A THREE-LAYER PRIVACY PRESERVING CLOUD STORAGE SCHEME BASED ON COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING

[1]IFROZE JAHAN, [2]Dr. Gulab singh chauhan
[1]mtech, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H. Tno:20S41D5811, ifrozejahan@gmail.com
[2]Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, gulsinchu@gmail.com

ABSTRACT: Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In order to solve this problem, we propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.

Keywords *– Cloud computing, cloud storage, fog computing, privacy protection.*

1. INTRODUCTION

Since the 21st century, computer technology has developed rapidly. Cloud computing, an emerging technology, was first proposed in SES 2006 (Search Engine Strategies 2006) by San Jose and defined by NIST (National Institute of Standards and Technology) [1]. Since it was proposed, cloud computing has attracted great attention from different sectors of society. Cloud computing has gradually matured through so many people's efforts [2]. Then there are some cloud-based technologies deriving from cloud computing. Cloud storage is an important part of them. With the rapid development of network bandwidth, the volume of user's data is rising geometrically [3]. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. Pursuing more powerful storage capacity, a growing number of users select cloud storage. Storing data on a public cloud server is a trend in the future and the cloud storage technology will become widespread in a few years. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately [4], [5]. Nowadays there are a lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications, which in turn leads to their success in attracting humorous subscribers.

Copyright @ 2022 Author

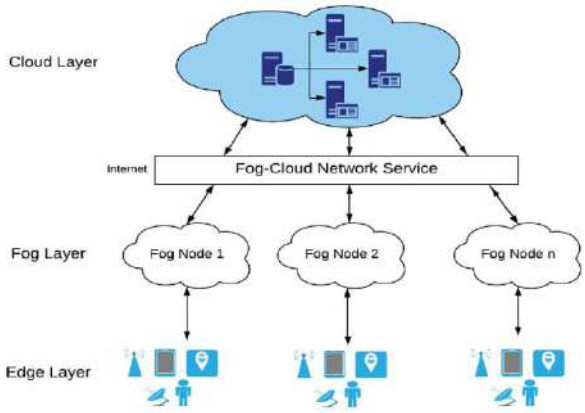

Fig.1: Example figure

However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. For example, Apples iCloud leakage event in 2014, numerous Hollywood actresses private photos stored in the clouds were stolen. This event caused an uproar, which was responsible for the users' anxiety about the privacy of their data stored in cloud server.

2. LITERATURE REVIEW

Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments

User provisioning options are greatly enhanced by cloud computing, with cloud providers offering a variety of reservation and on-demand buying options. As a result of the need to choose a reservation plan ahead of time, it must be suitable for the users' needs. Reservation plans may not be sufficient if demand is unknown, thus additional resources must be made available to meet demand on-demand. As a result of previous research, virtual machines were placed optimally with cloud providers in order to decrease total cost. Many apps, on the other hand, require a considerable quantity of bandwidth on the network. Consideration of merely virtual machines, thus, provides a partial picture of the system. Making use of SDN's recent advances, we present an integrated solution to virtual machine and network capacity provisioning that merges both. Due to uncertainty in the demand for virtual machines and network bandwidth, we solve a stochastic integer programming problem in order to attain the optimal provisioning of both. Numbers demonstrate that our strategy minimises user expenses and outperforms other methods. For cloud computing to enable network-intensive applications, we feel that this integrated strategy is the way to go forward.

Computational intelligence in wireless sensor networks

WLANs are a network of dispersed autonomous devices that can sense and monitor physical and environmental factors in concert. As a result of communication problems, storage and computing limits as well as limited power supply, WSNs confront various hurdles. Computing intelligence (CI) paradigms have been effectively used to a variety of problems in recent years including data aggregation and fusion, energy aware routing, task scheduling and security. When applied to complex and dynamic contexts, such as wireless sensor networks (WSNs), CI provides adaptive mechanisms that demonstrate intelligent behaviour. In addition, CI provides flexibility, autonomy, and robustness to topology changes, communication failures, and scenario modifications. WSN developers, on the other hand, are frequently unaware of the potential that CI algorithms offer or are only partially aware of it. WSNs pose a unique set of challenges that CI researchers are not accustomed with. This mismatch makes it tough to collaborate and develop. These gaps will be bridged in this paper, which provides a full overview of WSNs and their attributes in order to encourage collaboration. As a result, the study presents an exhaustive assessment of CI applications to various difficulties in WSNs from a variety of research areas. A

comparison of CI algorithms with standard WSN solutions is also presented. There is also an evaluation of CI algorithms that can be used as a guide for utilising them in WSNs.

