2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

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

[#1]KORRA PRIYANKA, [#2]M.NARENDHAR

M.TECH STUDENT, DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

ASSOCIATE PROFESSOR,DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

Abstract: Fog computing is an emerging technology in the field of network services where data transfer from one device to another to perform some kind of activity. Fog computing is an extended concept of cloud computing. It works in-between the Internet of Things (IoT) and cloud data centers and reduces the communication gaps. Fog computing has made possible to have decreased latency and low network congestion. The privacy protection schemes supported encoding technology. There are several privacy protective strategies within the aspect to forestall information in cloud. We tend to propose a three-layer storage security in cloud. The projected framework will each take full advantage of cloud storage and shield the privacy of knowledge. Here we designed to divide data into different parts . If the one information is missing we tend to lost the information. In this framework we tend to use bucket thought based mostly algorithms and secure the information then it will show the protection and potency in our theme. Moreover, supported process intelligence, this algorithmic program will reckon the distribution proportion keep in cloud, fog, and native machine.

Key Words:- *Cloud Computing, Cloud Storage, Fog Computing, Privacy Protection, Cryptography.*

1. INTRODUCTION

The Internet of things (IoT) will be the Internet of future, as we have seen a huge increase in wearable technology, smart grid, smart home/city, smart connected vehicles. International Data Corporation (IDC) has predicted that in the year of 2015,"the IoT will continue to rapidly expand the traditional IT industry" up 14% from 2014 [1]. Since smart devices are usually inadequate in computation power, battery, storage and bandwidth, IoT applications and services are usually backed up by strong server ends, which are mostly deployed in the cloud, since cloud computing is considered as a promising solution to deliver services to end users and provide applications with elastic resources at low cost. However, cloud computing cannot solve all problems due to its own drawbacks. Applications, such as real time gaming, augmented reality and real time streaming, are too latency-sensitive to deploy on cloud. Since data centers of clouds are located near the core network, those applications and

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

services will suffer unacceptable round-trip latency, when data are transmitted from/to end devices to/from the cloud data center through multiple gateways. Besides this, there are also problems unsolved in IoT applications that usually require mobility support, geo-distribution and location-awareness. Fog computing is usually cooperated with cloud computing. As a result, end users, fog and cloud together form a three layer service delivery model, as shown in Fig. 1[20]. Fog computing also shows a strong connection to cloud computing in terms of characterization. For example, elastic resources (computation, storage and networking) are the building blocks of both of them, indicating that most cloud computing technologies can be directly applied to fog computing.

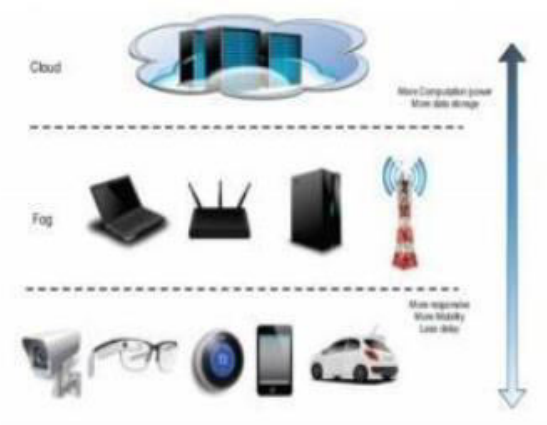

Fig.1.Architecture

However, fog computing has several unique properties that distinguish it from other existing computing architectures. The most important is its close distance to end users. It is vital to keep computing resource at the edge of the network to support latency-sensitive applications and services. Another interesting property is location-awareness; the geo-distributed fog node is able to infer its own location and track end user devices to support mobility. Finally, in the era of big data, fog computing can support edge analytics and stream mining, which can process and reduce data volume at a very early stage, thus cut down delay and save bandwidth. In the paper, we focus on the fog computing platform design and applications. We will briefly review existing platforms and discuss important requirements and design goals for a standard fog computing platform. We will also introduce some IoT applications to promote the fog computing.

