IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA SECURITY TECHNIQUE IN CLOUD COMPUTING

Garima Anand
MGM's College of Engineering & Technology, Noida

DOI: 10.5281/zenodo.1402460

ABSTRACT

Cloud computing is the delivery of computing services over the Internet. The platform of cloud computing gives peoples the opportunity of sharing and storing resources and information among the people across the globe. Most of organizations, individual and end users are making use of such online storage services to store their important information for the backup purpose. This new paradigm brings about many new security challenges. At present ensuring security in cloud computing platform has become one of the most significant concerns for the researchers. Many any new frameworks and technologies are used to preserve data that are stored in clouds. In this paper, a new data security scheme is developed for cloud computing platform. This scheme ensures data security in both the ways i.e., data storage security and data retrieval security. For data retrieval security, multi-level authorization technique is applied. Authenticity of user is done in 3 levels which includes registered key, one-time password (OTP) and image-based security mechanism. For data storage security, data partitioning is done along with the application of serialization concept. Both data retrieval security and data storage security provide a strong foundation that not only restricts the unauthorized user to access the data stored in cloud but also ensures the confidentiality and integrity of data.

Keywords: Cloud computing, Security challenges, Multi-level authorization, Data partitioning, Serialization.

I. INRTODUCTION

In the recent years, cloud computing has grown from a business concept to one of the fastest emerging sector in It industry to a basic need for people across the world. Cloud computing is everywhere. More and more people are, now days, depending on it. Cloud is the biggest buzz in the world of computers these days. The concept "cloud computing" is one of the most developing and evolving concept in the history of technological advancement. It provides resources, services and utilities to the user and stores their crucial data and information to make their life easier in this busy and hectic world. Due to cloud computing, we can utilize deployable and scalable resources within the confines of Internet. It uses system's hardware and software as computing requirement and provides services through the internet. Despite all these capabilities and potential advantages achieved from cloud computing, many organizations are still reluctant in adopting it due to the security and privacy issues associated with it. These issues hamper the growth of cloud computing. At present scenario, important data and documents are the only thing without which your life comes to a standstill and loosing such important data is no more than a horror experience! So, here the need of security and privacy of user's data rises. In cloud computing environment, all data or files of an individual stored in cloud are open to all. Thus, these data or file becomes more prone to attack. As a result, an intruder can easily access, misuse and destroy the data. The need of security becomes so vulnerable that now people and even though organizations look for security that cloud provider provides before they look for cloud services. There should be a strong security mechanism used by cloud service provider. The security mechanism should be strong enough to handle the basic concept of security i.e., integrity, confidentiality and authenticity. Any security mechanism covers these concept guarantees the security and privacy of user's data. Integrity ensures that the content of the data is not disturbed or changed by any intruder at all and originality of data is confirmed. Confidentiality ensures that the file or data is confidential and cannot be accessed by any unauthorized person. Only the authorized user can access or use it. Authenticity ensures that the person requesting for access is the one whom he claims to be and does not have any false identity. The users with false identity might act as an intruder. In this research paper, new security technique for cloud computing platform is proposed. Here, security is applied on both the sections i.e., while retrieving or accessing data from cloud called as data retrieval security and while storing data in cloud called as data storage security. It makes this security architecture stronger than ever. This proposed technique strictly follows the integrity and confidentiality of stored data as well as authenticity of users accessing cloud. Multi-

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

level authorization is applied for data retrieval security which checks user's authenticity at each level and allows only authorized users to enter the cloud. Data partitioning scheme is applied along with serialization for data storage security. This ensures integrity and confidentiality of user's data stored in cloud. Serialization makes completely impossible for anyone to read or change the contents of file and it also work as memory management process for managing data in cloud data centers.

