Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 363-369, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.ssps.205

Achieving Secure Data Access in Cloud Computing

[1]*P. Umaeswari and* [2]*B. Shanthini*

[1]Department of CSE, St. Peter's University, India
[2]Department of IT, St.Peter's College of Engineering and Technology, India

Abstract: Cloud computing conveys everything as a service over the web on user demand, like network, storage, hardware, software and resources. Benefits of cloud storage are easy access of the data to one's knowledge anyplace, anyhow, anytime and scalability. So each and every organization is moving its data to the cloud, it uses the secure storage service provided by the cloud provider. There is a need to protect the data against unauthorized access, therefore the need to use authentication. Secure the data in cloud means store it safely, authenticate and access easily. In cloud computing various security algorithms are used to store the data in a secure and safe manner. Various methods and different techniques are used to authenticate and to access the data comfortably. This paper explains about the cloud security algorithms, Authentication methods and Accessing techniques.

Key words: Cloud · Security · Authentication · Access

INTRODUCTION

Cloud computing is solution for providing computing service via the internet on demand and pay per use, access to a pool of shared resources namely networks, storage, servers, services and applications. So it saves managing cost and time for organizations. The flexibility of cloud computing provides industries, such as banking, healthcare and education. The cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources which provide processing power used, transactions carried out, bandwidth consumed, data transformation, or storage space consumption etc. Cloud computing is a completely internet dependent technology where client data is stored and maintained in the data center of a cloud provider like Google, Amazon and Microsoft etc [1].

Cloud computing is a model for producing benefits to the user, on-demand network services to a shared pool of configurable computing resources like networks, servers, storage, applications and services that can be rapidly provisioned and released with minimum amount of management effort or service provider interaction through internet [2]. Cloud computing is useful to provide scalable, security, privacy and inexpensive on-demand computing infrastructures with good quality of web-based service levels [3].

Types of Cloud Computing: The business software solutions and data are stored on servers at a remote location and can access anywhere at any time. Cloud computing remove the costs and communicating complexity, configuring and managing the hardware and software which is needed to build and deploy applications. These applications are released as a service over the cloud [4]. There are four types of clouds that are available:

Public Cloud: Multiple enterprises can subscribe on the infrastructure provided, at the same time [3].

Private Cloud: Cloud infrastructure is made available only to a specific customer and managed by the organization itself which provide more secure [3].

Community Cloud: Infrastructure is shared by several organizations for a shared resource that cause and may be managed by them [3].

Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. They include the mixture of private, public or community [3].

Corresponding Author: P. Umaeswari, Department of CSE, St. Peter's University, India.

Services Provided by Cloud Computing: The architecture of Cloud computing can be categorized according to the three types of delivery models, namely Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS). In cloud computing, everything is delivered as a Service.

Infrastructure as A Service (IaaS): It is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee.

Software as A Service (SaaS): It also operates on the virtualized and pay-per-use costing model. The software has limited functionality and its core pack can be expanded and contracted allowing easy customization which is billed accordingly.

Platform as A Service (PaaS): It is a service where cloud layer works like IaaS but it provides an additional level of "rented" functionality. The virtual machines act as a catalyst in the PaaS layer in Cloud computing [5].

Cloud computing is a web-based computer technology in which the data has to be stored and accessed in a secured manner.

Security Algorithms: Security algorithms produce the greater security and confidentiality in cloud computing atmosphere. The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography.

Symmetric-Key Algorithms: Symmetric-key algorithms are using the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [6].

Data Encryption Standard (DES) Algorithm: Secret key cryptography involves the use of only one key which is used for both encryption and decryption. The DES algorithm implements a more effective and flexible distributed verification scheme to address the data storage security issue in cloud computing [6]. Even though the algorithm have strengthened the key size and powerful great security algorithms, it is hard to communicate in the public/private cloud. Presently, all the data communications are move around to cloud based computing. In that case, a private/public cloud can generate the key in a secure manner using this methodology [7].

Blowfish Algorithm: There are various risks associated with the security. The major issue is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. The encryption way of block cipher algorithm like Blowfish for providing solutions to cloud security. Blowfish is a symmetric block cipher encryption algorithm which uses the same secret key to both encrypt and decrypt messages and divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It is suitable for cloud applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches [8].