A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing
Content-based image retrieval (CBIR) has been extensively investigated due to the growing importance of images in people's daily lives. Images take up a lot more storage space than text documents, so it's important to keep that in mind. A common cloud storage outsourcing scenario, then, would be to outsource its upkeep. Sensitive photos, such as medical and personal images, must be encrypted before being outsourced, making CBIR technologies in plaintext domain unsuitable for privacy-preserving applications. Here, we describe how to implement CBIR over encrypted photos while not disclosing any sensitive data to the cloud server. Features are first retrieved from the photos. After that, the pre-filter tables are generated using a locality-sensitive hashing algorithm to boost the efficiency of the search process. And the feature vectors and picture pixels have been encrypted using an industry-standard stream cypher. Defensively, we offer a watermark-based technique to prevent unauthorised users from illegally copying and disseminating photographs obtained from authorised query users. Before photographs are provided to the query user, the cloud server embeds a unique watermark immediately into each encrypted image. By extracting the watermark from the copied image, the illegal query user who circulated it can be identified. Analyses of safety as well as testing reveal that the proposed technique is safe to use.

Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data
Cloud computing's searchable encryption is a hot topic for researchers. A few methods do exist, but they use keywords or basic semantic parsing, which aren't clever enough to suit the consumers' needs. Deshalb, in this study we present a search technique that takes into account the content to make semantic search more intelligent. Zunächst, conceptual graphs are introduced as a method for knowledge representation (Knowledge Representation). A second set of schemes (PRSCG-TF) is then presented based on distinct scenarios. The original CGs are converted to linear form and then mapped to numerical vectors in order to do numerical calculations. Zweitens rely on CGs to address the challenge of privacy-preserving smart semantic search based on multi-keyword ranked search over encrypted cloud data. We raise PRSCG and PRSCG-TF to tackle this problem. This is followed by the use of CNN data set to test our model. We also examine in depth the privacy and efficiency of the proposed methods. According to the experiment results, our recommended schemes are effective and cost-effective.

Toward efficient multikey word fuzzy search over encrypted outsourced data with accuracy improvement
An essential utility in cloud computing today is keyword-based search across encrypted outsourced data. Multi-keyword exact match or single keyword fuzzy searches make up the majority of the strategies now in use. However, these strategies have less practical use in real-world applications than the multi-keyword fuzzy search technique over encrypted data. For the first time, Wang et al. used locality-sensitive hashing methods and Bloom filtering to achieve the goal of fuzzy multi-keyword search A one-letter typo in a keyword, however, was all that Wang's system could handle. It was also prone to server out-of-order errors throughout the ranking process and did not take keyword weight into account. It is our goal in this study to provide an efficient multi-keyword fuzzy ranked search strategy that can address the aforementioned issues based on Wang and coworkers' method A new keyword transformation mechanism based on the uni-gram is being developed, which will improve accuracy while also allowing for the handling of other spelling problems. The stemming technique can also be used to find keywords with the same root. When finding a suitable matching file set, we also take into account the keyword weight. Experiments with real-world data have shown that our technique is both practical and accurate in real-world settings.

3. METHODOLOGY

In this case, the user uploads data directly to the cloud server. The Cloud Server Provider (CSP) will then administer the data instead of the user. Consequentially, users do not have direct control over where and how they store their data. The CSP has full access to the cloud-based data and can search it at will. In the meantime,

attackers can also target the CSP server in order to steal the user's information. Both of the foregoing scenarios expose users to the risk of information leakage and data loss, which is a serious concern for consumers.

Due to Seny and Kristin's fear that the service provider cannot be completely trusted, they create a virtual private storage service based on recently established cryptographic algorithms. Such a solution combines the security of a private cloud with the functionality and cost savings of a public cloud to provide the best of both worlds.

Because users no longer have direct access to the data they've outsourced, Wang et al. argue that cloud computing has a difficult time protecting data integrity.

Disadvantages:

- There are no good solutions to this problem, no matter how much the algorithm is improved.
- These encryptions make cloud search more challenging.
- A CSP that cannot be trusted makes all of these schemes ineffective, and vice versa

When it comes to internal attacks, they're helpless. As long as hostile attackers have access to user's private information, it will be decoded, regardless of how advanced the encryption technologies are.
On the basis of the fog computing concept, we suggest a TLS method that uses Hash-Solomon code instead of the Reed-Solomon code. Users' data is divided into three sections and stored separately on the cloud server, the fog server, and the user's local computer in our approach. It also ensures that partial data cannot be used to retrieve the original data based on Hash-Solomon code properties.