II. SECURITY CHALLENGES IN CLOUD COMPUTING

Numerous issues or challenges pertaining to the security and privacy aspects of cloud computing have been observed. Such security challenges played the most important role in hindering the acceptance of cloud computing. Users are often concerned and suspicious about the security of their private and confidential data. It is primarily because of their concern that who else might have access their data. Thus, security is linked with the concepts of integrity, confidentiality, authenticity and availability. All these concepts should be carefully examined to overcome various security challenges and issues. In cloud computing, security should be such that it prohibits unauthorized access and eliminate the possibilities of data corruption to establish trust of peoples on the cloud services. Another major concern associated with the security is the verification of untrusted servers and service providers. It is vital for the users or customers to obtain guarantee on the service delivery from cloud service providers. The cloud service provider, who also experiences certain failures occasionally, may try to hide the data errors from customers for the benefit of their own and the more serious parts is that these service providers might neglect or deliberately delete user's rarely accessed data to increase the memory space and add up more customers in cloud. Cloud is facing such challenges because this paradigm is continuously evolving or expanding, and it lacks set of standards. Thus, maintaining, organizing and controlling cloud has become a herculean task. Also, cloud has a very complex architecture. It becomes quite impossible for the service providers to guarantee their services and claims about their servers as 100% working all the time and often leads to the breach of data security. All these security challenges are overcome with the security technique proposed in this paper.

III. PROPOSED TECHNIQUE

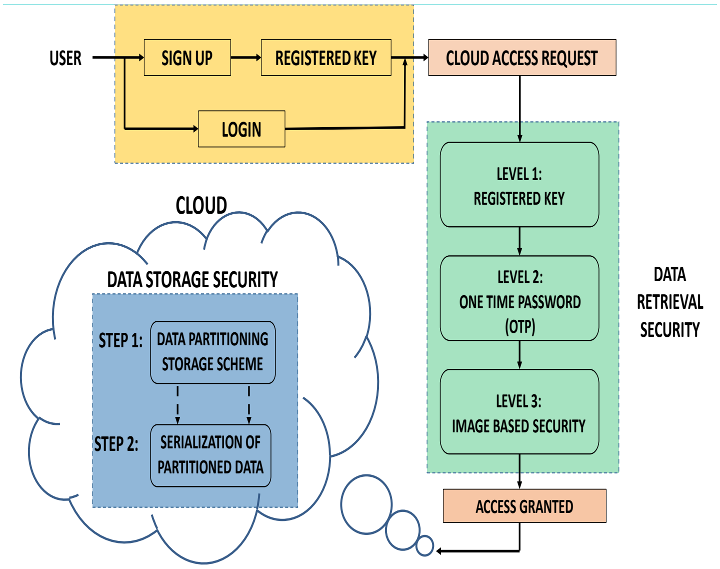

Fig 1: Data securitytechnique architecture

To improve the data security in cloud and eliminate cloud security issues and challenges, new security technique is proposed which covers all the aspects of security such as confidentiality, integrity, availability, authenticity and focuses on both the areas of data flow in cloud i.e., retrieval and storage.

A. End user

End user stores his important and confidential data in cloud and accesses that data according to his requirement. User can also perform various activities like sharing information and resources, perform work on his stored data, send files or media to another user. For performing all such tasks, user first needs to survive the security applied in this technique. All the users, irrespective of new or existing, must surpass the authentication levels before entering the cloud. The security applied on user's stored data is data partitioning and serialization. Existing user starts directly from the login section whereas new user must complete the registration process first i.e., signup section. As soon as user gets a unique registered key, registration process completes. Every user must clear all these security levels to enter the cloud. If any user fails at any of the 3 security levels, then he cannot reach further.

B. Data retrieval security

For data retrieval security, a multi-level authorization is applied. First security level i.e., level 1 authorization is based on registered key. Registered key is a unique key which user receives after the completion of registration process. This registered key will automatically send to the user's email address as well as database. Registered key will remain same every time that user passes through the first-level authorization. When registered key entered by user matches with the one stored in database, user enters the next level. Second security level i.e., level 2 authorization is based on one-time password (OTP). As soon as user clears the level 1 authorization, OTP is generated and send to the user's phone number and the database. If the OTP entered by user matches the one stored in database, then user enters the third level. Third security level i.e., level 3 authorization is image-based security. In this, an image is displayed to the user which is divided into sections. Each section has some meaning in the form of number which is not visible to the user. User clicks on those sections randomly and generate a password. This password will be accepted by user during the signup process. During signup process, when user saves this password, a 3-digit number is added in front of that password and stored in the database so that as many passwords can be generated. This 3-digit number, when attached, will be displayed to the user. Now, during 3rd level security, same image is displayed to the user and 3-digit number is written in the text field. User enters the password by clicking on the image (sections) displayed. Similarly, this password is matched from the one stored in database. If result is same, then access to the cloud is granted otherwise not.