II. RELATED WORK

There are a few terms similar to fog computing, such as mobile cloud computing, mobile edge computing, etc. Below we explain each of them.

i. **Local Cloud**: Local cloud is a cloud built in a local network. It consists of cloud-enabling software running on local servers and mostly supports interplay with remote cloud. Local cloud is complementary to remote cloud by running dedicated services locally to enhance the control of data privacy.

ii. **Cloudlet**: Cloudlet is "a data center in a box", which follows cloud computing paradigm in a more concentrated manner and relies on high-volume servers [4].Cloudlet focuses more on providing services to delay-sensitive, band width limited applications in vicinity.

iii. Mobile Edge Computing: Mobile edge computing [5] is very similar to Cloudlet

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

except that it is primarily located in mobile base stations.

iv. **Mobile Cloud Computing:** Mobile cloud computing(MCC) is an infrastructure where both data storage and data processing happen outside of mobile devices, by outsourcing computations and data storage from mobile phones to cloud [6]. With the trend of pushing cloud to the edge, MCC starts to evolve to mobile edge computing.

However, current definitions are all developed from different perspectives and thus not general. For example, though mobility comes first in edge computing, we do not necessarily narrow it down to mobile edge computing. Fog computing should be defined for a broader range of ubiquitous connected devices. The definition from [7] gives integrative view of fog computing but fails to point out the unique connection to the cloud. We need a more general definition that can abstract all those similar concepts. Here comes our definition: Fog computing is a geographically distributed computing architecture with a resource pool consists of one or more ubiquitously connected heterogeneous devices (including edge devices) atthe edge of network and not exclusively seamlessly backed by cloud services, to collaboratively provide elastic computation, storage and communication (and many other new services and tasks) in isolated environments to a large scale of clients in proximity.Currently there are a few existing works on the concept of fog computing. Stojmenovic et al. [8], [9] have surveyed [10]–[14]. Our previous work [3], [15] has surveyed additional related work [16]–[21]. In this paper, we further identify work [22], [23] on fog computing. References [4], [10], [16], [19] are about designing and implementing fog computing nodes. Cloudlet [4], [19] was built before the proposal of fog computing, but inherently coincides fog computing concept. Para Drop [16] is a fog computing platform implementation based on wireless router, using OS-level virtualization. Hong et al. [10] have proposed a high-level programming model for fog computing platform. References [11], [13], [14], [18], [22], [24] are about how exiting or new applications and services can benefit from fog computing. J. Zhu, et al. [11] have provided dynamic customizable optimization to web applications based on client devices and local network conditions collected by fog nodes. Ha, et al. [24] have designed and implemented a real-time wearable cognitive assistance on Google Glass backed by Cloudlet. Work [18] has designed a cloudlet mesh based intrusion detection system (IDS). Work [13] and [14] are about how rich information collected by fog computing platform can optimize operations or migrations for data processing in fog computing. Cao et al. [22] have explored to use fog computing in health monitoring such as real-time fall detection. Mohammed et al. [23] have conducted an experimental study by utilizing fog computing to assist mobile application in terms of computation offloading and storage expansion. There are also work related to underlying technologies of fog computing, security and privacy, readers can refer to our previous surveys if interested [3], [15].

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

III. PROPOSED METHOD

A. Three Layer Privacy

Now the cloud server is divided into three different layers for ensuring the security purpose and to avoid the location awareness. The three different privacy preserving layers are Cloud server, Fog server and Local server. A complete data is now partitioned and stored into three different layers. The ratio of the partition of data is major part of the data is stored in the cloud server, neither high nor low range of data is stored in the fog server and finally lower amount of local server. When the data required it can be combined in to a single data using pattern matching method.

