International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 03, Volume 4 (March 2017) www.ijirae.com

A Study on Cloud and Fog Computing Security Issues and Solutions

Archana Lisbon A*, Kavitha R**
**Department of Computer Science Christ University, Bengaluru, INDIA*
***Assistant Professor, Department of Computer Science Christ University, Bengaluru, INDIA*

***Abstract* — Cloud computing is the significant part of the data world. The security level in cloud is undefined. Fog computing is the new buzz word added to the technical world. And the term Fog was coined by CISCO. The need for Fog computing is security and gets the data more closely to the end-user. Fog Computing is not going to replace the Cloud computing, it will be acting as the intermediate layer for securing the data which is stored inside the cloud. The principal idea of this paper is to provide data safety measures to the Cloud storage through Fog Computing. Fog Computing will be playing the vital role for the future technology. The Internet of Things (IoT) will be using the Fog computing to implement the smart World concept. So, in the future we have to handle huge amount of data and we need to provide the security for the Data. This study gives the security solutions available for the different issues.**

***Keywords*— Cloud Computing. Fog Computing, Threats, Security solutions, Internet Of Things (IoT)**

I. INTRODUCTION

The perspective of seeing the world has been evolving day by day. The word is filled with enormous amount of data, generated from various sources like social media, e-commerce websites, personal data etc. we have to store this huge amount of data and maintain it, for various purposes. In 2000, the cloud computing came into existence. Cloud computing provided the easiest way to store data and access it from anywhere and anytime.

Many organizations moved from tradition way of storing data and they started using the cloud computing. The various cloud providers provide the storage to store the information. The main problem with the cloud storage is providing security to the valuable information stored in it. Huge amount of data is residing in various servers in distinct part of the world. The providers are responsible for providing the security for the data.

The Internet of Things is boomed in the IT field and gained more popularity in the research area. Fog computing is intermediary layer between the cloud computing and Internet of Things. The security to the data can be provided in the Fog. This document is a template. An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

II. OVERVIEW OF CLOUD COMPUTING

Cloud computing allows the users with many potentials such as storing huge amount of data and access it from anywhere and everywhere. To use the stored information the users need to have basic internet connection. The cloud computing can be classified based on the deployment model and service delivery model.

A. CLOUD COMPUTING DEPLOYMENT MODELS

- *Private cloud: The cloud model which provides services to single organizations. This type of cloud is implemented within the organization.[3]*
- *Community cloud: The cloud model which is shared or controlled by multiple companies and supports particular groups which has similar concerns [4]*
- *Public cloud: The cloud model which is maintained by various, Cloud Service Providers (CSP) [5]*
- *Hybrid cloud: The cloud model which consists of combination of more than one model [8]*

B. CLOUD COMPUTING SERVICE MODELS

The three basic service models offered by the cloud computing providers are Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

- *Infrastructure as a Service (IaaS): The virtual, physical, additional storage and networking devices are provided by the cloud computing providers. The hypervisors are used to run the virtual devices. The cloud users are responsible for installing operating systems on the virtual devices and application softwares. [19]*
- *Platform as a Service (Paas): The service model utilises the platform or the software provided by the Cloud Service Providers (CSP). This model allows the user to develop, run, and maintain the applications. [20]*
- *Software as a Service (SaaS): This service model avoids the support and maintenance of the software. The cloud infrastructure is installed with various softwares and the cloud users can be able to use the softwares which has been installed already in it. Hence forth installing software's in their machines can be eliminated. [21]*

III. FOG COMPUTING OVERVIEW

The view of CISCO towards fog computing is the extended version of cloud computing. Fog computing brings the services to edge of the network to the users. Fog computing is also called as the Edge computing. Fog computing is extremely virtual platform, which offers network services, storage space, computational services to the cloud servers and the end user devices. [14]

Fog computing plays major role in supporting, implementing the Internet of Things (IoT). Fog computing actually minimizes the latency, which enhance the Quality of Service (QoS).The main reason for the raise of fog computing is for the applications which are having the latency issues. When the Internet of Things is implemented billions of devices will be added into the network. The cloud computing will not be able to provide mobility support, location awareness and low latency. Fog computing promises to overcome all the problems mentioned above.