Reverse Caesar Cipher (RCC) Algorithm: The main problem associated with cloud computing is data privacy, security etc. The new level of data security solution with encryption using ASCII full characters is the idea of Reverse Caesar Cipher (RCC) Algorithm. The scope of the algorithm to solve the security issues in both cloud providers and cloud consumers. The main drawback in the earliest Ceaser Cipher method is that the plaintext and key used only 26 alphabets. To overcome the above problem plaintext is used which case sensitive and allows numbers and special characters in order of ASCII full characters (256 char). This method which is the inverse of Caesar Cipher supports more security for the data compared with the earliest Caesar Cipher. And also it can be used simply to encode the message for preserving privacy. It is complicated to understand the cipher text compared with the other encoding and decoding methods [9].

Asymmetric-Key Algorithms: A type of encryption where the different key is used to encrypt and decrypt the message is called asymmetric algorithm. The encryption algorithms support compliance, protect the user against breach incidents and secure information against advanced threats. There are a lot of security algorithms which are implemented in the cloud [10].

RSA Algorithm: The RSA algorithm architecture provides a mechanism that used to get secure communication as well as hiding the information from unauthorized users. RSA encryption algorithm for to maintain confidentiality of data [11]. RSA consists of public-key and private-key. In Cloud environment the Public-Key is known to all whereas private-key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only [12].

Message Digest 5 Algorithm: Message digest functions which are also called as hash functions, used to generate Digital Signature of the information which is known as message digest.

MD5algorithm is used to implement integrity of the message which producem message digest of size 128 bits. Message digest algorithm has two advantages. Identical messages always generate the same message digest. If one of the bits of the message changes, then it provide different message digest. The next advantage is that message digests are much shorter than the document from which digests are generated. The usage of MD5 algorithm model highly secure for both sender and receiver [12].

Homomorphic Encryption Algorithm: The basic concept of the algorithm is to encrypt the data before send it to the Cloud provider. But it needs to decrypt data at every operation. The client will need to provide the private key to the server (Cloud provider) to decrypt data before execute the calculations required, which might affect the confidentiality and privacy of data stored in the Cloud. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data [13].

A user sends a request to add the numbers 1 and 2, which are encrypted to become the numbers 33 and 54, respectively. The server in the cloud processes the sum as 87, which is downloaded from the cloud and decrypted to the final answer, 3. Fig. 1 shows a string concatenation example of Homomorphic Encryption [14].

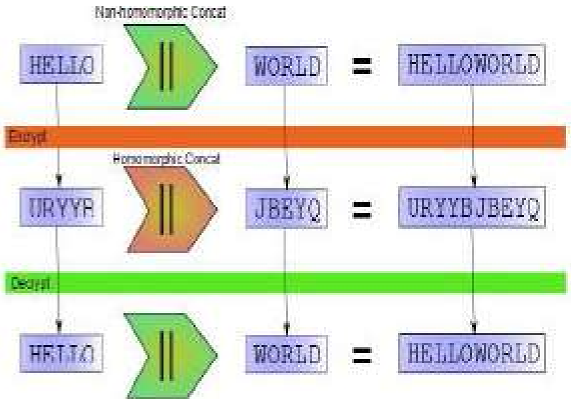

Fig. 1: A string concatenation example of homomorphic encryption

Attribute Based Encryption (ABE) Algorithm: Attribute-Based Encryption (ABE) is a new mechanism for the kind of access control policy in a cryptographic way. It is intended for one-to many encryption in which ciphertexts are not necessarily encrypted to one particular user. ABE provides normal encryption and extra access control function. The advantage of ABE is more efficient, flexible and suitable than other cryptographic techniques [15]. The complexity of encryption and decryption linearly increases with the enhance number of attributes which are desired for large systems, the challenge to make system collusion resistant need to be handled efficiently [16]. There are two kinds of ABE schemes, Key Policy ABE (KP-ABE), Ciphertext Policy ABE (CP-ABE) schemes explained as follows.

Key Policy Attribute Based Encryption (KP-ABE) Algorithm: By decrypting the access structure an attribute key will be generated which will also be a secret key and will be different for each user based on access to different attributes. In this system even if the users collude the attribute key will be different for each authority of access structure providing two levels of security. This scheme is suitable for structured association with rules about who may read particular documents [16].

Cipher Text Policy Attribute Based Encryption (CP-ABE) Algorithm: CP-ABE access structure used for computation of ciphertext and user's private keys deal with a set of the attributes. In CP-ABE scheme the user's private key is computed using attributes assigned to the user. This scheme also used sum of the ASCII values of each character of every attribute. So the user's private key is a number which is easy to remember. So it has overcome the limitation of the complex key size of the existing systems [17].