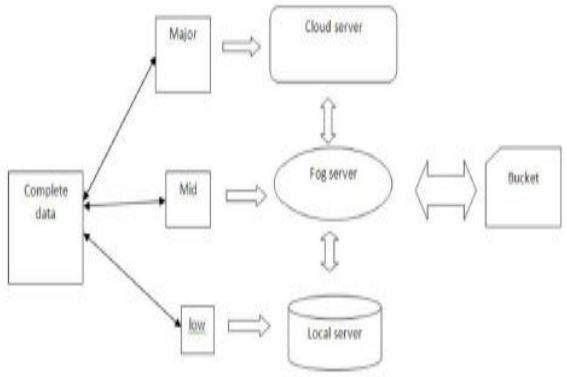

Fig.2.Three-layer privacy preserving cloud storage architecture

B. Fog Computing

Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer. Fog computing layer can perform critical data transmission to cloud server. And finally the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer

IV. ALGORITHM

The security degree is an important metric to measure the quality of cloud storage system. Furthermore, data security is the most important part in cloud storage security and it includes three aspects: data privacy, data integrity and data availability. Ensuring data privacy and integrity has always been the focus of relevant researches. On another hand, data privacy is also the most concerned part of the users. From a business perspective, company with high security degree will attract more users. Therefore improving security is an crucial goal no matter in academia or business. In this section, we will detailedly elaborate how the Transport Layer Security framework protects the data privacy, the implementation details of work flow and the theoretical safety and efficiency analysis of the storage scheme.

Three-Layer Privacy Preserving Cloud Storage Scheme

The framework can take full of cloud storage and protect the privacy of data. Here the cloud computing has attracted great attention from different sector of society. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

In our system we using a bucket concept so reduce the data wastages and reduce the process timings. We are using a BCH (Bose–Chaudhuri– Hocquenghem) code algorithm. It's High flexible. BCH code are used in many communications application and low amount of redundancy. The Bucket Access manage resource represents the Access Control Lists (ACLs) for buckets inside Google Cloud Storage. ACLs let you specify who has access to your data and to what extent. The three layer cloud storage stores into the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.

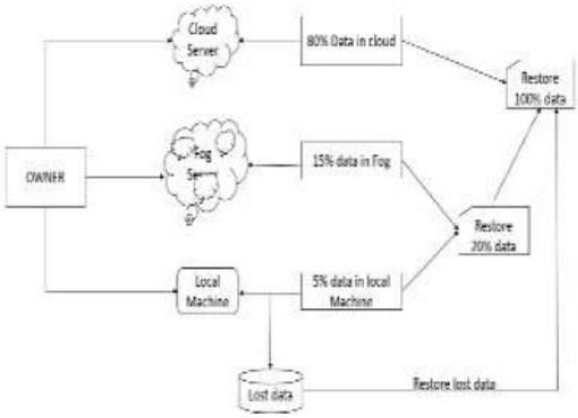

Fig -3: System Architecture

V.RESULTS

The performance analysis is also carried out in terms of running time of various algorithms in the fog server and the service time taken for transferring the files to the for server and to the cloud server also analyzed.

A. Message Integrity Analysis

Message integrity analysis can be done using HMAC algorithms. A family of cryptographic hash functions is a Secure Hash Algorithm (SHA). Another family of hash functions is Message Digest (MD). Based on the analysis, SHA-512 is a more preferable algorithm for HMAC code generation than MD. HMAC code produced by different hash functions is shown in table 2.

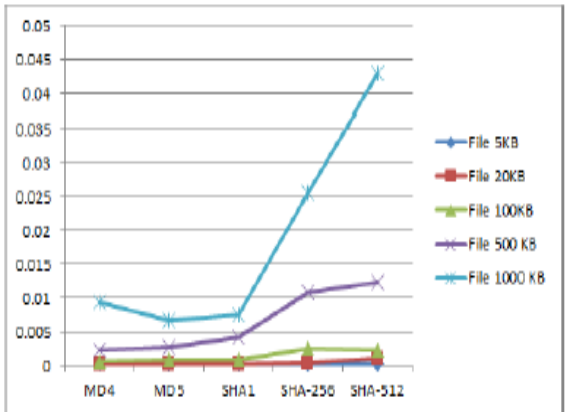

Figure. 4. Service Time of HMAC algorithms

The following results show that SHA-512 is better than MD5. The longer hash code is more difficult to break that is why SHA-512 is used in this project. But comparatively, the time taken for execution is more by SHA-512 than MD5 and analysis chart is shown in table 1.

