MACHINE LEARNING ASSISTED CLOUD STORAGE IN MULTI-CLOUD PLATFORMS FOR DATA OFFLOADING PROCESS

V. Divya

Department of Information Technology, Vivekanandha College of Engineering for Women, India

Abstract

In recent years, abstract cloud computing has become critical, and the security issues associated with the cloud paradigm are increasing. In order to audit the risks associated with cloud protection, the current networks use an independent authentication mechanism or personal search. In order to perform this report, the data holders must be online. This article explores a new approach for personal auditing that is enabled by one time password (OTP). The records can be protected against the user of theft using this OTP generation/creation technique. The machine learning algorithm Reverse Data Encryption Standard supports the owner to download the file. The files are converted and stored in separate cloud instances into smaller computers. For better protection in various circumstances the files as well as the content will be encrypted and saved in the cloud server. This authentication method will prevent the error user from hacking at the cloud end. The OTP is created and propelled to the user when the download takes place. This OTP must be used to search the user before the appropriate files are downloaded.

Keywords:

Cloud Computing, Security Issues, Secret key, Machine learning

1. INTRODUCTION

The information technology is imagined as an integral part of cloud computing. The systemic architecture lists exceptional compensation in the IT history such as self-services on-demand, omnipresent network connectivity, and autonomous reserve pooling positions, quick supply availability, use-based pricing charges and threat transfer [1]. Cloud Computing converts the very essence of the way companies employ information technology [4] [5] as a struggling machinery with reflective suggestions. One of the basic aspects of this transition is the centralization of or outsourcing of data records into the cloud [2] [3]. From the point of view of consumers and IT efforts, it is useful to gather data in a soft on-demand mode from a distance to the cloud, release database loading, widespread data access separate from the position and escape resources from hardware, applications and servicing by employees [6] [7]. Cloud storage makes these benefits more interesting than yet, but before customers are outsourced [8] it still brings fresh and challenging security risks. Data outsourcing simply waives the user's eventual right-of-way over their data's fortune [9]. First, while the technology below a cloud is much more efficient and secure than personal computing systems, both domestically and peripherally they face a wide variety of data reliability risks [10].

In the absence of data owners, an auditing method that resolves the issue of regeneration of failed authenticators starts a substitution for the traditional public audit scheme which is beneficial for restoring the authenticators. A modern public authenticator that can be demonstrated and restored by a series of keys using fractional keys. This scheme will then free data owners completely from online problems [11]. Safe and efficient cloud computing storage facilities. Risks to the consistency of data in the cloud. A stable, efficient cloud storage provider [12] has a problem with data error position in order to focus on this new task, hence only given the binary impact on storage authentication. We are researching the challenge of data security in the cloud data management which is essentially a distributed storage system. This dilemma, if not properly handled, will impede the cloud architecture design to work victoriously.

The crisis of data protecting solitude is not completely deciphered but only reduced to the one of the organisation. Illegal outflow of data is also a problem because the encryption key's future experience [13]. The audit findings should not only consider data accuracy, but should also be smart to assume that the agency is responsible for the problem [14]. In this method it is not optimally sparse and direct over a random linear coding to shorten the correspondence, storage and measurement values. The major advantage of decentralised erasure codes is that harmonisation between data nodes is not necessary [15]. We display random and different data nodes, and can generate excellent, sparse erasure codes. Randomized network algorithm and the Wiedemann algorithm. The main problem is open, such that it is not likely to be achieved with a marginal computation and connectivity in this vigorous dispersed storage. The key scheme designed to help third parties' audits should allow users to safely assign activities to Third-Party Auditors (TPA) without worrying that cloud storage will be used. TPA should be able to easily track the cloud data storage without needing local data copies and does not place additional cloud user's on-line burden.