Customers will need to have a way to access their resources that are located within the cloud. It is important to manage the resources in a secure manner. So everybody require authentication.

Authentication: In Cloud security, authentication is the very important factor. Authentication is generally referred to as a mechanism that establishes the validity of the claimed identity of the individual. There are basically four kinds of authentication methods:

- Something an individual KNOWS (password, Personal ID)
- Something an individual POSSESSES (a token or card)
- Something an individual IS (fingerprint or voice pattern)
- Something an individual DOES (history of Internet usage)

Recently many security researchers are focusing on various new techniques of authentication in cloud computing that include one or more of the above mentioned methods of authentication [18]. Authentication is a process by which a method verifies and validates the character of a user of the system who wishes to access it [19].

Multi-Factor User Authentication in Cloud Computing: Multi-factor authentication (MFA) is an approach to authentication which requires the production of two or more of the three independent authentication factors like Knowledge factor *(something only the user knows)*, Possession factor (*something only the user has)* and Inherence factor (*something only the user is)*. Cloud provides open interoperation across (proprietary) cloud solutions at IaaS, PaaS and SaaS levels, manages multi-tenancy at large scale and in heterogeneous environments with dynamic and seamless elasticity from in-house clouds to public clouds for unusual (scale, complexity) and/or infrequent requirements. The explosive growth of cloud computing has made the provision of adequate and effective security challenges. Multi- factor user Authentication is an effective technique for preventing unauthorized access [19].

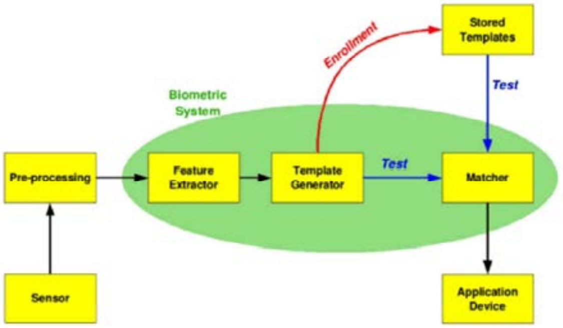

Fig. 2: Basic block diagram for biometric system

Biometrics: Biometric systems allow identification of individuals based on behavioral or physiological characteristics. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. These characteristics are unique and slow intrusive. Biometric systems can be used in two different modes.

Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. Identification (also called search) occurs when the identity of the user is unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all.

The fig.2 shows the above specified identification and verification process. Two types of biometric methods are:

- Physical biometrics: Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Finger print, hand geometry and facial recognition are leading physiological biometrics.
- Behavioral biometrics: Behavioral biometrics is based on measurements and data derived from an action and indirectly measure characteristics of the human body, Voice recognition, keystroke-scan and signature-scan are leading behavioral biometric technologies [20].

Face Recognition: The human face plays an important role in our social communication network. Facial recognition is one of the preferred methods of biometrics because it is a neutral, non-intrusive, easy-to-use, which requires minimal physical contact as compared with other biometrics systems. Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips and chin or on the overall analysis of the face image that represent a face as a number of recognized faces. Face image can be captured from a distance without touching the person being identified and the identification does not require interacting with the person. Face Recognition System (FRS) enables only authorized users to access data from cloud server. There are several advantages as stated, Non-intrusive, Unique, Cheap Technology, Fast Identification and Contactless Authentication [21].

One Time Password: The password is used to keep the user account secure and secret from the unauthorized user. Whenever a user login to the system, user will be provided with a new password for using it in the next login. This is usually provided by the system itself. This password will be generated randomly. Each time a new password is created for a user, the previous password for that user will be erased from the system. New password will be updated for that particular user. A single password will be used for login only once. The password will be sent to the users authorized mail account. Therefore at the same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account will be able to connect to the cloud system [22].

Email ID: It involves authenticating users using registered Email in the cloud computing. The user sends request to subscribe for specific services in the cloud. The cloud system sends to the user registration form with condition terms, one of the most important condition terms is the Email of the user, which is compulsory. It acts as the ID of the user where the link of authorized service may send to it and accessed by the user mail itself. The user submits the form. The cloud system capture the details filled in the form that the user has chosen during registration process. In order to make approval for it, cloud then returns information of successful registration. By using this authorization method, only the registered user with exact Emil ID may authorize to access the requested service by using user Mail-ID as an additional form authentication and authorization [23].