C. One time password (otp) generator

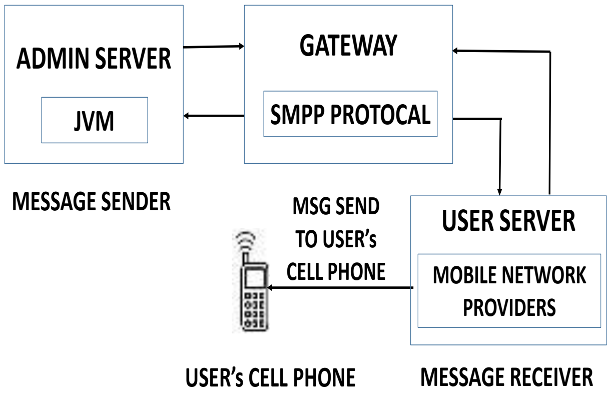

Fig 2: One time password (OTP) framework

OTP is an authentication procedure used in this technique for secure retrieval or access to the data on cloud. The basic requirements for generating OTP are 2 servers i.e., admin server and user server, JVM install on admin server, a gateway for interfacing and a cell phone device. For interfacing between the 2 servers, a gateway is used which provides SMPP protocol. SMPP protocol is a flexible data communication interface for sending short messages. Admin itself should be the user of gateway being used and sends messages to cloud user using this gateway. For sending SMS, first information regarding the SMS such as phone number of user and message is taken by JVM from admin server to the gateway. It then verifies that the admin server which sends this information is its registered user or not. If this is verified than gateway creates an instance of SMPP protocol for that user to JVM at the admin server. For each user, an instance of SMPP is created and each time same instance is used for sending messages to the same user. When a new user is added a new instance of SMPP protocol is created for that user. Now, JVM inserts that information to the instance and send that instance to user server using gateway. User server on receiving that instance checks if the gateway is a client of that mobile network provider. If the client is verified, then user server sends the SMS to user's cell phone. Thus, OTP received to the users also gets stored in database.

D. Data storage security

For data storage security, the basic question that arises in our mind is how data is being manipulated and managed in cloud data centers? How data integrity and privacy is achieved? And is the technique used is space and time effective? The answer to these questions explains a lot about cloud storage security being used and how efficiently user's data are being taken care of. The technique mentioned in this research paper is simple, unique, and gives optimized answer to the above questions. A data partitioning scheme is applied along with the concept of serialization-deserialization for storage security in this paper. Here, when a user stores a file in cloud then the whole file gets partitioned into several smaller parts depending upon that file. Now, the content of each partitioned part is separately converted into a non-readable format i.e., into a byte stream using serialization and stored at random locations predefined by admin in the cloud data centers. When user retrieve or download that file, partitioned parts are fetched from the cloud data centers and the non-readable content of each part is converted into original content separately by using deserialization. Now these parts are joined together according to the sequence of partitioning and displayed to the user. The complete log of user's data and location of partitioned parts are maintained at the admin server.

E. Partitioning of data in clouds

In data partitioning, a file that user uploads in cloud is split into number of smaller parts to store data effectively and in quick manner as files having smaller sizes are easy to handle and store. These partitioned files are then serialized i.e., converted into a non-readable format and store randomly at the locations allocated by the admin in cloud data centers.

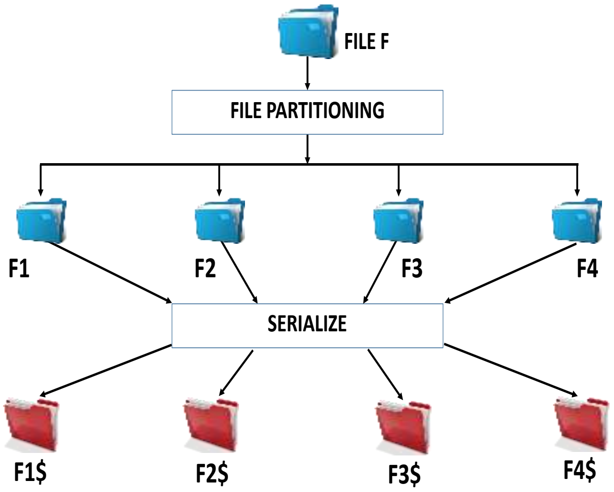

Fig 3: File uploading process

Algorithm1: file partitioning

1. Load the input file.
2. If input file is a text file
3. Then, read number of lines.
4. Break the file after every fixed no of lines.
5. If input file is an image
6. Then, file is split in terms of rows and columns.