While a fraction of redundant data blocks will be produced by applying Hash-Solomon code during the decoding phase. This can boost storage dependability by increasing the number of redundant blocks, but it also results in more data storage.

Advantages:

- We can provide a higher level of privacy protection from the inside, notably from CSPs.
- We can secure user privacy by allocating data in a sensible manner. Complex calculations are required to create the Hash-Solomon code, which can be aided by computational intelligence (CI).

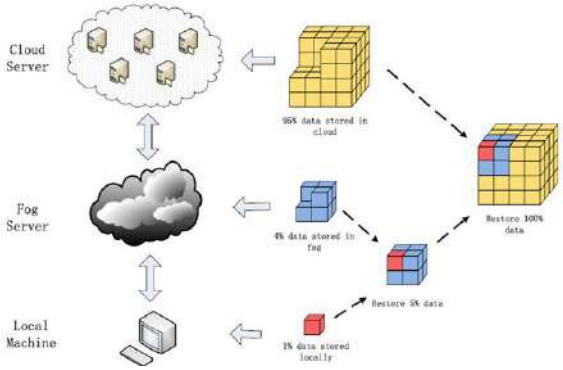

Fig.2: System architecture

Combining with the fog computing model, the three parts of data will be stored in the cloud server, the fog server and user’s local machine according to the order from large to small. By this method, the attacker cannot recover the user’s original data even if he gets all the data from a certain server. As for the CSP, they also cannot get any useful information without the data stored in the fog server and local machine because both of the fog server and local machine are controlled by users. As shown in Fig, the TLS framework makes full use of fog server’s storage and data processing capability. The architecture includes three layers, the cloud server, the fog server and the local machine. Each server saves a certain part of data, the storage proportion is determined by users’ allocation strategy. Firstly, user’s data will be encoded on user’s local machine. Then, for example, let 1% encoded data be stored in the machine. Then upload the remainder 99% data to the fog server. Secondly, on the fog server, we do

similar operations to the data whichcomes from user's machine. There will be about 4% data stored in the fog server and then upload the remainder data to the cloud server. The above operations are based on Hash-Solomon code.

4. IMPLEMENTATION

Constructing the System

First, we design a module called System Construction, which will analyse and implement the concept of Division and Replication of Data in Cloud (DROPS) in order to optimise performance and security. Users and Cloud entities are created to achieve this end goal. Update uploaded File blocks are available for users of the User entity.
There are two types of entities in our system model: cloud servers and users. Users who uploaded files to cloud servers are called "original users," whereas subsequent users are those who proved ownership of a file but did not upload it.
• The cloud entity first verifies that users are authenticated before granting access to their data. Users' data is stored in blocks in the cloud entity.
On the other hand, if n is the number of blocks and |b| is the number of challenged blocks, then our approach is asymptotically better than other schemes. Asymptotic performance of our system is superior to that of other schemes, save for one that simply provides a poor security guarantee, for example.

Fragmentation of the data:

In this subject, we'll learn how to create data fragments. In order to compromise a single file, you will need to penetrate only one node. To decrease the amount of compromised data, it is possible to create pieces of a data file, which are then stored on different nodes. Success in gaining access to a single or few nodes will only grant access to a small percentage (or even none at all).

The chances of an attacker finding fragments on all nodes are extremely low if he or she does not know where the fragments are located. Because of this, we fragment the data file and transfer it to the cloud so that no one can access it. An attacker's chances of gaining access to a large volume of data are greatly reduced with cloud-based computing systems. As a result, placing each fragment in the system more than once will result in a longer time for retrieving the data.
Fragments can be reproduced in a way that minimises retrieval time without increasing the aforementioned probability to enhance data retrieval time.

Centrality:

In a graph, a node's centrality is a proxy for its relative importance. Due to the goal of reducing retrieval time in replication, the centrality measurements become more essential.
For example, closeness, degree, betweenness, eccentricity, and Eigenvector centrality are some of the different metrics of how central something is. These three centralities are only discussed in detail because we will be relying on them in this study.

