International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

PRIVACY PRESERVING CLOUD STORAGE BASED ON A THREE LAYER SECURITY MODEL BASED ON COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING

VADDI PRAVALLIKA, B.SIVA KUMAR
PG SCHOLAR.DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE, AP, INDIA
ASSOCIATE PROFESSOR, DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE,, AP, INDIA

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 pro-posed 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.

1. INTRODUCTION

The computer technology has developed rapidly. Cloud computing has gradually matured through so many people's efforts. Then there are some cloud-based technologies deriving from cloud computing. 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.

2. LITERATURE SURVEY

Security and Privacy in Fog Computing: Challenges**.** Fog computing paradigm extends the storage, networking, and computing facilities of the cloud computing towards the edge of the networks while offloading the cloud data centers and reducing service latency to the end users. However, the characteristics of fog computing arise new security and privacy challenges. The existing security and privacy measurements for cloud computing can not be directly applied to the fog computing due to its features such as mobility, heterogeneity, large-scale geo-distribution. This article provides an overview of existing security and privacy concerns, particularly for the fog computing. Afterward, this survey highlights ongoing research effort, open challenges, and research trends in privacy and security issues for fog computing.

Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues**.** With the explosive growth of Internet of Things devices and massive data produced at the edge of the network, the traditional centralized cloud computing model has come to a bottleneck due to the bandwidth limitation and resources constraint. Therefore, edge computing, which enables storing and processing data at the edge of the network, has emerged as a promising technology in recent years. However, the unique features of edge computing, such as content perception, real-time computing, and parallel processing, has also introduced several new challenges in the field of data security and privacy-preserving, which are also the key concerns of the other prevailing computing paradigms, such as cloud computing, mobile cloud computing, and fog computing. Despites its importance, there still lacks a survey on the recent research advance of data security and privacy-preserving in the field of edge computing. In this paper, we present a comprehensive analysis of the data security and privacy threats, protection technologies, and countermeasures inherent in edge computing. Specifically, we first make an overview of edge computing, including forming factors, definition, architecture, and several essential applications. Next, a detailed analysis of data security and privacy requirements, challenges, and mechanisms in edge computing are presented.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Then, the cryptography-based technologies for solving data security and privacy issues are summarized. The state-of-the-art data security and privacy solutions in edge-related paradigms are also surveyed. Finally, we propose several open research directions of data security in the field of edge computing.

3. EXISTING SYSTEM

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. Cloud storage is a cloud computing system which provides data storage and management service Nowadays there are a lot of companies providing a va-riety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large ca-pacity of storage and various services related to other popular applications, which in turn leads to their success in attracting humorous subscribers. However, cloud storage service still exists a lot of security problems. 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.

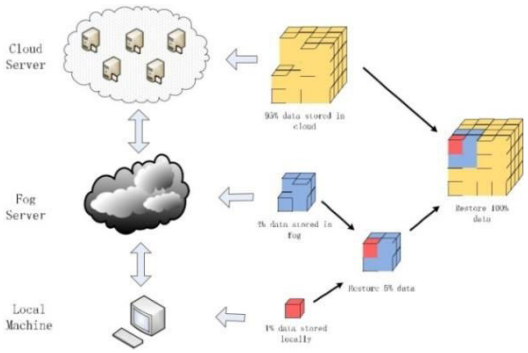
User uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data The CSP (Cloud service provider) can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data.

4. PROPOSED SYSTEM

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. The introduction of fog computing can relief the cloud computing layer, improving the work efficiency.

Users do have full control of their stored data. The CSP (Cloud service provider) or attackers can't access stored data in the cloud, with the protection of three layer security system Introduced TLS ensure the original data cannot be recovered by partial data.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

Owner Module:

In the first module we develop the Owner functionalities, In Owner module, owner can upload a new File, and owner can check file divided into blocks and saves in 3 locations with MAC code.

Fog Server Module:

In Fog Module Owner can check the file details and files download history like cloud, in fog server some part of data will save for security purpose of full data. If full file need to access, Fog server stored data also required for full access of file, with our part data file can't be access completely. So the Fog module also will have the file download history.

Cloud Module:

In this module we focus on storage and security of data. Once the file upload to cloud by downer, file details can view in cloud.

Can view the user request details and can view file download histoy.

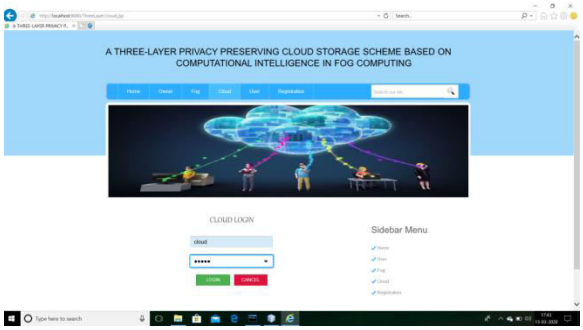
User Module:

In this module we design user functionalities. User can view the files available and can send request for file accessing.

On receipt of key from data owner, user can download the file completely.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

7. RESULTS



8. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

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 cloud computing: 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 virtual machine and bandwidth allocation in software defined network (sdn) and cloud 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 data storage 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 collection in 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. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

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

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