7. Break the image after every fixed no of row and columns.
8. If input file is an audio or a video
9. Then, file is split in terms of time.
10. Break the files after every fixed no of seconds.
11. Partitioned files are then serialized separately.
12. Then store these files at random locations as predefined by admin.

If user downloads the stored data, all the partitioned files are fetched from cloud data centers and then get deserialize i.e., converted into readable format (original content). These files are then joined together according to the index number and original file is generated.

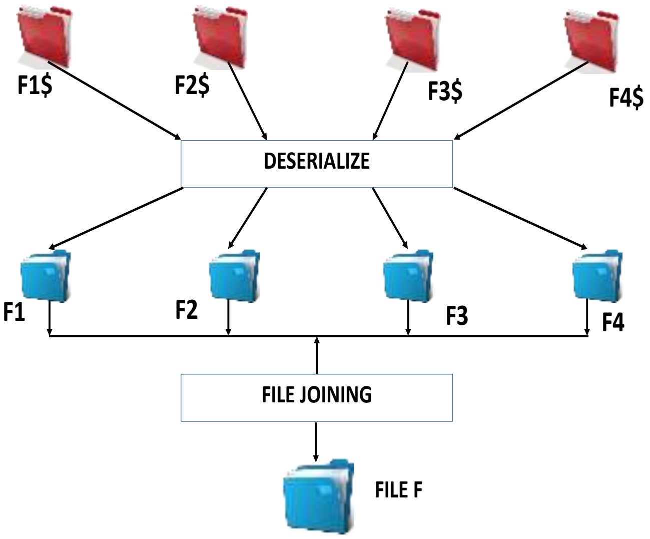

Fig 4: File downloading process

```
Algorithm2: file joining
1. Input the file name.
2. Extract files based on
   a) file name in step 1,
   b) index no,
   c) .ser extension.
3. Deserialize each file separately.
4. Join the file according to index no.
5. File is ready to use.
```

F. Serialization-deserialization of data contents

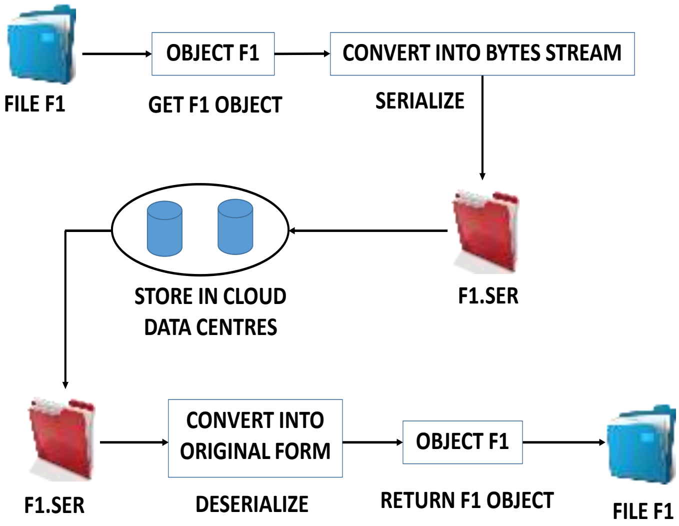

Fig 5: Serialization-deserialization process

This serialization-deserialization plays a crucial role in data storage part of this technique. Serialization performs a very high degree of storage space reduction as it converts the content of file into a compressed manner and then stores it. Thus, we do not require much space to store serialize files. For serializing, files are first stored in a string constant pool as their temporary location. Then these files are picked up one by one from pool, file object is taken from each file and serialize it. These serialized files are then stored in cloud data centers. When the file is retrieved, deserialization is done. It converts the byte stream content into original, readable content and returns the file object.

G. Admin's role in this security technique

Admin has a vital role in managing user's data and activities on cloud. He is fully aware of data that is being stored on clouds with respect to the users and the number of partitions of a file has been created and location of these partitions on cloud data centers. A complete log of data storage as well as user operations such as addition, deletion, and modification of stored data is maintained at admin server. Admin will even have the knowledge of which stored data has been accessed by which user at what duration of time. Most importantly, admin will not have any read or write access rights regarding any of the stored data. He can only check the file name and their storage locations in data center but cannot sees its content to ensure security. Another important role that admin performs in this security mechanism is that if any user in the cloud is acting maliciously and performs risky behavior and might cause harm to the user's data then admin can remove that user from the cloud immediately and all the data stored by that userin cloud will be deleted. Thus, admin too ensures security of data in clouds and plays a major role in data management.