DROPS:

On the DROPS process, the file is fragmented and replicated in the cloud. So that even a successful attack on a node exposes no critical information, the fragments are spread so that each node in a cloud stores more than one fragment. Each fragment is duplicated only once in the cloud as part of the DROPS approach. Although controlled replication does not enhance retrieval speed to the extent of full-scale replication, it increases security in a considerable way. -
User transmits data file to cloud via DROPS approach. (a) fragmentation; (b) first cycle of node selection and storage of one piece of data per selected node; and (4) second cycle of node selection and fragment replication by the cloud manager system (which is a user-facing server in the cloud that responds to user requests). Assumed to be a secure entity, the cloud manager keeps track of the fragment placements.

5. EXPERIMENTAL RESULTS

Fig.3: Home screen

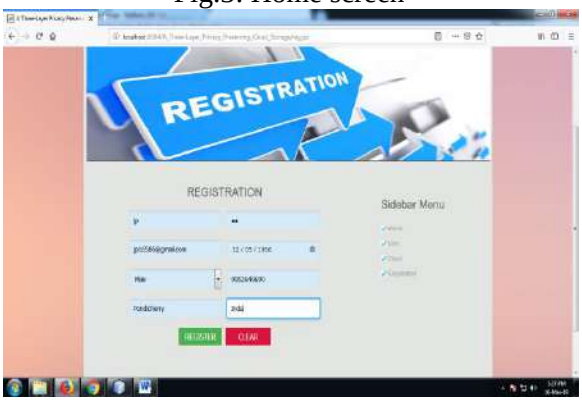

Fig.4: registration page

Fig.5: Cloud login

Fig.6: User screen

Fig.7: File upload

Fig.8: MAC code

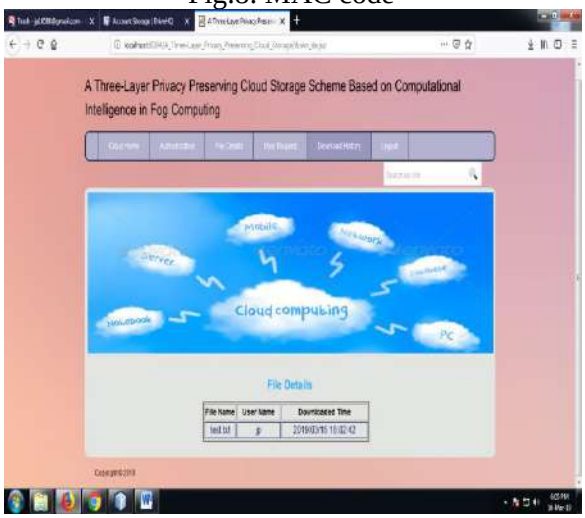

Fig.9: File details

6. CONCLUSION

We will gain many benefits as cloud computing continues to rise. Using a cloud storage service, clients may easily increase their storage capacity. Cloud storage does, however, have a number of security concerns. When consumers use cloud storage, the ownership and administration of data is split between the user and the cloud service provider. For cloud storage privacy, we've developed a Hash-Solomon algorithm and TLS framework based on the fog computing concept. A theoretical safety analysis has verified the scheme's practicality. On each server, we can protect privacy by distributing data blocks in an appropriate ratio. The encoding matrix, on the other hand, is theoretically impossible to crack. To protect fragmented data, hash transformations might be used. While testing cloud storage efficiency in the experiment, both the encoding and decoding processes were

successful. The Cauchy matrix is found to be more efficient in the coding process in order to achieve maximum efficiency.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *Nat.Inst. Stand. Technol.*, vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloudcomputing: Architecture, applications, and approaches," *Wireless Commun.Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtualmachine and bandwidth allocation in software defined network (sdn) andcloud computing environments," in *Proc. IEEE Int. Conf. Commun.*, 2014,pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving datastorage service in public cloud," *J. Comput. Res. Develop.*, vol. 51, no. 7,pp. 1397–1409, 2014.

[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collectionin sensor-cloud system with multiple mobile sinks," in *Proc. Adv. Serv.Comput., 10th Asia-Pac. Serv. Comput. Conf.*, 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," *J. DataAcquis. Process.*, vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomoncodes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, "T1: Erasure codes for storage applications," in *Proc. 4thUSENIX Conf. File Storage Technol.*, 2005, pp. 1–74.

[9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligencein wireless sensor networks: A survey," *IEEE Commun. Surv. Tuts.*,vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreservingand copy-deterrence content-based image retrieval scheme incloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11,pp. 2594–2608, Nov. 2016.

Copyright @ 2022 Author