IV. ISSUES IN CLOUD COMPUTING

Cloud computing has more advantageous characters. Even though the cloud is more flexible, cost effective, reliable due to lack of security concerns, it has got tremendous issues which need to be solved.

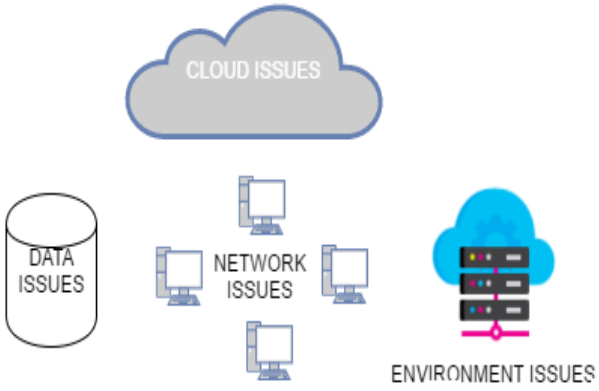

Fig. 1 Threats in Cloud

There are numerous threats within the cloud storage, we can categorize them into three major classification.

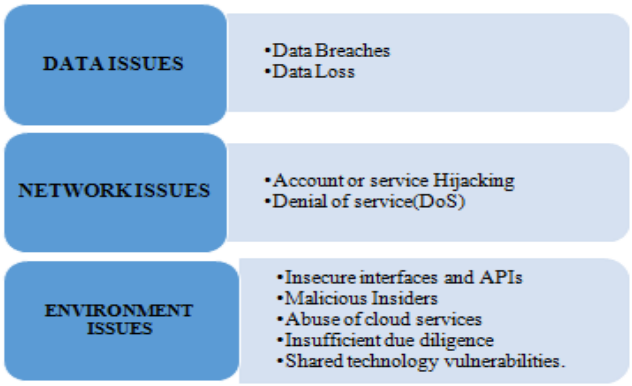

Fig. 2 Classification of threats in Cloud

A. Data Issues

Data threats are the vulnerability in the cloud which affects the data and causes more insecurity for the information which has been stored in the servers. When the data is available in unauthorized hands, it makes more impact on the sensitive data. Data are more precious piece of fact. Any issues to the data can bring down the organization and cause huge effect and crisis in the company.

- *Data Breach*

  Data breach is a traditional data issue, which leads to data leakage of organization and gives the consumers detail to the unauthorized users. The cloud providers are accountable to protect their consumer's data. This issue cause problem to the providers as well consumers.The main technique to overcome the data breach threat in the cloud level is encryption of the data [2],[3].Multifactor authentication can also resolve the problem [1]. Multifactor authentication (MFA) is authentication system which needs more than one strategy for validation from independent classifications of credentials to check the user's identity for access. In the Fog layer in order to avoid the data breach threat we need to use the Decoy Technique [10],[12], [14].The number of data threats occurred from 2005 to till 15th June 2016 is 6,284 [13].

- *Data Loss*

  Data loss is a data related threat. Data loss is actually losing of the data due to data deletion, data corruption, and fault in the data storage or unavoidable causality. In 2013, around 44 percent of cloud service providers have attacked by brute force method which lead towards data loss and data leakage [15].In both cloud and the fog level to avoid the threat is we need to have data backup and data recovery technique.

B. Network Issues

Internet becomes an important part in determining how effectively the communication of cloud works, with end users. Majority of the organization which is providing cloud solution is not considering providing security to the network is not so important. When we are not providing enough security to the network it causes vulnerabilities and results inter-network issues. Most harmful network hazards in cloud computing are account or service hijacking, and denial of service attacks.