IV. PERFORMANCE ANALYSIS

Performance analysis is the measurement that gives the exact idea about the performance of this technique in terms of storage space (memory) and time. For storage space measurement, space complexity is calculated whereas for time measurement, time complexity is calculated. Space and time complexity of this technique, calculated for worst case, comes out to be O(n) which is a linear space and time complexity and the cyclomatic complexity of this technique is 7 which means that the technique implementation is efficient, not complex and without any risk. The result of performance analysis ensures that implementing this technique leads to high storage space and time reduction.

V. CONCLUSIONS

In this research paper, a simple, unique and efficient technique of data security in cloud computing platform is proposed. This technique consists of two areas i.e., data retrieval security and data storage security. Data retrieval security ensures high degree of authentication and authorization of users. It enables to verify the identity of the user i.e., user requesting for access is the one whom he claims to be and does not have any fake identity. Multi-level authorization provides a strong framework which strictly restricts the entry of unauthorized users in the cloud. All the three levels are systematically organized one after the other. Data storage security focuses on integrity and confidentiality of data stored in clouds. The data partitioning technique enables storing of the data in easy and effective manner. Data storage technique also works as a memory management process due to the use of serialization concept. Serialization stores data in a very compressed manner. Thus, memory is utilized effectively. The space and time is effectively reduced during data storage. This complete data security technique is cost effective in every manner.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving PublicAuditing for Storage Security in Cloud Computing,” Proc. IEEEINFOCOM, Mar. 2010.

[2] C. Wang, K. Ren, W. Lou, and J. Li, “Towards Publicly AuditableSecure Cloud Data Storage Services,” IEEE Network Magazine, vol.24, no. 4, pp. 19-24, July/Aug. 2010.

[3] Takabi. H, Joshi.J.B.D and Ahn.G, "Security and Privacy Challengesin Cloud Computing Environments," Security & Privacy, IEEE,vol.8, no.6, pp.24-31, Nov.-Dec. 2010.

[4] Paredes, L.N.G.; Zorzo, S.D.;, "Privacy Mechanism for Applicationsin Cloud Computing," Latin America Transactions, IEEE (RevistaIEEE America Latina) , vol.10, no.1, pp.1402-1407, Jan. 2012.

[5] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans.Computers, preprint, 2012.

[6] Wang Cong, Wang Qian, Ren Kui, Cao Ning and Lou Wenjing ,"Toward Secure and Dependable Storage Services in CloudComputing," Services Computing, IEEE Transactions on , vol.5,no.2, pp.220-232, April-June 2012.

[7] Hsiao-Ying Lin; Tzeng, W.-G.; , "A Secure Erasure Code-BasedCloud Storage System with Secure Data Forwarding," Parallel andDistributed Systems, IEEE Transactions on , vol.23, no.6, pp.995-1003, June 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data StorageSecurity in Cloud Computing,” Proc. 17th Int’l Workshop Quality ofService (IWQoS ’09), pp. 1-9, July 2009.

[9] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha,” PDDS -Improving Cloud Data Storage SecurityUsingDataPartitioningTechnique” 3rdIEEE International Advance Computing Conference(IACC),2013.

[10] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the PublicCloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[11] John Harauz, Lori M. Kaufman, Bruce Potter, “data Security in the World of Cloud Computing”, The IEEE Computer SOCIETIES, August, 2009

[12] IEEE - The Application of Cloud Computing in Education Informatization, Modern Educational Tech... center Bo Wang, HongYu Xing.

[13] Neil M.Haller, “THE S/KEY ONE-TIME PASSWORD SYSTEM”, 1993

[14] Neil Haller, “A One-Time Password System”, October 23, 1995

[15] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, “Security Issues for cloud computing”, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[16] Mladen A. Vouk, “Cloud Computing – Issues, Research and Implementations”, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. “On Technical Security Issues in Cloud Computing” In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.

[18] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. “What’s Inside the Cloud? An Architectural Map of the Cloud Landscape.” *IEEEExplore*, pp 23-31, Jun. 2009.

CITE AN ARTICLE

Anand, G. (2018). DATA SECURITY TECHNIQUE IN CLOUD COMPUTING. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(8), 538-544.