Fog Computing and its Major Role in Cloud Security

A. Umamaheswari[1], Arulsrinivaasan[2], S. Sabarinathan[3]

[1]AP/ CSE, Mahendra Engineering College, Tamil Nadu, India.
[2,3]B.E (CSE) 4th year, Mahendra Engineering College, Tamil Nadu, India
Email: umamaheswarime2004@gmail.com, srini.arul@zoho.com, sabarisadasivam@gmail.com

Abstract - In the past, people depended on physical computer storage or servers to run their programs. As a technological development, cloud computing provides an easier way for accessing and managing the data. Now a day to achieve better operational efficiency many software companies and small or medium agencies are shifting towards Cloud environment. But it also has some severe security risks. Very common risks now days are data theft attacks. To deal with such cases and malicious intruders, there are some techniques which are used to secure user data. A new technology called "Fog computing" is gaining attention of the cloud users nowadays. Fog computing promises more security by implementing decoy system in cloud computing and also improves the quality of service. Fog computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. Even though fog computing faces new security and privacy challenges besides those inherited from cloud computing.

Keywords - Cloud Computing, Fog Computing, Data theft, security, privacy, decoy system.

I. INTRODUCTION

In today's world, the small as well as big -big organizations are using cloud computing technology to protect their data and to use the cloud resources as and when they need. Cloud is a subscription based service. With the fast growth of World Wide Web (WWW) user can access virtually any database for which they have proper access right from anywhere in the world. By registering into cloud the users are ready to get the resources from cloud providers and the organization can access their data from anywhere and at any time. The way of use computers and store our personal and business information can arise new data security challenges. To overcome by this problem, we are using a new technique called as fog computing. It also provides more security. once the user is ready by filling up the sign-up form he will get the message or email that he is ready to take the services from fog computing.

II. DATA BREACHES IN CLOUD

Cloud computing security does not focus on ways of secure the data from unauthorized access as shown in Figure 1. Encryption does not provide much security to our data.

Fig. 1 Affected domains

The second threat to cloud computing security is data loss. Permanently loosing data hosted on a cloud can result from several reasons; malicious hackers, accidental deletion by the cloud service provider, or a natural disaster could all result in permanent data loss unless adequate measures are taken to backup data, from both the provider and client's initiatives.

III. FOG COMPUTING

Fog Computing system is trying to work against the attacker especially malicious insider. Malicious insider refers to the employers in the service provider site. Fog computing architecture and further used it for improving Web site's performance with the help of edge servers. They said that the emerging architecture of Fog Computing is highly virtualized. They presented the idea that the Fog servers monitor the requests made by the users and keep a record of each request by using the user's IP address or MAC address. In the fog network, privacy-preserving algorithms can be running in between the fog and cloud while those algorithms are usually resource- prohibited at the end devices. Fog node at the edge usually collects sensitive data generated by sensors and end devices. Techniques such as homomorphic encryption can be utilized to allow privacy-preserving aggregation at the local gateways without decryption. Figure 2 shows the architecture of the fog computing mitigating insider data theft attacks in the cloud.

IV. CLOUD SECURITY BY FOG COMPUTING

There are various ways in which user can save the date in remote service through internet. The issue of providing security to confidential information is core security problem. It is good to say that all the standard approaches used for providing security have been demonstrated to fail from time to time for a variety of reasons, including faulty implementations, buggy code, insider attacks, misconfigured services, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Decoy data, such as decoy documents, honeypots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to „poison" the thief's ex-filtrated information. Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appears completely normal and legitimate. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features: [1] validating whether data access is authorized when abnormal information access is detected, and [2] confusing the attacker with bogus information that is by providing decoy documents.

