Paper Presented in: '2 day State Level workshop on Cyber Fest 17', conducted by: 'Department of Computer Engineering, Marathwada Mitra Mandal College of Engineering, Pune' on 22-23 Feb 2017

A SURVEY ON FOG COMPUTING SECURITY ISSUES AND CHALLENGES

B Vinayak[1], P Kavita[2,] Pranav B[3], N.P Neha[4]

[1]*(Dept of Computer Engg, MMCOE, Savitribai Phule Pune University, Pune, India)*
[2]*(Dept of Computer Engg, MMCOE, Savitribai Phule Pune University, Pune, India)*
[3]*(Dept of Computer Engg, MMCOE, Savitribai Phule Pune University, Pune, India)*
[4]*(Dept of Computer Engg, MMCOE, Savitribai Phule Pune University, Pune, India)*

Abstract— *The already prevailing problems in cloud computing such as abeyance, curtailed mobility, absenteeism of location awareness have given birth to a decentralized computing framework known as fog computing/fogging. It is the prolongation of cloud at the periphery of the network. To curtail the amount of data transferred to cloud for processing, analysis and storage is the objective of fog. The aggravation of ubiquitous user demand and gargantuan mobile traffics is dexterously addressed by fog computing. This survey discusses the fog computing architecture security and privacy issues in fog, algorithms and challenges for fog computing.*

Keywords—Fog computing; Sensors; Cloud; Big data; CISCO; VPN

1. INTRODUCTION

Smart phones and gadgets are becoming key trends of this era which subsequently demands handling of unprecedented variety and volume of data, its storage and the corresponding quick services towards the user's edge. But consecutively it has also introduced challenges like security, managing traffic of many ubiquitous devices and mitigating different threats and attacks. Fog computing- a new technology, coined by CISCO proves to be a promising solution for managing these UbiCom devices. It is an extension to the cloud computing for decentralizing the devices connected in the network towards user to optimize the user experience by improving the quality of service. It also provides security and reliability of the data, reduction in latency and improves the performance by making services available to the user anytime anywhere. Fog computing helps in real time analysis, computing Bigdata and in accelerating the decision making.

2. BENEFITS OF FOGCOMPUTING

Extending the services of the cloud closer towards the devices has enlarged the business possibilities like

- Greater Business Agility: Fog customizes the services and tools as per the business requirements and hence Fog Computing is prevailing these days
- Secure Services: Fog provides better security but it is also prone to attacks. So, research in recovery management and security algorithms for fog computing must be done
- Analysis of Data: Fog analyzes the data locally before it could take the services of the cloud and hence it provides ease of use.
- Reduced operating cost: Fog Computing provides cost effective strategy in terms of proper and easy resource management and utilization [1]

3. ARCHITECTURE OF FOGCOMPUTING

The proposed fog computing system comprises of the following components:

A. The Cloud Platform:

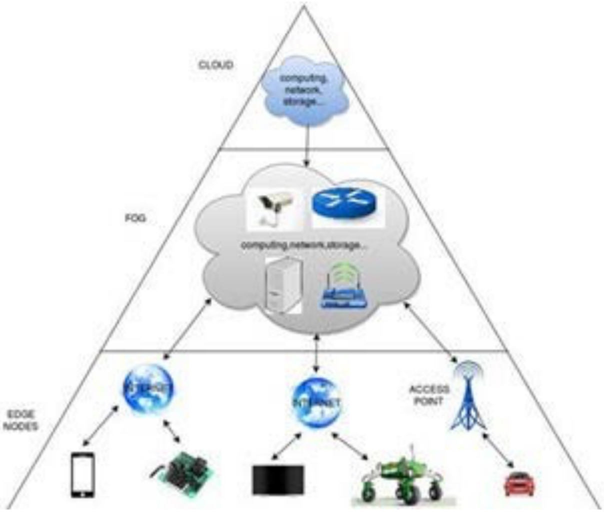
The data produced by the fog nodes is received, analyzed and aggregated by the cloud platform. This aggregated data is then used to gain business insight. These insights help generate new application rules for the fog nodes.

