Fog Computing: Defense from Security Threats Cyber Attacks and Prevention

[1]Khemendra Kumar Gangwar, [2]Dr. Rajesh Yadav,
[1]PG Student M.tech CSE, [2]Associate Professor GITAM,
[1]Computer Science Engineering,
[1]Ganga institute of Technology and Management, kablana , haryana, India

Abstract : **-** Fog computing is currently daily in favor of all sorts of business units. We can access and store all types of application and data in Fog . As it comes up with a lot of facilities, it becomes exhausting to entrust security. Fog computing provides different security approaches than conventional slant like cryptography. By observing actions and reactions of user whereas accessing the info, we will realize the abnormal behavior. If unauthorized access detected even after prying difficult queries verification, then we can introduce disinformation attack and provide the fake worthless information to attacker. It will be useful to regulate effectiveness of data. Experiments done by author, shows that, this method might give extraordinary level of security for knowledge in Fog computing atmosphere. Fog computing is preventive disinformation attack.

***IndexTerms* –: Cryptography1, Fog computing2, Entrust security3,**

I. INTRODUCTION

Traditional business applications and platforms square measure terribly difficult and big-ticket. They need a data centre, complex software's and a team of experts to run them. So Fog computing becomes more and more popular because of its flexibility, cost effectiveness, easy deployment. The Fog Security Alliance (2009) declares that the " Fog describes the utilization of a group of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. As Fog computing offers such a large amount of advantages to businesses, its security and trustworthiness has always been in question. Security is a very vital demand for any IT application, as nobody wants their data to be accessed by unauthorized users. There are many Fog security methods available for external threats. The methods available for external attack have not been able to prevent data theft. Van Dijk and Juels have shown that the solutions like encryption and decryption are not sufficient data protection mechanism when used alone by using fully homomorphism encryption. The ability to leave no trace of an attack is the biggest security challenge for this Fog environment. The lack of resources and evidence makes it difficult to find Fog -based cyber attacks. Data theft attack detection is very difficult when attacker is insider. According to the 2011 Cyber Security Watch Survey conducted on 607 businesses, government executives, professionals and consultants, 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the corporate executive attacks were a lot of expensive and damaging to organizations Insiders may get the credentials of authorized user of by password sniffing or key logger etc for accessing system or network. Rocha and Correia show that it's terribly simple to steal passwords for a malicious corporate executive of the Fog service provider .Another case can be like insider may attack on system by taking advantage of victim's unwise trust like person leaves terminal open or permitting to use terminal to workfellow are often create as masquerade attack. So that service provider cannot get plan of Associate in nursing attack on the system as a result of offender has identity of licensed user. The most common method wont to observe masquerade attack is to stay record of user behaviour and to search out abnormalbehaviour. In this approach, user's actions are profiled to form a baseline of normal behaviors. Salvatore J. Stolfo and Malek Ben Salem proposed a unique approach to secure Fog by mistreatment decoy info technology that they known as as Fog Computing

This technique can use the Mac , IP address, Time Slot and AES formula.

The MAC address improves the chances of identifying attacks details. , AES algorithm will encrypt the requested Password by the User. And Time Slot Use for attacker Attacks the Data.

1.OBJECT

Breach of security happens from outside of the organizations additionally as from at intervals. Consistent with Cyber Security Watch Survey conducted in 2017 on 700 professionals, businesses, consultants and government executive's insiders are chargeable for 22% of the total cyber-attacks. 34% of the respondents contemplated that the attacks by the insider were additional expensive and damaging to organizations. The foremost common within attacks are unauthorized access to and use of company data (64%), unplanned revealing of personal or sensitive information (58%), virus, worms, or alternative malicious codes (38%), and larceny of belongings (34%). The Fog computing vulnerabilities to malevolent corporate executive are: inexact roles and responsibilities, poor social control of role definitions, non pertinences of need-to-know principle, AAA vulnerabilities, system or OS vulnerabilities, and scant physical security procedures, unusefulness of process information in encrypted kind, application vulnerabilities or poor patch management. Malicious disruption of an organization's sensitive data resources might lay the complete victim organization's operation on the road. There are three kinds of Fog -related corporate executive threats: the villain administrator, insiders who exploit Fog vulnerabilities, and also the insiders who use the Fog to conduct infamous activity. Villain administrator has privilege to steal unprotected cases, brute-force hit over passwords, and transfer customers' information from the casualty organization. Insiders who utilize Fog vulnerabilities try to gain unauthorized access to confidential information in an organization; they may create a fortune by merchandising the sensitive data, or use the data for his or her future businesses. Insiders who use the Fog to conduct wicked activity perform attacks beside its own employer's IT infrastructure. While the insiders are conversant in the IT operations of their own corporations, the attacks are usually tough to be derived victimization rhetorical analysis.

