Proposed Technique for Securing Critical Data Over Cloud

Amit Wadhwa
Assistant Professor
Department of Computer Science and Engineering
Amity University Haryana, India

Abstract: Cloud computing has emerged as a new computing platform where users are able to use services provided by cloud service providers on basis of pay per use model. The services can vary from using infrastructure and platform or software as a service. From the origination of Cloud Computing technology, the major concern for the users is to secure their data being stored over cloud storage servers. Although there are different cryptographic algorithms being implemented over cloud to secure user's data but still there are instances of unauthorized intrusions emerging over cloud platform. To tackle the situation of securing user's cloud based data or files a new approach is being proposed here in this paper. Further, this paper also focuses on securing cloud based data from malicious insider attacks with the help of the proposed technique.

Keywords **– Cloud Computing, Data Security, Sensitive Data Protection**

I. INTRODUCTION

From the advent of cloud computing the security of data is of major concern to its adopters or users. Users using the cloud for various types of features always are in dilemma for using cloud or not as their data or files are always available to third party administrators.

The concern of the cloud users is about storage space provision and its associated privacy or security of data available over cloud. Storage data over a cloud often tempt the malicious attackers to attack such system with vulnerabilities. They attack by making unauthorized access to cloud storage, accessing confidential data leading to financial damages for organizations and even harm their goodwill as an enterprise in market. This ultimately affects their customer base and trust among them.

This situation requires the CSP's (i.e. Cloud Service Providers) providing solutions so that these type of situations and vulnerabilities can be prevented. There are providers in market like Dropbox which uses encryption algorithms like AES to secure their customers data [1]. But to make this situation work trust should be established among data owners cloud providers. Apart from this the location to store data files is not provisioned to be specified by CSU (i.e. Cloud Service User). So, the foremost considered solution to be adopted for data protection in this type of scenario is encrypting confidential data files and uploading them to cloud storage servers [1].

Problem arising out of this situation is related to data sharing among CSU's. Data sharing is one of the most common operation among cloud users associated with an organization. So, If the data stored over cloud is encrypted then sharing it might also requires sharing of decryption keys [1], which ultimately pretends as a security threat. It might also lead to depleting bandwidth for other associated operations.

Organization of paper-it begins with introduction about the problem of data security over third party storage server. Next section discusses the literature related to previously adopted security algorithms presented and adopted by researchers over the years. Further, a proposed technique to be adopted for securing the data files stored over cloud storage server is being presented. It includes the new algorithm proposed to be adopted for securing critical cloud user files. Finally, it provides the feasibility for adoption of the proposed technique over cloud platform and its associated benefits. In the end, conclusion and future directions are provided for the presented work followed by references.

II. LITERATURE WORK

Data security over cloud has been a huge challenge to be handled by CSP's providing various types of cloud platform based services. Earlier, till now most of the researchers have proposed or presented different ways of protecting user data over cloud using various cryptographic techniques. Apart from these other algorithms or techniques used are access control protection based or authentication oriented algorithms. For access control the algorithms or models proposed are like Discretionary access control [12] model, mandatory access control model and role based or attribute based access control models etc. Some of the above-mentioned algorithms or techniques presented by researchers over the years are discussed here.

In year 2010, U. Somani et. al. [2] proposed a solution to enhance the security of data providing solutions to problems of ensuring CIA in a cloud platform. To provide the necessary solution, the techniques of digital signature with encryption [2] are proposed to be used. The technique used is found to be effective to certain extent and useful for cloud environment.

Further in the year 2013, N. Jose, et. al. [3] proposed a data security enhancement model for cloud platform which composes of multi-layer security model. In first layer OTP based user authentication is employed, followed by data encryption at layer second providing integrity and user protection. Last layer comprises of a mechanism for fast data recovery using byzantine fault tolerant algorithm [3]. The was found to be providing fine grained data access with private user key distribution and encrypted files for data protection and integrity verification.

Later in year 2014, R. Kaur, et. al. [4] proposed a novel model for providing security over cloud using different encryption algorithms along with scheme for integrity verification. The system works based on division of three different security sections [4] like public, private and mixed (i.e. hybrid). Different encryption techniques are being employed providing CIA along with authentication based security and non-repudiation. Private section employs a specific token generation technique ensuring user authenticity. Fast encryption and decryption is employed in public area whereas mixed section provides on demand security level. Different sections provide specific level of security using alternate algorithms. Implementation of the system is simulated using cloud analyst simulator and found effective.