In Fig: 4, the execution time taken by different algorithms is shown, in which the vertical axis represents the time in seconds. This comparison is done with a 32-bit key size.

1. SHA generates more strong hashes than MD5. MD5 can be broken easily. SHA hash code is longer than MD5.
2. Occurrences of collision are less in SHA than MD5. It means that we get the same HMAC code for two different inputs i.e., hashes are not always unique.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

3. SHA-512 has a good avalanche effect- when there is a small change in the input, the output changes significantly.
4. SHA-512 has the property that every bit of the hash code is a function of every bit of the input.

Performance analysis of Cloud and Fog Computing

The performance analysis is done in terms of transmission time required for uploading files to the cloud server and to the fog nodes. It is observed that the time needed for uploading files to the cloud server is more than to the fog node. The processing time is also more in the cloud server. Sarkar et.al in their paper [1] explained the service latency, processing latency and transmission latency required for cloud and fog server in detail. Therefore we can conclude that fog computing technology is more efficient when real time applications increase.

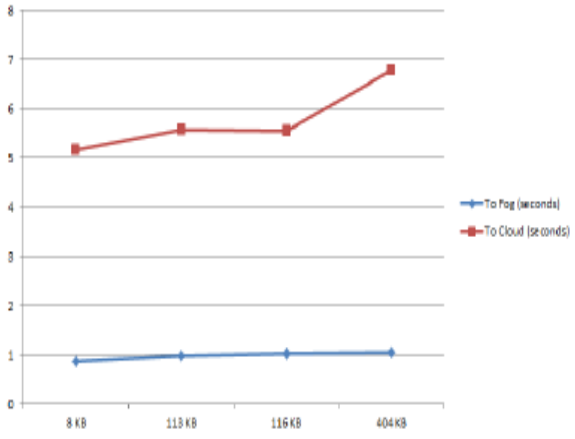

Figure.5. Comparison between cloud and fog computing

VI. CONCLUSION

These works mainly focus on securing patient's digital data within the cloud computing environment with the help of fog computing technology. First of all, a legitimate user can access original medical databases after verifying their authenticity twice. Here we need to set a decoy medical database to confuse attacker while the original medical database is kept hidden in a cloud data-center. The data from the decoy database can be returned if the authentication failed. The proposed new V2I binding algorithm is a more efficient method for securing surgery videos or private videos in their own profile photo. The analysis shows that the proposed method works well than the other cryptographic algorithms.

REFERENCES

[1] J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud assisted urban data sharing framework for ubiquitous cities, Pervasive and Mobile Computing (2017),http://dx.doi.org/10.1016/j.pmcj.2017.3.013

[2] Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z.(2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing.IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2018.2793350

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

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

AUTHOR'S PROFILE:

[1]. **M.RUCHITHA,** Pursuing *M.Tech in CSE* **at** Scient Institute Of Technology, Ibrahimpatnam, Rangareddy, T.S.

[2]. **M.NARENDHAR,** He pursued his B.Tech in CSIT from JNT University Hyderabad, M.Tech Software Engineering from JNT University Hyderabad, Ph.D pursuing from JNT University Hyderabad. He is currently working as Assoc Prof & HOD in Department of CSE at Scient Institute of Technology Ibrahimpatnam. He has 14 years of Academic experience. His research areas include Software Engineering and Data mining. He is a professional member in Computer Society of India. He has published 10 international journals and participated in One International Conference.He Attended and Conduted Many Workshops in different areas.