1.2 EXISTING SYSTEM

Fog computing guarantees to considerably amendment the means we have a tendency to use computers and access and store our personal and business info. With these new computing and communications paradigms arise new information security challenges. Existing information protection mechanisms like cryptography have unsuccessful in preventing information felony attacks, particularly those perpetrated by a business executive to the Fog supplier. Much analysis in Fog computing security has targeted on ways that of preventing unauthorized and illegitimate access to information by developing subtle access management and cryptography mechanisms. However these mechanisms haven't been ready to stop information compromise

2. PROPOSED SYSTEM

We propose a different approach for securing data in the server using offensive decoy technology. We monitor data access in the Fog and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a server environment. We propose a completely different approach to securing the server using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

3. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules:

1. Fog Computing.
2. Decoy documents.

Fog computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It divides into three type

1. Application as a service.
2. Infrastructure as a service.
3. Platform as a service.

Fog computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.

2. Cost is claimed to be reduced and in a public Fog delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

3. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

4. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

5. Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

6. Utilization and efficiency improvements for systems that are often only 10–20% utilized.

7. Reliability is improved if multiple redundant sites are used, which makes well-designed Fog computing suitable for business continuity and disaster recovery.

8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

9. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private Fog installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

10. Maintenance of Fog computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

2. Decoy documents.

We propose a different approach for securing data in the Fog using offensive decoy technology. We monitor data access in the Fog and detect abnormal data access patterns. We launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) Confusing the attacker with bogus information..

3. CONCLUSIONS

Fog security is one of the major important point to be considered in Fog computing. Masquerade or insider is the person who behaves as a normal user by stealing credentials of authorized person. Insider attack is very difficult to diagnose. So the given approaches help to provide the higher and intelligent level of security in terms of insider attacks. The approaches are based on the predefined user behaviours and monitoring as well as profiling it using decoys. In case of abnormal behaviour i.e. insider attack, decoy documents are presented to the user which is actually a bogus information. These decoy documents can also be checked to detect such insider attack. Thus using these approaches the very important and hard to detect attack i.e. insider attack can be handled and the data can be very well secured. The false positive percentage for these approaches is very low..

4 ACKNOWLEDGEMENT

For all the efforts behind the paper work, I first & foremost would like to express my sincere appreciation to the staff of Dept. of Computer Sci.& Engg., for their extended help & suggestions at every stage of this paper. It is with a great sense of gratitude that I acknowledge the support, time to time suggestions and highly indebted to my guide associate Professor Dr . Rajesh Yadav and Dr. Neetu Sharma (HOD). Finally, I pay sincere thanks to all those, who indirectly and directly helped me towards the successful completion of the this paper.

5.REFERENCES

1. *Data Center Companies*, Jul. 2017, [online] Available: https://www.datacenters.com/directory/companies.

2. F. Bonomi, R. Milito, J. Zhu, S. Addepalli, "Fog computing and its role in the Internet of Things", *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, pp. 13-16, Feb. 2012

3 *Cisco Delivers Vision of Fog Computing to Accelerate Value from Billions of Connected Devices. Press Release*, Jul. 2017, [online] A

4 M. Aazam, E. N. Huh, "Fog computing: The cloud-IoT/IoE middleware paradigm", *IEEE Potentials*, vol. 35, pp. 40-44, May 2016.