Public Third Party (TPA) regeneration-code-based cloud auditing process. We are initiating a surgery, which is helpful to regenerate authenticators, in the common public audit replica in order to overcome the renewal problems of botched authenticators in the absence of data holders. A new public proved authenticator built with a pair of keys and partial keys can be regenerated. The data owners will then be absolutely rescued from the online saddle by this method. Furthermore, the random coefficients of the programme may be randomised to protect information security. A thorough safety review shows the verifiable secure of the current design by the random oracle paradigm and a timely evaluation, which specifies that the scheme proposed is highly competent and can be plausibly implemented in the resurrected cloud storage facilities of code-based design. Therefore, the data security principle cryptographic mechanisms cannot explicitly be managed by the user; verification of precise data storage in the cloud must be achieved without explicit knowledge of the full data. Considering the various forms of data for each customer stored in the cloud and their requirement for long-term data protection, it becomes much harder to verify data storage consistency in the cloud. It's not just a data warehouse for third parties. Clients will rationalise the data processed in the cloud regularly.

- *Security*: The built model preserves the safety and integrity of stored information against vendors and unauthorised end users of cloud services. Only endorsed users should read the stored data and no effort to retrieve them should be allowed or noticeable.
- *Data Protection*: the rights of access and use of a single end-user should not be discernible to all users
- *Flexibility*: The user is allowed to access the information after a verification process; user details are shown here such as photo, name, mobile number, location, city etc. The credential search process is valid and is performed through personal audits.

2. PROPOSED METHODOLOGY

An effective personal audit for consumers based on OTP has been proposed. It will deter users of theft. The file can be assigned to smaller units using an R-DES algorithm and packed in a number of cloud storage systems and accessible via cloud services. Here we used upload encryption and download file decryption. The study proposed a cloud storage auditing scheme that displays personal audit rights of the owner. Data are created and hosted by the owners in the cloud.

2.1 ARCHITECTURAL DESIGN DESCRIPTION

We provide a user-friendly GUI for the device in our security structure. As data owner and data user, it has a twofold function. You are the owner of the file when transferring files, and whenever you explore another file, you are the data recipient. Users may build their profiles and the page consists of the information of users, for which they have different pages. This allows only approved users using an authentication process to use the new system.

First of all, after the file has been uploaded, the OTP (secret key) will be defined as the preliminary stage when the file is uploaded. This key is taken as a file credit. The OTP (secret key) is designed to be used to import and upload processes. The OTP of that file will be created after the owner's authentication if the user wants to download and if he gives the download order. To track your credentials, the created OTP will be sent to the administrator, which will prevent the entry of erroneous users.

File upload is only available after the owner's approval has been reviewed. The author obtained separate OTPs (Secret Keys) to the corresponding mail identification when he set his username information on the cloud to make sure that the authorised owner's upload was finished.

Initially the user gets an OTP (secret key) in the email identity of the customer for the upload and download process. Then the encrypted server data then decrypts the hidden key to retrieve the necessary data from the server storage device.

The OTP (secret key) to the respective user's mail id must be retrieved and then file data can be decrypted with the use of this file.

The R-DES decryption mainly looks like an encryption method, and it follows as follows: the ciphertext input in the R-DES algorithm. The R-DES algorithm requires the exact calculations form to be accepted on the code and the encrypted result to be obtained when the decrypted result correlates to the result of plaintext operations. The data is encoded in the cloud until it is propelled, the operations on the encrypted information are completed and the results are decrypted, the operations on the initial data are similar. This cryptosystem provides anonymity and security. In cryptography, the plaintext currently comprises one method and the cypher text still has an identical role.

An algorithm is symmetrical as it is made to measure, deduct and spread. We use multiplication when encrypting data in the proposed process. The following steps consist of this algorithm: key processing, encryption and decryption. This algorithm and file converted into tiny units and packed in various cloud storage systems encrypts the data owner's files and claves. It may be specified how many times the files must be encrypted. The Cloud service provider will inquire whether the data owner wants his file to be retrieved. Without understanding something, the Cloud Service Provider would do calculations with the encrypted info. The data owner is supported by the results. The encryption algorithms play a very important role in maintaining safe communication across the network. It is the fundamental mechanism for data security. The encryption algorithm converts the data to scratched form with a key, and the recipient has a key for decrypting the data.

