Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fog Computing Providing Data Security: A Review

Manreet kaur
Information technology,
Chandigarh University, India

Monika Bharti
Computer Science engineering,
Chandigarh University, India

Abstract— Cloud computing is a delivery platform which promises a new way of accessing and storing personal as well as business information. It provides resources to its users through the Internet. But it also has a risk that is the involvement of a third party which makes it difficult to trust that user data is secure enough and will not be misused. To provide security, new technology called Fog computing has arrived through which user data can be secured. In this paper, we discussed this paradigm in detail and review the work that has been done using this technology.

Keywords— cloud computing, fog computing, decoy technique , insider theft attacks.

I. INTRODUCTION

Cloud computing is achieving popularity and gaining attention in business organizations. It offers a variety of services to the users. It is an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [1]. Due this ease, software companies and other agencies are shifting more towards cloud computing environment. To achieve better operational efficiency in many organizations and small or medium agencies is using Cloud environment for managing their data. Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and other which rely on the Internet. It is considered as a delivery platform in which resources are provided as a service to the client through the Internet. Although, Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. There are some traditional security mechanism such as identity, authorization and authentication, but now these are not sufficient [2].

Very common risks now days are data theft attacks. Data theft is considered one of the top threats to cloud computing by the Cloud Security Alliance [3]. Moreover, if the attacker is an insider than the chances of data theft increase as the insider may already have some personal information. The common notion of a cloud insider as a rogue administrator of a service provider is discussed, but we also present two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource [11]. 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. Salvatore J. Stolfo et al. used it for making disinformation attacks against the malicious intruder or attackerFog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network. This concept of Fog computing is explained in the literature survey.

Shifting from cloud to fog : Fog computing improves the Quality of service and also reduces latency. According to Cisco, due to its wide geographical distribution the Fog computing is well suited for real time analytics and big data. While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization [12].

Fog computing provides- Low latency and location awareness, it has Wide-spread geographical distribution, supports Mobility, is compromised due to the huge number of nodes.
The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of the network. Here the term edge refers to different nodes to which the end user is connected and it is also called edge computing. If we look according to architecture fog is situated below the cloud at the ground level. The term fog computing is given by CISCO as a new technology in which mobile devices interact with one another and support the data communication within the Internet of Things.

But here we consider Fog Computing as a paradigm through which we can provide local access to the user and with the help of decoy technology, we provide security for user data and prevent insider theft attacks.

In this paper, we review the literature for Fog Computing security and reliability concerns and various techniques followed in Fog computing. Section II presents the literature Survey and in Section III is the comparison of research done by various authors. Section IV provides the conclusion to the paper.

II. LITERATURE REVIEW

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 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, we can effectively address cloud computing's future security needs. They also emphasize on the of providing data confidentiality which can impact the incident reporting.

Grobauer B. Et al. (2012), [8] provided an overview of vulnerabilities in security of cloud. They explained the meaning of the term vulnerability that it it's the probability that an asset is unable to defend itself against a threat.they said vulnerabilities should always be defined in terms of resistance to attacks or threat.Control challenges typically 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 web applications and services which use SaaS and PaaS platforms, virtualization and said that there are many such security requirements which are solvable only with the help of cryptographic techniques. Thus, these challenges are of special interest for further cloud computing security research.
Sabahi, F. (2011) [9] mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In this paper he has summarized reliability and availability related issues of cloud resources provided by the trusted third party. He discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [9].He said that security is the most argued concern in cloud computing because user's entire data is stored at a remote location and that location needs to be secure enough that it could deal with data thefts and malicious intruders.

Claycomb, W. R. (2012) [10] 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 breach 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 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.

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

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

Madsen.H and Albeanu. G [5] presented the challenges faced by current computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one. A multi-tier architecture is followed in Fog computing platforms. In first tire there is machine to machine communication and the higher tiers deal with visualization and reporting. The higher tier is represented by the Cloud. They said that building Fog computing projects are challenging [5] but there are algorithms and methodologies available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible. Z. Jiang et al. [6] Discussed 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 that their 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. Further, when a user requests for same website increases than a given number (N is tunable parameter) then the user's browser can cache the common CSS and JS files and then onwards send them externally. They also mentioned that it is possible to measure page rendering speed with the help of snippets.

III. COMPARISON TABLE

Paper title	Advantages	Techniques
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	Developed a technique that was a software decoy for securing cloud data using software
Reliability in the Utility Computing Era: Towards Reliable Fog Computing	Provides the concept of Fog computing and its feasibility for real life projects	Three tier architecture for Fog Computing is discussed.
Improving Websites Performance using Edge Servers in Fog Computing Architecture	Concept of Fog Computing Architecture is used in such a way that various methods are combined with unique knowledge to improve the performance of rendering a web page	Minimizing HTTP requests, reducing the size of web objects and reorganizing the web page.
Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud	Monitor data and provides data security from malicious intruders and also helps in confusing the attacker about the real information	1- User Behavior Profiling 2- Decoy Information technology

IV. CONCLUSIONS

With the increase of data theft attacks the security of user data security is becoming a serious issue for cloud service providers for which Fog Computing is a paradigm which helps in monitoring the behavior of the user and providing security to the user data. Other techniques discussed in this paper use Fog computing for optimizing the website performance. We hope that by continuing this work using Fog Computing platforms can lead to improved defensive techniques and would contribute in increasing the level of security if user data on the cloud.

ACKNOWLEDGMENT

This research paper is made possible with the help and support of my parents, teachers, family, friends, and all the people who guided me throughout my work.Especially, I am thankful and I express my gratitude to the following people who contributed and helped to make this work possible:

First and foremost, I would like to thank Ms. Monika Bharti for her support and encouragement with which I was motivated and was able to write this paper. She kindly read my paper and suggested me

Advices on grammar, matter, and the title of the paper. Second, I would like to thank all the other professors of my department who have suggested me and helped me in writing this paper.

Finally, I sincerely thank to my parents, family, and friends, who gave me emotional and financial support. Without the support of these kind people the product of this research paper would not be possible.

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, 4(1), pp. 1-13.

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

[3] Archer, Jerry, et al. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).

[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] 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.

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

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

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

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

[10] 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.

[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] 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).