B. The Fog Platform:

The fog platform comprises of the fog nodes which include routers, switches, wireless access points, video surveillance, cameras, servers, etc. Any device which is capable of storing and computing the data generated by the edge devices and has a network connectivity can be a fog node. The fog nodes can be deployed at any place which possesses a network connection. All the fog devices are interconnected, each of which is connected to the cloud.

C. The Edge Nodes:

The fog extends the cloud paradigm towards the edge devices like sensors, mobiles, smart televisions, cars, robots and other embedded devices which have a network connectivity. The data produced by the edge devices is collected and processed by the fog nodes.



4. SECURITY AND PRIVACY ISSUES

Fog computing provides flexibility and it allows the users to access data from anywhere but it also proliferates security issues, privacy issues and authentication issues to the user. Creating a trust zone is very necessary for securing data. Smart phones and gadgets has their own IP, which can be tampered by malicious user. Intruder can get control over the data on could. Another few challenges like ARP spoofing, man-in-the-middle-attack, IP spoofing, DNS poisoning, flooding, DoS attack makes utilization of devices difficult. Building a secure infrastructure over cloud is an important aspect. It becomes more challenging to secure data while it migrates from fog nodes towards cloud. Few threats to data over cloud are as follows: [8]

1. Man-in-the-middle cryptographic attacks: In this attack communication between two parties is manipulated maliciously. Attacker secretly listens to communication. Some possible solutions for these attacks are using one time passwords (OTP), forensic analysis and verifying trust by using authorized certificates.
2. ARP spoofing: Attacker links its MAC address with the IP address of server on the network and maliciously tampers or falsifies ARP packets.
3. IP spoofing: Attacker gains an unauthorized access over the network. In this attack, IP packets are manipulated by the attacker.
4. DNS poisoning: In this Domain Name System is corrupted due to which data traffic is diverted to the intruder's system. The target is provided with the fake information which will mislead the target system.
5. Dos attack: In Denial-of-service attack, attacker overloads the cloud service system by multiple requests and makes the server unavailable for providing service to the host systems
6. Authentication attack: Authentication is the process of verification. In this attack, attacker tampers the verification process to steal the sensitive information.
7. DDOS attack: In Distributed Denial of Service attack a single system is targeted by multiple systems. Traffic comes from multiple resources.
8. ARP Cache Poisoning: Attacker sniffs over the network and monitors the traffic and spoofs the ARP packets.
9. Session hijacking: Attacker captures the cookies and tries to obtain parts of the session established between the host system and the server
[8]

5. ENCRYPTION ALGORITHMS AND TECHNIQUES

Encryption algorithms convert the sensitive data to cipher text to preserve its confidentiality. Even if the intruder gets access to the fog, he won't be able to normally read the data.

A. *Symmetric Algorithms*

It is the type of encryption where encryption and decryption utilizes the same key. Symmetric key cryptographic systems handle high rates of data throughput. The ciphers can be composed together to produce a strong key. Even if the symmetric Key algorithms are currently unbreakable, they fail against brute force attack. The Brute force attack runs entire space of keys to obtain the right key, i.e. it will try 2^n combinations for n-bit key. Larger the key size greater is the security. Increase in the key size increases the time required to guess the key on a normal machine decreasing the possibility of successful attack. Due to the arrival of quantum computing the time required for the attack to be performed is very less, even the large keys can be guessed in very less time. Some famous symmetric key algorithms are:

a. Data Encryption Standard (DES): 64-bit
b. Advance Encryption Standard (AES): 128,192 and 256 bit
c. Triple DES (TDES): 168-bit
d. Blowfish: 32-bit – 448-bit

B. *Asymmetric Algorithms*

It includes a pair of keys, the public key and the private key. Encryption is done using the public key and private key is used for decryption. Same key cannot be used for both, Encryption and Decryption. Asymmetric key cryptographic systems are good for digital signatures and key exchange use cases. The effectiveness of asymmetric key depends on mathematical function used in the public key. Such functions consume much time. Thus, asymmetric algorithms keys are more resistant to attacks than the symmetric keys.