The Personal Audit (PA) is responsible for validating an account and for assigning user role keys. The hidden code key for the secure protocol connecting PA and data warehouse is created when the users are able to access the attributes. They use the arithmetic protected protocol for their own master secret keys and provide a customer with unassignable key pieces. The use of the main components obtained separately from the authorities will provoke the entire hidden key.

The protected protocol prohibits them from learning the master secrets of each other so that nobody can invoke all the user's private keys. The datacenter recognises the revocation list in this environment and does not contravene the protection criteria, since cypher text may only be re-encrypted and no functionality can be given concerning the user's attribute keys. As certain concepts in our construction, such as access tree, encryption and decryption algorithms are recaptured on the proposed scheme.

Besides protection, time complexity can be minimised. Security analysis with personal audit architecture complies with authentication, data reliability and confidentiality protection requirements which follow directly from the use of traditional cryptographer primeval, message authentication code and encryption in our system. Errant users will only be refused if they are willing to send a special picture of the trustworthy authority that they recognise (TA).

PA conducts a specialised audit method for cloud storage as mentioned below; it usually includes the owner and the cloud server (server). The owners save the data and transfer it to the cloud servers. The cloud servers manage the owners data and access the users with data (data consumers).

The auditor is a trustworthy entity with experience and the ability to supply all proprietors and cloud servers with data storage audit tests. The auditor should be a trusted government-run entity that can give shared data owners and cloud servers unbiased audit reports.

3. RESULTS

This section illustrates the output information obtained from the proposed model. The Fig.1 and Fig.2 display time and time of decryption measurements as well as analyses of results.

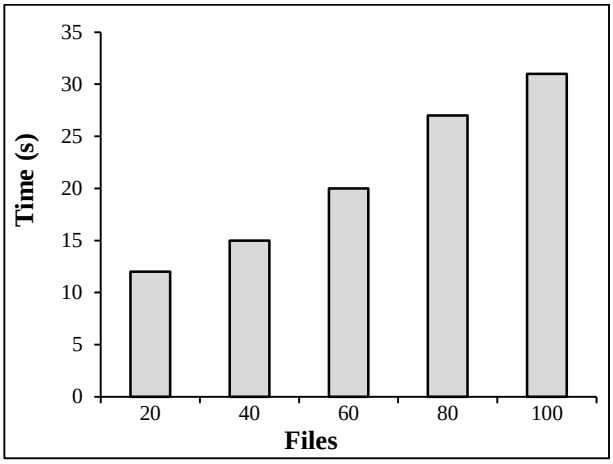

Fig.1. Encryption Time

The x-axis is the number of documents which were encrypted to be preserved in the cloud in Fig.4. The y-axis is the time needed for encryption. There are 20, 5s encrypted documents with 40 encrypted documents at 12s period. The time used for encryption is 20 seconds until it exceeds 60 files. The model also took 27 and 31 seconds to encrypt 80 and 100 files.

The owner uses the reverse method of the DES encryption algorithm (R-DES), until the OTP is retrieved and the cypher text is forwarded to the owner. R-DES decryption for the retrieval of the server's original plaintext. The recipient is then safely obtaining the proposed files.

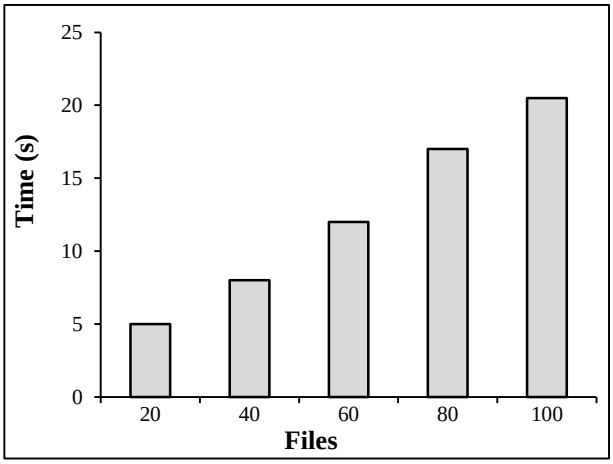

Fig.2. Decryption Time

The output is seen in Fig.5, which shows the x-axis to the amount of encrypted files, and the y-axis to the time in seconds. Initially, in 5 seconds, 20 records were downloaded. Decryption is performed on the time of 8, 12, 17 and 20.5s for 40, 60, 80 and 100 files. However, the decryption time is relatively short of the encryption time.