The advantage of cloud computing reduces the cost of hardware and software. Instead of buying the whole infrastructure required to access the data using the internet network communication and save bulk of data into the required system. So user needs accessing techniques.

Accessing Techniques: Even though there are lots of accessing and searching techniques available, they are not giving efficient search results. For example the search results returns 40 records and in those 30 records are relevant and the remaining 10 records result contain irrelevant data. To achieve effective data access, that is a need to focus on searching methods which will improve the efficiency of searching. Both keyword search and concept based search methods are used in order to retrieve the relevance search criteria. This method will retrieve the documents based on broader conceptual entities, which will improve the efficiency of data retrieval [24].

Ranked Keyword Search Algorithm: In Cloud Computing, data owners may allocate their outsourced data with a large number of users, who might want to only retrieve certain specific data files. One of the most popular ways to do so is through keyword-based search. Such type of keyword search technique allows users to selectively retrieve files of interest.

Ranked keyword search method produces best result for achieving effective utilization method to access data which was remotely stored and encrypted in Cloud Computing. A search engine mainly works using crawling, indexing, storage and ranking. Search engines are always working towards improving their technology to crawl the web more deeply and returns increasingly relevant results to users. Search engines have a short list of critical operations that allow them to provide the relevant web results when searchers use system to find information [25].

Multi Keyword Retrieval over Top-K Algorithm: The user can access the cloud data with appropriate encrypted cloud in a secure and efficient manner. Sensitive information is protected by data encryption at data owner side followed by verification of the received files. It employs Two Round Searchable Encryption Scheme (TRSE) that supports top-k Algorithm multi keyword retrieval and address security issue. Top-k Algorithm Multi-keyword ranked search retrieves data accurately when compared to single keyword search. The owner side encryption scheme and index file generation helps the data user to get secure and protected data with better quality, efficient and more secure. Multi-keyword ranked search retrieves data accurately when compared to single keyword search [26].

Multi Related Keyword Based on Clustering Technology: An efficient clustering technique is used to retrieve encrypted cloud data for multiple related keywords. Inclusion of clustering technique to group related keywords together retrieves efficient and accurate cloud data. The system ranks cloud data based on end user feedback on top of existing ranking algorithms which simply relies on keyword occurrence in a document and enhance the accuracy of data retrieved. It is always advisable and it makes sense to get user feedback. The search result as the user manually reads the document 'rates' the document based on the accuracy of retrieval for the given multiple related keyword. The system displays Not relevant, Relevant, Most relevant 'radio buttons' and make easy the user to rate the documents retrieved for the particular keywords [27].

CONCLUSION

For the protective privacy of the deposited data, proper encryption is needed before uploading to the cloud. In this paper, we discussed the different cryptographic algorithms to store the data in a secure manner. For authentication of authorize user one can use in cloud computing are Password, face recognition, Biometrics, One Time Password, Email Id etc. After authentication the cloud based data will access by many more retrieval algorithms and search process is as per requirements of the user query are used.

REFERENCES

1. Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy, 2011. "Cloud Computing: Security Issues and Research Challenges", International Journal of Computer Science and Information Technology and Security (IJCSITS) Vol., 1(2): 136-146.
2. Gnanavelu, D. and G. Gunasekaran, 2014. "A survey on cloud computing data storage security issues", International Journal of Computer Technology and Applications, ISSN: 2229-6093, Vol., 5(2): 389-392.
3. Abhinay B. Angadi, Akshata B. Angadi, Karuna C. Gull, 2013. "Security Issues with Possible Solutions in Cloud Computing-A Survey ", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Vol., 2(2): 652-661.
4. Ashalatha, R., 2012. "A survey on security as a challenge in cloud computing", International Journal of Advanced Technology and Engineering Research, National Conference on Emerging Trends in Technology, Vol., 2(4): 1-4.
5. Ramgovind, S. M.M. Eloff, E. Smith, 2010. "The Management of Security in Cloud Computing", IEEE,.
6. Rashmi Nigoti, Manoj Jhuria and Shailendra Singh, 2013. A Survey of Cryptographic Algorithms for Cloud Computing, International Journal of Emerging Technologies in Computational and Applied Sciences, ISSN:2279-0055, pp: 141-146.
7. Govinda, K., E. Sathiyamoorthy and Surbhit Agarwal, 2013. Secure Key Exchange for Cloud Environment Using Cellular Automata with Triple-DES and Error-Detection", International Journal of Engineering and Technology, ISSN: 0975-4024 Vol., 5(2): 1004-1009.
8. Leena Khanna and Anant Jaiswal, 2013. "International Journal of Advanced Research in Computer Science and Software Engineering", ISSN: 2277-128X, Vol., 3(3): 279-283.
9. Padmapriya, A. and P. Subhasri, 2013. "Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT), Volume, 4(4): 1067-1071.
10. Madhubala, P. and P. Thangaraj, 2014. "Comprehensive and Comparative Analysis of Cryptographic Solutions in Cloud", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol., 2(10).
11. Sonal Guleria and Sonia Vatta, 2013. "To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm", International Journal of Application or Innovation in Engineering and Management, ISSN, Volume, 2(6): 2319-4847.