V. K. Pant, et. al. [5] in year 2015, also proposed a model providing 3 step model enabling data security of cloud based data. Three steps are employed in a way like using cryptography with RSA algorithm as first line of defense, further at second level steganography technique [5] was implemented hiding our data within the image and at third level data from image is being fetched and further decrypted with initially used RSA technique. The proposed and implemented method works not only for hiding using images but also for hiding using audio and even video files.

D. Singh, et. al. [6] in 2016, proposed a solution to override from security concerns of Privacy, Authentication and Integrity. They proposed a model or framework for protection of data Confidentiality and Integrity over cloud. They proposed for thin clients like mobiles or PDA's, using AES and SHA1 algorithms with node to node key agreement protocol. Proposed system was designed to overcome or handle attacks like man in the middle, non-repudiation and identity spoofing. The scheme proposed was found to be effective as it reduces computation power required and computation time is also reduced.

Later in 2016, N. R. Patil, et. al. [7] also proposed a secure cloud based architecture for mapping security issues like secure user authentication and CIA with privacy. OTP method has been proposed to be adopted for secure user authentication, with SHA2 being adopted for data integrity check and AES for securing data stored over third party storage server. The proposed system requires the user to login using OTP method followed by encryption using AES. The proposed system was supposed to overcome pre-image and collision attacks.

A. Wadhwa, et. al. [8] in year 2014 also discussed a technique or framework for securing data and files over cloud using technique of cryptography combined with digital signature. They discussed that for hashing they require use of SHA1 algorithm and further the hashed file is encrypted with AES encryption-decryption algorithm to provide extended security to data files.

Later in year 2017, they also provided the theoretical analysis of the earlier proposed framework and compared it with other such or similar algorithms - using any of the selected encryption decryption algorithms [9] or some access control and authentication mechanisms adopted to provide extended security to cloud based data. For the analysis part a weighted summation of different algorithms or frameworks is presented after selecting various properties for analyzing the frameworks. After complete analysis of all the selected models the proposed framework [9] was found to be effective based on the security and other features associated for drawing the analysis.

Later in year 2018, they further provided the implementation and simulated analysis of above theoretically analyzed technique or framework using cloud sim simulator. The analysis of the simulated framework reveals the impact of implementing digital signature (using SHA1) and encryption-decryption (using AES) on the access time and performance of the system. The model was further analyzed based on total execution time [10] for the process with and without using AES with SHA1 [10]. The model also incorporates an algorithm having provision for selecting the associated extension of files to be replaced with randomly selected one from given list of extensions.

The discussed literature above shows that almost all algorithms proposed over the years have been using the technique of cryptography (i.e. encryption-decryption) or a combination of it with digital signature[11] for security of data over cloud. Along with this very few of them are focused towards protection of critical data files [13], [14] to be stored over cloud storage servers. So, here in our work the focus will be on proposing a technique or algorithm suitable for providing protection to critical data files to be stored over cloud storage servers. The next section is focused towards the above illustrated requirement.

III. PROPOSED TECHNIQUE

As can be seen from the literature work part discussed in previous section, most of the security models or frameworks provides security to data adopting cryptography techniques of encryption and decryption. Over the years the security to stored cloud data has become a major point of concern for new adopters of cloud computing environment. Considering this aspect of cloud based security a new and novel technique is presented here for securing data stored over cloud storage.

Proposed idea: Providing security to data to be stored over cloud storage corresponding to a user can be achieved using a method to change extension of a file with a randomly selected combination of three or four sequence of characters interpreted as new extension for the given file. New combination should not be same as original extension.

Along with it, the requirement is that it should not be matching with other similar type of extensions which could reflect the data present in it by simply looking at the contents of data file.

The step by step procedure for the proposed technique is as shown in Figure 1:

void Extension Inverting Algorithm (String Filename)
Step 1: Receive the original data file to be stored over cloud storage from requesting user.
Step 2: Separate the extension of the file from the complete filename and store it.
Step 3: Call Random Extension Generator Algorithm with stored original extension and file name as input.
Step 4: Receive and store the Randomly Generated extension value returned from step 3, which must not be matching with any value from the initial common category of extensions and original file extension.
Step 5: Attach the new stored extension with the original file name and save the file in cloud storage of the respective user.
Step 6: Also keep a record of the filename with original and new extension, required to be used when the authorized user requests the required file from his/her account with CSP.