4. CONCLUSION

In this article, we suggested a personal auditing method for data protection in cloud computing that safeguards personal privacy. The personal audit focused on OTP deals with the protection of storage and time control. The customer is checked by a combination of protected parameter and hidden key by OTP based personal auditing. In this job, the distribution of the secret key is prevented by establishing its OTP validity. The hacking and exchanging of the mails are also significantly reduced by verifying the combination of the protected parameter and OTP. The time required for the results is analysed and compared to a third-party audit current model. In contrast with the current model, the innovating model used a lot less time to decrypt 20 data.

REFERENCES

[1] Suresh Chari, Josyula R. Rao and Pankaj Rohatgi, "Template Attacks", *Proceedings of International Workshop Cryptographic Hardware and Embedded Systems*, pp. 13-28, 2002.

[2] Xinjie Zhao, Fan Zhang, Shize Guo, Tao Wang, Zhijie Shi, Huiying Liu and Keke Ji, "MDASCA: An Enhanced Algebraic Side Channel Attack for Error Tolerance and New Leakage Model Exploitation", *Proceedings of International Workshop Constructive Side Channel Analysis and Secure Design*, pp. 231-248, 2012.

[3] Michael, M., Godfrey and Mohammad Zulkernine, "Preventing Cache-Based Side-Channel Attacks in a Cloud Environment", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 4, pp. 395-408, 2014.

[4] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren 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*, Vol. 24, No. 1, pp. 131-143, 2013.

[5] William Stallings, "*Network Security Essentials (Applications and Standards)*", Pearson Education, 2004.

[6] Jose J. Amador and Robert W. Green, "Symmetric-Key Block Ciphers for Image and Text Cryptography", *International Journal of Imaging System Technology*, Vol. 3, No. 2, pp. 43-49, 2005.

[7] Bruce Schneider, "*Applied Cryptography*", 2nd Edition, John Wiley and Sons, 1996.

[8] Nawal El-Fishawy and Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", *International Journal of Network Security*, Vol. 3, No. 2, pp. 1-14, 2007.

[9] R. Nivedhaa and J. Justus, "A Secure Erasure Cloud Storage System using Advanced Encryption Standard Algorithm and Proxy Re-Encryption", *Proceedings of International Conference on Communication and Signal Processing*, pp. 1-6, 2018.

[10] X. Song and Y. Wang, "Homomorphic Cloud Computing Scheme based on Hybrid Homomorphic Encryption", *Proceedings of International Conference on Computer and Communications*, pp. 13-16, 2017.

[11] A. Sude and V. Shinde, "Authenticated CRF Based Improved Ranked Multi-Keyword Search for Multi-Owner Model in Cloud Computing", *Proceedings of International Conference on Computing, Communication, Control and Automation*, pp. 1-5, 2017.

[12] M. Thangapandiyan, P.M. Anand and K.S. Sankaran, "Enhanced Cloud Security Implementation using Modified ECC Algorithm", *Proceedings of International Conference on Communication and Signal Processing*, pp. 12-17, 2018.

[13] D.R. Kumar Raja and S. Pushpa, "Diversifying Personalized Mobile Multimedia Application Recommendations through the Latent Dirichlet Allocation and Clustering Optimization", *Multimedia Tools and Applications*, Vol. 78, pp. 24047-24066, 2019.

[14] K. El Makkaoui, A. Beni-Hssane and A. Ezzati, "Can Hybrid Homomorphic Encryption Schemes be Practical?", *Proceedings of International Conference on Multimedia Computing and Systems*, pp. 1-7, 2016.

[15] A. Yun, J.H. Cheon and Y. Kim, "On Homomorphic Signatures for Network Coding", *IEEE Transactions on Computers*, Vol. 59, No. 9, pp. 1295-1296, 2010.