- *Account Hijacking*

  Account or service hijacking is a network related problem for the cloud computing. Account Hijacking is the process where the attacker is try to hack the account in order to steal the identity of the particular user. Multi-level authentication at different levels is the solution to avoid account hijacking. Identity management for the user should be very strong, Network monitoring [5], Data Leakage Prevention Technology [8] Vulnerability Detection Technology [8].Combination of both the techniques decoy and data recovery [10], [11], [12] will help to overcome the threat in fog layer.

- *Denial of Service (DoS)*

  Denial of service is basically an incursion which denies the communication or the network resource for the particular user. There occurs delay in communications between the end user and cloud services. Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks [8].Alternative method for securing cloud from DDOS incorporates utilising intrusion detection system in VM. In this system when an IDS identifies as an unusual rise in inbound traffic, the targeted applications are moved to VMs hosted on alternative data servers.

C. Environment Issues

Most of the cloud users conclude cloud environment issue is the primary threat. The authority for controlling the cloud environment is mainly by the cloud service providers. Excluding service provider problems, few issues are particular to cloud computing for example providing insecure interfaces and APIs to users, malicious cloud users, shared technology vulnerabilities, misuse of cloud services and insufficient due diligence

- *Insecure Interface and API'S*

  Inadequate group of APIs and interfaces causes various security problems in cloud. Cloud providers basically provide their APIs to third party to give services to customers. ·However, weak APIs leading to the third party having opportunities to access security keys and censorious information in cloud. With the security keys, the encrypted customer data in cloud can be read which results in, Loss of data Integrity, Confidentiality and Availability. Authentication mechanism and access control can avoid the problem in cloud level [4].In the fog layer we have to use the cryptographic hash function MAC MD5 HMAC.

- *Shared Technology Vulnerabilities*

  In Cloud computing the communication is provided by sharing of infrastructure, platform and software. In many cases, unique components such as CPU might not give cloud security needs such as perfect isolation. Mostly, many applications are designed without utilising trusted computing methods because of that there are chances of shared technology issues can arise that can be exploited in different ways [8].

- *Insufficient Due diligence*
  When customers has lack of knowledge regarding security methodology, Auditing, Log details, and Data storage, Data access, which leads in generating unspecified threat profiles in cloud. In certain cases, the developers and designers of applications might not be aware of their effects from deployment on cloud that can result in operational and architectural issues [7].
- *Malicious insiders*
  This issue is also called as the insider's threat. It is the most common threat in the cloud environment. The main reason for this issue is the curiosity of the employee to know sensitive information about different consumers. The employees try to steal the consumer's information to misuse. The prevention for this problem could be providing different access control for the employees. This is well known way to overcome this issue [4].
- *Abuse of cloud services*
  Many of the cloud users might not have enough knowledge to use the cloud services. In such scenarios there is a possibility, the cloud users try to misuse the cloud services and violate the contract provided by the cloud providers. The cloud users need to know the basic knowledge to handle the cloud servicers in order to avoid the abuse of cloud services issues. The service level agreement must incorporate the important polices of the organization need to be followed by the consumers.

The cloud computing is more popular; due to its vulnerabilities it has numerous issues. The issues need to be solved in order to provide secure platform for the users. It is really challenging to provide security for the cloud computing. There are fewer solutions are available for certain issues. The table below explains all the details regarding various issues and causes for the problems, available solutions in both the cloud and Fog computing. The threat column defines the top level issues and the cause column states the reasons for the problems. The cloud solution and fog solutions defines the various available solutions for the threats.