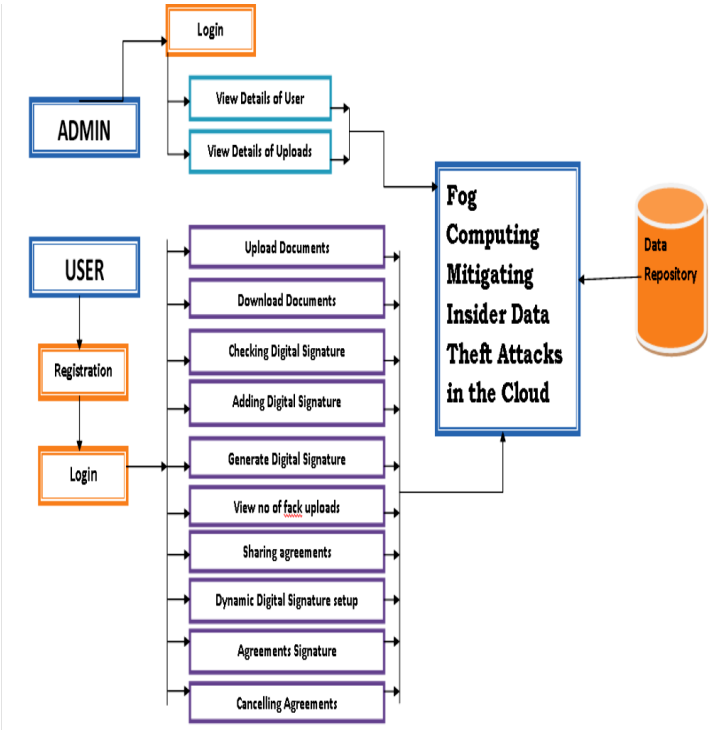

Fig. 2 Architecture

V. DECOY SYSTEM SECURITY

The file system is packed together with traps these traps are upload on the system by the Cloud service provider. These traps can contain documents like credit card details, tax returns, bank statements. These documents are places in highly egregious places. A masquerade who is not acquainted with the system and who has an ill intent may is likely to click on these false documents. Thereby the system can be notified of masquerade activity. The hash code of all the legitimate and decoy documents upload on the system is calculated. The hash code of every document downloaded is matched with the hash code of the decoy document. If a match is found, then the document is deemed to be a decoy document and an alert is generated. An insider attacker would not be able to escape detection if they access a decoy document. The hash code is

based on keyed-Hash Message Authentication Code (HMAC). HMAC that is keyed hashed message authentication code which is used for calculating a message authentication code. It involves a cryptographic hash function along with a secret key. We are calculating the HMAC code of the document by using the MD5 Algorithm.MD5 processes a document of variable length into a fixed length output of 128 bits. Figure 3 shows the procedure for unauthorized access detection.

- Variable length to fixed length output.
- Input n-bit blocks
- Input divided into 512 bit blocks
- Padding is done
- Buffer initialization
- Output 128 bit

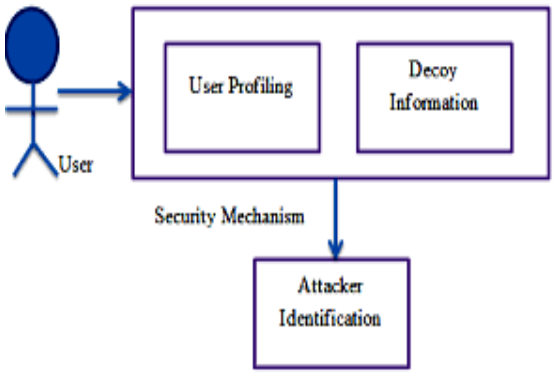

Fig. 3 Unauthorized access detection

VI. CONCLUSION

The system was developed only with email provision but we have also implemented the SMS technique. In Fog Computing we presenting a new approach for solving the problem of insider data theft attacks in a cloud using dynamically generated decoy files and also saving storage required for maintaining decoy files in the cloud. Thus, it provides more security in cloud computing.

REFERENCES

[1] Majid Hajibaba and Saeid Gorgin "A Review on Modern Distributed Computing Paradigms: Cloud Computing, Jungle Computing and Fog Computing", Journal of Computing and Information Technology, CIT 22, Vol. 2, 69–84, 2014.

[2] Zhu, Jiang, "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture", Service Oriented System Engineering (SOSE), IEEE. 2013.

[3] Luis M. Vaquero and Luis Rodero-Merino "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing" ACM SIGCOMM Computer Communication Review – Vol. 44, No. 5, October 2014.

[4] Luis M. Vaquero, Daniel Moran, Fermin Galan, and Jose M. Alcaraz-Calero. Towards runtime reconfiguration of application control policies in the cloud. J. Netw. Syst. Manage., Vol. 20, No. 4, pp. 489-512, 2012.

[5] Kirak Hong, David Lillethun, Umakishore Ramachandran, Beate Ottenw¨alder, and Boris Koldehofe, "Mobile fog: A programming model for large-scale applications on the internet of things", In Proceedings of the 2nd ACM SIGCOMM Workshop on Mobile Cloud Computing, MCC-13, pp. 15–20, 2013.