"Fog computing for securing data on Cloud–A Review"

Prof Sushil Goel[#1], Gurmeet Kaur[*2]

[#]*Associate Professor & Head, Deptt. Of Computer Sciences, Dyal Singh College, Karnal*

[*]*Assistant Professor, Dyal Singh College, Karnal*

[1]sgoel1021@gmail.com

[2]grmtkaur02@gmail.com

***Abstract*— Cloud computing is using as a delivery platform which is a promising way for storing user data and provides a secure access to personal and business information. The users are provided with on-demand services through the Internet. But there is a risk of the involvement of a third party which makes it difficult to trust that user data is secure enough and will not be misused. To deal with such malicious intruders there are some technology which are used to secure user data called "Fog computing". It is gaining attention of the cloud users nowadays. This paper review the work that has been done using this technology and discussed the paradigm for preventing misuse of user data and securing information.**

I. INTRODUCTION

Small and medium businesses (SMBs) are increasingly opting for outsourcing data, information and computation to the Cloud. Cloud computing is achieving popularity and gaining attention in business organizations. It provides a variety of services to the users. It is a convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources [1].

Business agencies and software companies are admiring cloud computing for its ease of access and flexible architecture. For attaining more and more operational efficiency and managing data organization with small or large businesses are using cloud environments. Cloud Computing is a combination of many computing strategies and service oriented architecture such as virtualization and networking. Although, Cloud Computing provides an easy way for managing, accessing and computation of user data, but it also has some severe security risks as data leakage, data theft. There are some traditional security mechanism such as authorization, identity, and authentication but now these are not sufficient [2].

To resolve these issues a mechanism which can detect such malicious activities is required. For this, Fog computing is introduced by CISCO which monitors the data and helps in detecting an unauthorized access. According to CISCO, due to its wide geographical distribution the Fog computing is well suited for big data and real time analytics. As Fog nodes provide localization, therefore enabling low latency and context awareness, while Cloud provides global centralization [3]

Salvatore J. Stolfo [4] et al. used fog computing for making disinformation attacks against the malicious intruder or attacker Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, storage, compute, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it supports mobility too. Set-up boxes and Access points are used as end devices to host services at the network. These end devices are also termed as edge network.

Sabahi, F.[5] mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In his paper he has summarized availability and reliability elated issues of cloud resources provided by the trusted third party. He also discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology providing the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [5].

Claycomb, W. R. (2012) [6] has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers to break the security. They have also presented two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and also the insider who uses cloud systems to carry out an attack on an employer's local resource. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

II. NEED OF SECURITY ON CLOUD

Kaufman L. et al. (2009) [7] has examined some security issues and the associated regulatory and legal concerns that have arisen as cloud computing. Interestingly, a major concern included in the Security Content Automation Protocol (SCAP) is the lack of interoperability between system-level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, it is effectively address cloud computing future security needs for providing data confidentiality which can impact the incident reporting.

Godoy et al. [8] explained that there is a need of such profiling strategies or methods through which user profiling can be done. As there is a huge amount of data and information available on the internet therefore from last few years personal information agents are helping the users to manage their information. In his paper the authors have discussed a learning technique for data acquisition for user profiling and mentioned some methods for adaption with the changes which happen timely by changing user's interest. They said earlier only supervised learning technique used in general. But for moving the information agents to the next level authors are focusing research on assessment of semantically useful user profiles. They also said that account hijacking is a disadvantage for such user profiling.

III. Literature survey

Madsen.H and Albeanu. G [9] presented the challenges faced by cloud computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is primarily done for the need of the geographical distribution of resources instead of having a centralized one. A multi-level architecture is followed in Fog computing platforms. In first level there is machine to machine communication and the higher level deal with visualization and reporting. The higher level is represented by the Cloud. They said that building Fog computing projects are challenging and difficult [4]. But there are methodologies and algorithms available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible.

Grobauer B. Et al. (2012), [10] provided an overview of vulnerabilities in security of cloud. They explained the meaning of the term vulnerability that its the probability that an asset is unable to defend itself against an threat or attack. They said vulnerabilities should always be defined in terms of resistance to attacks or threat. Control challenges mainly highlight situations in which otherwise successful security controls are ineffective in a cloud setting. They have discussed about the core cloud computing technologies such as services and web applications which use PaaS SaaS and platforms, virtualization and said that there are many such security requirements which are solvable only with the help of cryptographic techniques.