V. SOLUTIONS FOR THE THREATS IN CLOUD COMPUTING AND FOG COMPUTING

TABLE I

NO	THREAT	CAUSE	CLOUD SOLUTION	FOG SOLUTION
1	Data Breaches	Defect in physical and organisational structure, software design, and functional problems. Lack of authentication, Authorization, internal controls. Malice user who has virtual machine (VM) on the identical physical system who wants to access in unauthorized[1]	Multifactor authentication, Encryption of the data[2][3] Trusted computing which provides the data privacy and secured virtualization platform cloud.[16]	Decoy technique([10],[11],[12]) Biometric based authentication method can provide authentication to the users[17]
2	Data loss	Malice attacker [7] Deleting data unexpectedly, Data errors during read write operation. Misplace of data encryption key Defects in storage methods, or unforeseen events.	Data recovery, Data segregation, [6] Data backup Techniques: High Security Distribution and Rake Technology (HSDRT), Parity Cloud Service Technique (PCS),Cold and Hot Backup Service Replacement Strategy (CBSRS)[9]	Data recovery[3]
3	Account Hijacking	Theft of user details to control his account, information and services. The stolen details could be used to control cloud services. The network attacks such as: Fraud Phishing, Cross Site Scripting (XSS), Botnets Software vulnerabilities such as buffer overflow causes account or service hijacking	Multi-level authentication at different levels, Employing intrusion detection systems (ids) in cloud. Identity management, Inter-network monitoring [5]. Data Leakage Prevention Technology, Vulnerability Detection Technology[8]	Combining both the techniques(10],[11],[12])

4	Denial of Service	Denial of Service (DOS) is usually blocking the authorized users to access cloud resources. The vulnerabilities in web servers, databases, and applications results in delay of services and inadequacy of resources.	Intrusion Detection System (IDS) [8] is the most approved method for this type of issues. Preventive tools are, Firewalls, Switches, Routers	Not specific solution available
5	Insecure Interfaces and APIs	Weak Api's and third party control to the security keys.	Authentication mechanisms, Access controls[4]Open Web Application Security Project (OWASP) standards and guidelines to develop secure applications can help in avoiding such interfaces.[1]	Not specific solution available
6	Shared Technology Vulnerabilities	Sharing of infrastructure platform and software.	Implementing Isolation between VM's. Hypervisor should be secure to provide exact operation of other virtualization components[1],[8]	Not specific solution available
7	Insufficient Due Diligence	Lack of knowledge regarding Internal security systems, monitoring, activity records ,Data storage and Data access[1]	Risk assessment procedures for certain period of time, To evaluate the storage, flow, and process of data.[1]	Not specific solution available
8	Malicious Insiders	Eagerness to know the details of the customers	Access control[4], Separation of work in the management level[1]	User behaviour profiling[12] Decoy technique ([10],[11],[12])CUSUM ALGORITHM[14]
9	Abuse of Cloud Services	Not following the contract with the service providers.	Providing the Service level agreement (SLA) for end user and service provider.	Not specific solution available

The Fog computing provides solutions to most of the data related issues and insider attackers. The network issues and the Environmental issues are not having solutions in Fog level. The reason for not having enough solution for environmental issues and network issues is, the Fog computing is still in the evolving phase to provide security to the cloud computing [18].The improvements in fog computing will help us to implement the IoT. The basic idea of this technology is making all the physical devices connect with internet and make them smart to build the smart world. It is hypothetical situation to prove the security of fog. Fog computing has many challenges to overcome and provide the overall security to the users

VI. CONCLUSIONS

The various solutions will be providing the clear idea how to prevent the distinguish threats in the Cloud and Fog computing. This study, concludes that Fog computing is expansion of cloud with some prominent attributes for the service providers as well end user. Fog Computing is not a standby for Cloud Computing. This paper, explains cloud computing characteristics and security threats of cloud computing that is obvious motive for the growth of fog computing. According to the current state of big data, Fog Computing is functioning as the support to the current cloud computing systems. The upcoming Edge computing in Fog will offer new ideas, opportunities and solutions to network providers and end users. Fog computing will give better quality of service to various applications such as smart grid etc. Therefore Fog computing includes one more colour to IOT Worlds

REFERENCES

[1]. F. Y. Rashid, "The dirty dozen: 12 cloud security threats," InfoWorld, 2016. [Online]. Available: http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html. Accessed: Feb. 10, 2017.
[2]. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 384–394, Feb. 2014.
[3]. Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1 (2013): 5.