Figure 1 Extension Changing Algorithm

Steps for the Random Extension Generator Algorithm are as shown in Figure 2:

String Random Extension Generator Algorithm (String Filename, String orgExt)
Step 1: Select a flag and set it to false, initialize a 1-d array containing all available English language characters from 'a' to 'z'.
Step 2: initialize an array containing list of common categories of extensions to be ignored while selecting the desired extension.
Step 3: Iterate over loop and generate a specific length of three or four character long string acting as new extension value for the file to be stored.
Step 4: If the new extension is found different from common category and original extension received initially, then return the extension to calling function else goto step 3.

Figure 2 Random Extension Generator Algorithm

Proposed technique of securing critical CSU's data is presented here using algorithms given in Figure 1 and 2 respectively. As per the extension changing algorithm it requires the original file as input, which is used to extract the original extension from its filename. Then that extracted extension value is fed as input along with original file details to the next algorithm i.e. Random Extension Generator Algorithm as shown in Figure 2 here.

This algorithm works by taking input as Filename and original extracted extension value. The algorithm uses an array of characters to consider and randomly generate the new extension to be compared with extensions from common category and original extracted extension. If new generated extension doesn't match with any of the compared extensions then it is returned to the calling function otherwise the process for searching a new extension continues.

Along with this, if the data file to be stored over cloud storage area is encrypted before or after using the above listed algorithms, it leads to extended security for data files.

For every user accessing his/her stored data files over cloud storage, the only way to access his files is through his/her registered account with CSP, whose login security is maintained with some secure access control mechanism. This makes the file un-usable for the attacker or malicious insider directly fetching it from cloud storage server by simulating an attack.

IV. CONCLUSION AND FUTURE DIRECTIONS

Cloud computing security is an ever-growing domain where many new techniques for securing user data or service access are being developed and presented by researchers on a regular basis. Still there is always a scope for new algorithms or techniques to be presented for adoption over cloud architecture. In view of it a new approach, algorithm or technique is presented here which if used along with encryption would make unauthorized access to it much more difficult for the attacker or malicious insider. So, the proposed technique as provided in the previous section if implemented is expected to provide a different way towards storing and securing cloud based data files rather than just implementing or using alternate techniques of encryption-decryption. In future, the implementation of it could be simulated to further justify its usage and implications.

REFERENCES

[1] D. M. Polson, S. Sabitha and R. M. S, "Fine Grained Key Computation Scheme for Secure Data Sharing in Cloud," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, 2016.

[2] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in *First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, Solan, 2010.

[3] N. Jose and C. K. A, "Data Security Model Enhancement In Cloud Environment," *IOSR Journal of Computer Engineering*, vol. 10, no. 2, pp. 01-06, 2013.

[4] R. Kaur and R. P. Singh, "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques," in *International Conference on Advances in Computing,Communications and Informatics (ICACCI)*, Greater Noida, 2014.

[5] V. K. Pant, J. Prakash and A. Asthana, "Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques," in *International Conference on Green Computing and Internet of Things (ICGCloT)*, Bangalore, 2015.

[6] D. Singh and H. K. Verma, "A new framework for cloud storage confidentiality to ensure information security," in *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, 2016.

[7] N. R. Patil and R. Dharmik, "Secured cloud architecture for cloud service provider," in *World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, 2016.

[8] A. Wadhwa and V. K. Gupta, "Framework for User Authenticity and Access Control Security over a Cloud," *International Journal on Computer Science and Engineering*, vol. 06, no. 04, pp. 138-141, 2014.

[9] A. Wadhwa and V. K. Gupta, "Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud," *International Journal of Applied Engineering Research*, pp. 15715-15722, 2017.

[10] A. Wadhwa and V. K Gupta, "Practical Implementation and Analysis of MLBAAC Model for Cloud," International Journal of Computer Engineering & Technology, 9(3), 2018, pp. 14–22

[11] C.-C. Chang and Y.-F. Chang, "Signing a digital signature without using one-way hash functions and message redundancy schemes," *IEEE Communications Letters*, pp. 485-487, 2004.

[12] M. Auxilia and K. Raja, "Dynamic Access Control Model for Cloud Computing," in *Sixth International Conference on Advanced Computing (ICoAC)*, Chennai, 2014.

[13] A. Wadhwa, "Comprehensive Analysis of Security Issues and Solutions While Migrating to Cloud Environment," *International Journal of New Innovations in Engineering and Technology*, vol. 4, no. 4, pp. 127-130, 2016.

[14] D. H. Patil, R. R. Bhavsar and A. S. Thorve, "Data Security over Cloud," *IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT2012)*, pp. 11-14, 2012.