Park, Y. Et al. (2012) [11] developed a technique that was a software decoy for securing cloud based data using software. They proposed a software-based decoy system that aims to detect the exfiltration of proprietary source code and to deceive insiders. The system designs a Java code which provides valuable information of the attacker. Further static obfuscation method is used to generate and transform original software. Bogus programs are designed by software that is automatically transformed from original source code, but designed to be dissimilar to the original[11].This deception method confuses the insider and also obfuscation helps the secure data by hiding it and transferring bogus information for insider. Beacons are also injected into the bogus software to detect the exfiltration and making an alert if the decoy software is touched, executed or compiled.

Salvatore J. Stoflio et al [4] proposed a new technology and named it as Fog computing. They implemented security by using decoy information technology. They discussed two techniques, namely User behavior profiling and Decoy technology. In User behavior profiling they checked how, when and how much amount of data and information a user is accessing. They monitored their user's activity to check for any abnormality in the data access & usages behavior of the user. The second technology is decoy in which information which is bogus or one can say fake such as honey pots, honey files etc. are used to confuse the malicious intruder or attacker by depicting the information in such a way that it seems real.

Z. Jiang et al. [12] discussed Fog computing architecture and used it for improving Web site's performance using of edge servers. They said that the emerging architecture of Fog Computing is highly virtualized. They presented their idea that the Fog servers, monitor each and every requests made by the users and keep a record of each request by using the user's MAC address or IP address. Further, when a user requests for same website increases than a given decided number (N is tunable parameter) then the user's browser can cache the common CSS and JS files and then furthers send them externally. They also mentioned that it is possible to measure page rendering speed with the help of snippets.

IV. Securing clouds using fog

The proposals for cloud based services describe methods to store documents, files, and media in a remote service that may be accessed are broadly accepted concerns guarantees for securing a user's data in a manner where that guarantees only the authorized user and no one else can gain access to that data.

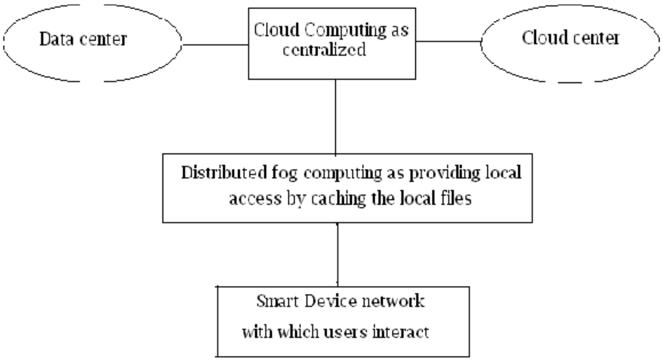
Data center
Cloud Computing as centralized
Cloud center
Distributed fog computing as providing local access by caching the local files
Smart Device network with which users interact

Fig. 1 Role of fog computing for security on cloud computing

The problem of providing security of confidential information remains a main core security problem that, till date, has not provided the levels of assurance most people desire. Figure 1 shows role of fog computing for security of data on cloud.

Many proposals have been made to secure remote data in the Cloud using encryption and standard protocols. It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety insider attacks, mis-configured services, faulty implementation buggy code, and the creative construction of effective and

Sophisticated attacks not envisioned by the implementers of security procedures.

A Twitter incident [13] is one example of a data theft attack from the Cloud Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and subscriber's accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker used a Twitter administrator's password to get access to Twitter's corporate documents hosted on Google's infrastructure & server as Google Docs.

A trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no right way to get it back. One needs to prepare in advance for such accidents. The basic idea is that limit the damage of stolen data if we decrease the value of that stolen data and information to the attacker. This can achieve through a 'preventive' disinformation attack.

To overcome this Fog computing tries to secure the storage of data in the by using decoy information. This technology introduces disinformation against harmful persons or malicious insiders, preventing real sensitivity data to worthless data.

A. Case study

The services can be implemented by giving two features:

1) *User Behavior Profiling:* It is expected that access to a user's data and information in the Cloud will exhibit a normal method of access. User profiling is a well known technique that can be applied here to model how, when, and how much times a user accesses their information in the Cloud. In this way 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This technique of behavior-based security is commonly used in fraud detection applications and services. Such profiles would actually include volumetric information, how many documents are typically read and how often.

Legitimate users of a computer system are familiar with the files on that system and where they are located. Any search for specific files is likely to be targeted and limited. A masquerade or harmful person is one which gets access to the victim's system illegitimately or unofficially, is unlikely to be familiar with the structure and contents of the file system. Their search is likely to be widespread and untargeted. On the bases of this key assumption, user search behavior is profiled and developed user models trained with a one class Modeling technique, namely one-class support vector machines. The importance of using one-class modeling originates from the ability of building a classifier without having to share data from different users. The privacy of the user and their data is therefore preserved.