[4]. A. O. Joseph, J. W. Kathrine, and R. Vijayan, "Cloud security mechanisms for data protection: A survey," International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 9, pp. 81–90, Sep. 2014.
[5]. Roschke, Sebastian, Feng Cheng, and Christoph Meinel. "Intrusion detection in the cloud." Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on. IEEE, 2009.
[6]. Eken, Hanim. "Security threats and solutions in cloud computing." Internet Security (WorldCIS), 2013 World Congress on. IEEE, 2013.
[7]. Z. Tari, "Security and privacy in cloud computing," IEEE Cloud Computing, vol. 1, no. 1, pp. 54–57, May 2014.
[8]. Charanya, R., et al. "Levels of security issues in cloud computing." International Journal of Engineering and Technology 5.2 (2013): 1912-20.
[9]. Rawat, Neha, et al. "Data Security Issues in Cloud Computing." Open Journal of Mobile Computing and Cloud Computing 1.1 (2014): 9-17.
[10]. Sonali Khairnar ., "FOG COMPUTING: A NEW CONCEPT TO MINIMIZE THE ATTACKS AND TO PROVIDE SECURITY IN CLOUD COMPUTING ENVIRONMENT," International Journal of Research in Engineering and Technology, vol. 03, no. 09, pp. 124–127, Sep. 2014.
[11]. Ashwini, Thogaricheti, and Mrs Anuradha SG. "Fog Computing to protect real and sensitivity information in Cloud."
[12]. Raut, Rajashri, et al. "Fog Computing Using Advance security in Cloud." International Journal of Engineering Research and Technology. Vol. 3. No. 2 (February-2014). ESRSA Publications, 2014.
[13]. "ID theft resource center 888-400-5530," ID Theft Center, 2017. [Online]. Available: http://www.idtheftcenter.org. Accessed: Feb. 10, 2017.
[14]. Arbat Rashmi Vinod ., "HINDERING DATA THEFT ATTACK THROUGH FOG COMPUTING," International Journal of Research in Engineering and Technology, vol. 03, no. 09, pp. 427–429, Sep. 2014.
[15]. T. of Use and P. Policy, "Security as A service – cloud security provider," 2010. [Online]. Available: https://www.alertlogic.com/. Accessed: Feb. 10, 2017.
[16]. Kong, Jinzhu. "A practical approach to improve the data privacy of virtual machines." Computer and information technology (cIT), 2010 iEEE 10th international conference on. IEEE, 2010
[17]. Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International Conference on Wireless Algorithms, Systems, and Applications. Springer International Publishing, 2015.
[18]. Wang, Yifan, Tetsutaro Uehara, and Ryoichi Sasaki. "Fog computing: issues and challenges in security and forensics." Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual. Vol. 3. IEEE, 2015.
[19]. Tiwari, Pradeep Kumar, and Bharat Mishra. "Cloud computing security issues, challenges and solution." International Journal of Emerging Technology and Advanced Engineering 2.8 (2012): 306-310.
[20]. "NIST page,". [Online]. Available: http://nvlpubs.nist.gov. Accessed: Feb. 10, 2017.
[21]. "NIST computer security resource center," 2017. [Online]. Available: http://csrc.nist.gov. Accessed: Feb. 10, 2017.
[22]. Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International Conference on Wireless Algorithms, Systems, and Applications. Springer International Publishing, 2015.
[23]. Wang, Yifan, Tetsutaro Uehara, and Ryoichi Sasaki. "Fog computing: issues and challenges in security and forensics." Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual. Vol. 3. IEEE, 2015.
[24]. Tiwari, Pradeep Kumar, and Bharat Mishra. "Cloud computing security issues, challenges and solution." International Journal of Emerging Technology and Advanced Engineering 2.8 (2012): 306-310.
[25]. "NIST page,". [Online]. Available: http://nvlpubs.nist.gov. Accessed: Feb. 10, 2017.
[26]. "NIST computer security resource center," 2017. [Online]. Available: http://csrc.nist.gov. Accessed: Feb. 10, 2017.

