needs several computational resources. Fast and efficient data transfer will be possible only by having several simultaneous connections. In relational databases two kinds of data has been detected: tables which define a relationship and tables which contain payload data. The first type tables define all the relationship between the tables which contain payload data, also it contains foreign and primary keys that are attached to the tables which have payload data. In some cases these tables can connect together and store in a CSP. Thus, in revealing and showing the result, just a part of the result instead of the whole of it will be shown. The second type contains payload data, e.g. all data that finally will be stored in the table and makes the basic structure of the relational database and also is connected to the linking tables. For optimizing the cost of processes data stored on tables will be divided into small pieces, these are called piece. This technique uses fragmentation to gain data confidentiality and reliability in three steps. These three steps must be performed before storage process. 1- Database must be in three normalization level, so that every table is considered as an independent piece. 2- Reliability level defines data importance

Volume 6, Issue 3
June 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



in the piece. 3- User requests causes additional transferring of pieces. The most important thing is independence and lack of connection between vital tables. The normalization will be get if: 1- Every table be an independent identity. 2- No additional data is stored. 3- Extraneous characters is dependent only to the master key. 4- data integrity and consistency must be provided [6].

## 4.3 PROPOSED METHOD BY TIRODKAR

For preventing data intrusion it is better to user a framework which has two stages. The first stage is encoding and classification which will be performed before storage process. This means in storage process, encoding has the most important priority. So encoding will be classified according to confidentiality, security and accessibility. Using proposed algorithm leads to grading information or CR. Security will be performed by three dimensions. The second stage is retrieving data via the user. Before accessing to the data, the user validation and verification is required. After verifying the user, data must be decoded.

The first step is preparing data for storage. In this step the user can encode the data, so that additional security layer will be provided. Then according to the level of sensitivity, security and accessibility data will be transferred into the cloud server. Then according to this ranking data location will be defined in one of the three loops. This will increase internal protection and confidentiality [7].

### Encoding

The most important priority in storage process is encoding. This will help the user to increase data security. Another most important issues is who manages the cipher keys? The answer would be "users". For having better security level, it would be better that the users manage the cipher keys [7].

### Decoding

After downloading the data, the cipher key will be revealed and the user can access the data [7].

## 4.4PROPOSED METHOD BY GOHARBAKHSH

Virtualization is an efficient way to increase security in cloud computing. In this technology operating system, middle-ware and application will be identically copied, assembled and then put into a physical computer or part of a server. Virtualization increases security in cloud computing by preserving integrity in guest virtual machine and cloud component infrastructure. The most important capability of virtualization is automatic allocation of resources when and where needed. Virtualization allows cloud providers to run any kind of operating systems that users need, also it allows running concurrent operating system and other applications in a physical machine [8].

## 4.5 COMPARISON OF PROPOSED METHODS IN CLOUD COMPUTING SECURITY

| Parameter Reference | Environment | Data Protection | Encryption | Computational Overhead | Technology |
|---|---|---|---|---|---|
| Borse K / 2014 | Multi-cloud | yes | Symmetric cryptography | Medium | SIC architecture |
| Parveen S / 2012 | Multi-cloud | Yes | - | Low | Table normalization |
| Sagar Tirodkar /2014 | Single - cloud | Yes | - | High | 3 loop protection |
| Gowhar / Bakhsh 2013 | Single-cloud | Yes | - | - | Virtualization |

## 5.CONCLUSION

Comparison of 8 methods proposed for security and privacy in cloud computing shows that it would be possible to combine 2 of the best methods proposed for each context to gain a distinct method that can enhance level of security and privacy of mobile cloud computing. The best proposed method in cloud computing security is virtualization, in this method resources are automatically assigned to users on demand. Virtualization allows users to run any operating system needed, also it allows simultaneous execution of operating system and applications in one physical machine. The best proposed method in cloud computing privacy is increasing cryptography, in this method for initial encryption of data algebraic structures will be used. It allows processing of encrypted end data according to initial encrypted data for making changes on unprocessed data. For sharing encrypted data, without having initial decryption, re-encryption will be performed. This re-encrypted data will be used only by legal users using authentication methods. The main focus of the paper is combining these two methods to have better security and privacy in cloud computing.

## 6. REFRENCE

[1] Sdral sadaty, Mohsen MJ "security challenges in cloud computing and provide a solution to improve the security at the National Conference on Computer Engineering and sustainable development with a focus on computer networks, modeling and security," the development of public services, e-government system What, Mashhad, Institute for Higher education Question: 1392

[2] Weichao Wang, Zhiwei Li, "Secure and Efficient Access to Outsourced Data", CCSW'09, November 13, 2009, Chicago, Illinois, USA, 2009.

[3] ME. Ethan "a procedure for privacy in cloud computing" extra-regional conference on new developments in science, engineering, Branch, Institute for Higher Education posterity: 2014.

[4] Ganji Hamida "provide a new method for privacy in the cloud environment by using data mining" First National Conference on Innovation in Computer Engineering and Information Technology, Branch, Institute for Higher Education aurora: 2014.

[5] Borse K, Deshpande A, Hardas J "SECURITY IN MULTI-CLOUD DATA STORAGE WITH SIC ARCHITECTURE", IJRET International Journal of Research in 71 Engineering and Technology, 3(2), 81-84, 2014.

[6] Parveen S and Suganya C R "Information Security through Normalization in Cloud Computing", International Journal of Scientific and Research Publication, 2(5), 2012.

[7] Sagar T, Sagar U and Ashok J, "Improved 3-Dimensional Security in Cloud Computing" IJCTT International Journal of Computer Trends and Technology, 9(5), 2014.

[8] Gowhar FZ, Ghadirli H, Dindarloo R “Increasing Data Security Using Virtualization” Second Iranian Sotfware Engineering Conference, 2013.