2) *Decoys Technology:* Decoy information, such as decoy documents, honey pots, honey files, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's exfiltraed information. Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. Decoy files or documents are trap files. The traps can be placed within the file system. The traps are decoy files downloaded from a Fog computing site, an automated service that offers several types of decoy documents such as medical records, tax return forms, e-bay receipts credit card statements.

The decoys, then, serve two purposes:

a. Validating whether data access is authorized or legal when abnormal information access is detected, and
b. Obfuscating or confusing the attacker with bogus information. The decoy documents carry a keyed-Hash Message Authentication Code (HMAC), which is hidden in the header section of the document. The HMAC is computed or designed over the file's contents using a key unique to each user.

The advantages of placing decoys in a file system are three ways:

a. The detection of masquerade or harmful activity
b. The confusion of the attacker and the additional costs incurred to distinguish real from bogus information, and
c. The deterrence effect which, although hard to measure, plays a significant role in preventing masquerade party activity by risk-averse attackers.

Combining the User Behavior Profiling and Decoys Technology: The correlation of search behavior anomaly detection with trap-based decoy files system should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. It is hypothesize that detecting abnormal search operations performed prior to an unsuspecting or unauthorized user opening a decoy file will confirm the suspicion that the user is indeed impersonating another victim user. This scenario covers the threat model of illegitimate or unauthorized access to Cloud data. Furthermore, an accidental opening of a decoy file by a legitimate or authorized user might be recognized as an accident if the search behavior is not deemed abnormal. In other words, detecting abnormal behavior search and decoy traps together may make a very effective masquerade or harmful activity detection system. Combining the two techniques improves detection accuracy.

In addition to these techniques fog computing suggest that user profiles are accurate enough to detect unauthorized Cloud access .When such illegitimate or unauthorized access is detected, one can respond by presenting the user with a decoy document or with a challenge question to validate whether the access was indeed unauthorized, similar to using decoys in a local file setting, to validate the alerts issued by the anomaly detector that monitors user file search and access behavior.

V. CONCLUSION

With the increase of data theft attacks or threat, the security of user data is becoming a serious issue for cloud service providers, for which Fog Computing paradigm is introduced which helps in monitoring the behaviour of the user and providing security to the user data. The paper title "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud "discussed about how to monitor data and provides data security from harmful person or malicious intruders and also helps in confusing the attacker about the real information by using User Behavior Profiling and Decoy Information technology[4].The paper title "Software decoys for insider threat "discussed a technique that confuses the insider and also used obfuscation which helps to secure data by hiding it and making it bogus information for insider using a technique that was a software decoy for securing cloud data using software[11] .The paper title" Reliability in the Utility Computing Era: Towards Reliable Fog Computing "Provides the concept of Fog computing and its feasibility for real life projects using three level architecture for Fog Computing [9]. By continuing this work using Fog Computing platforms can lead to improved defensive techniques for masquender activity and would contribute in increasing the level of security if user data on the cloud.

REFERENCES

[1] Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. "An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 2013.

[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472484.

[3] Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13-16.

[4] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[5] Sabahi, F. "Cloud computing security threats and responses", In Communication Software and Networks (ICCSN), 2011 IEEE 3rd In ternational Conference on 2011,pp. 245-249.

[6] Claycomb, W. R., & Nicoll, A. "Insider Threats to Cloud (Computing: Directions for New Research Challenges", In Computer Software and Applications Conference COMPSAC), IEEE 36th Annual, 2012, July, pp. 387-394.

[7] Kaufman, L. M. "Data security in the world of cloud computing". Security & Privacy, IEEE, 2009, 7 (4), 61 -64.

[8] Godoy D., "User profiling for web page filtering", IEEE Internet Computing, Jul. 2005, vol. 9, no. 4, pp. 56–64.

[9] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

[10] Grobauer, B., Walloschek, T., & Stocker, E. "Understanding cloud computing vulnerabilities". Security & Privacy, IEEE, 2011, pp. 50-57.

[11] Park, Y., & Stolfo, S. J. "Software decoys for insider threat", In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94).

[12] Zhu, Jiang, et al. "Improving Web Sites Performance Using Edge Servers in Fog Computing

[13] Architecture." Service Oriented System Engineering (SOSE), 2013 IEEE.

[14] [13] P. Allen, "Obama's Twitter password revealed after French hacker arrestedfor breaking into U.S. president'saccount,"March 2010. [Online].Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-passwordrevealed-French-arrested.html.