12. Sudhansu Ranjan Lenka and Biswaranjan Nayak, 2014. “Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm”, International Journal of Computer Science Trends and Technology, Vol., 2(3): 60-64.
13. Maha TEBAA and Said EL HAJII, 2013. “Secure Cloud Computing through Homomorphic Encryption”, International Journal of Advancements in Computing Technology, Vol., 5(16): 29-38.
14. Shashank Bajpai and Padmija Srivastava, 2014 “A Fully Homomorphic Encryption Implementation on Cloud Computing”, International Journal of Information and Computation Technology, ISSN, 0974-2239, Vol.,4(8): 811-816.
15. .Phyo Thandar Thant, 2012. ”Security of Cloud Service Provisioning using Attribute Based Encryption”, International Journal of Emerging Trends and Technology in Computer Science, ISSN, 2278-6856, Vol., 1(1): 96-100.
16. Pooja, K. Patil and P.M. Pawar, 2013. “Security Of PHR Model On Public Cloud Using Multi Authority And Key Policy Attribute Based Encryption”, International Journal Of Computer Applications, ISSN: 0975-8887, Vol., 84(12): 46-52.
17. Rewadkar, D.N. and V.S. Dhumal, 2014. “Hierarchical CP-ABE Scheme Implementation on Amazon EC2 cloud” International Journal of Science and Research, ISSN (Online): 2319-7064, Vol., 3(7): 712-715.
18. Ziyad, S. and S. Rehman, 2014. ”Critical Review of Authentication Mechanisms in Cloud Computing”, International Journal of Computer Science Issues, Vol. 11, Issue 3, No. 1, ISSN (Print): 1694-0814, ISSN (Online): 1694-0784, pp: 145-149.
19. Deepa Panse and P. Haritha, 2014. “Multi-Factor Authentication in Cloud Computing for Data Storage Security”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277- 128X, Vol., 4(8): 629-634.
20. Himabindu Vallabhu and R.V. Satyanarayana, 2012. “Biometric Authentication as a Service on Cloud: Novel Solution”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol., 2(4):163-165.
21. Akshay A. Pawle, Vrushsen P. Pawar, 2013. “Face Recognition System (FRS) on Cloud Computing for User Authentication”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol., 3(4): 189-192.
22. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque and A. Hashem. M.M., 2012. “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, International Journal of Advanced Computer Science and Applications, Vol., 3(10): 181-186.
23. Abdelmajid Hassan Mansour Emam, 2013. “Additional Authentication and Authorization using Registered Email-ID for Cloud Computing”, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol., 3(2): 110-113,.
24. Kiruthigapriya Sengoden and Swaraj Paul, 2013. “Improving the Efficiency of Ranked keyword Search over Cloud Data”, International Journal of Advanced Research in Computer Engineering and Technology, ISSN: 2278-1323, Vol., 2(3): 881-883.
25. Ramya Majeti, Mahalakshmi Tejaswi Palvadi, P. Venkata Naresh and S. Satyanarayana, 2013. ”Ranked Keyword Search in Cloud Computing”, International Journal of Computer Trends and Technology, ISSN: 2231-2803, volume, 4(4): 508-510.
26. Suman, M. Chempavathy, 2014. “An Approach for Efficient and Secure Retrieval of Encrypted Cloud Data Based On Top-K Multikey words”, International Journal of Computer Science and Information Technologies, ISSN:0975-9646, Vol., 5(3): 3239-3241.
27. Jayasree V. and M. Nithya and S. Prabaharan, 2013. ”Cloud Data Retrieval for Multi Related Keyword Based on Clustering Technology”, International Journal of Communication and Computer Technologies, ISSN: 2278-9723, Vol., 1(4): 85-91.