Famous asymmetric key algorithms are:

- Ranold Shamir Adleman (RSA): 1024, 2048, 3072-bit
- Diffie-Helman key exchange

C. *User behavior profiling and Decoy Systems*

The current user's behavior is compared with his past behavior and if there exists a change more than a predefined threshold limit then the user is suspected to be an anomaly. The user must answer the security questions. If he provides correct answer within the threshold limit and attempts, then only he is treated as normal user. This can only become possible if the behavior profile is created for each user. As there are numerous users, it becomes a cumbersome task to manage their profiles.

Decoy system generates the falsified but related data for the original files for misleading the attacker so that he should not be able to identify between the actual and the decoy files.

6. SECURITY REQUIREMENTS AND KEY CHALLENGES FOR FOGCOMPUTING

Services for Internet of Things

Cloud cannot connect to thousands of different types of sensors and smart products spread across the globe. Capturing IoT with Fog Computing power requires scalability for heterogeneous types of devices, sometimes in harsh environmental conditions for sensors. New types of communication protocols are required. Enhanced physical and cyber security is fundamentally expected. Handling volume, variety and velocity of data becomes a key challenge. [1]

Transparency Enhancing Technologies Heterogeneous type of data gets dumped over the cloud on daily basis. Most of the data stores used for storing and managing data uses the concept of auto sharding. In this once the data is dumped over the cloud by user, he loses the control over the data and all the data storage tasks are taken care by the data stores. But it sometimes becomes important for user to know where his data is getting stored and which service provider is handling that request. Hence Transparency Enhancing Techniques are required for customer profiling. [5] Authentication, Authorization and Accounting Kerberos Authentication protocol is used for this purpose. Basically, a mechanism is required to monitor the various users. The Access control levels according to the user types and their corresponding permissions for data access should be monitored. Authenticating users based upon the credentials they have provided is a most fundamental security requirement for any fog computing application. [5]

Digital Forensics

A scalable storage is required over cloud which should be tampering- proof. The Audit logs, Service Level Agreements, different flags and forensic evidences should be maintained for better security. [5]

Location Awareness

To provide the services and for collecting data from devices, Fog Computing must locate the devices for sending and receiving data. So globally positioning the objects and the devices is necessary.

7. CONCLUSION

In this paper, we have outlined the vision of fog computing, its benefits and subsequent challenges. The security of data present over cloud and fog needs to be secured. Though fog computing is prevailing for business there is a need and scope for research in security mechanism for better services and utilities.

REFERENCES

[1] White paper by CISCO on ,”Fog Computing and the Internet of Things: Extend the cloud to where the things are,” pp-1-6,2015.

[2] White paper by CISCO on ,”Cisco Fog Computing solutions: Unleash the power of the Internet of Things,” pp-1-6,2015.

[3] A joint white paper by Symantec and Vmware on “ Securing the cloud for the Enterprise”

[4] Evan Stojmenovic, Sheng Wen, “The Fog Computing paradigm: scenarios and security issues”, proceedings of the IEEE Federated Conference on Computer Science and Information Systems, 2014,pp. 1-8.

[5] Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

[6] M.T. Dlamini, H. S. Venter, J.H.P. Eloff, “Security of Cloud Computing seeing through the Fog”

[7] Salvatore J. Stalfo, Malek Ben Salem, Angelos D. Keromytis, “ Fog Computing: mitigating insider data theft attacks in the cloud”, pp. 125- 128, IEEE Security and Privacy Workshops, position paper, 2012

[8] Tadapaneni, N. R. (2016). Overview and Opportunities of Edge Computing. Social Science Research Network.

[9] Chirag Modi, Dhiren Patel, BhaveshBorisaniya, Avi Patel, MuttukrishnanRajarajan, “ A survey on security issues and solutions of different layers of cloud computing”, Springer Science+ Business MediaNew York, 2012, Pp. 561-592

[10] Weisong Shi, Jie Cow, Quan Zhang, Youhuizi Li, LanyuXu,”Edge Computing: Vision and Challenges”, IEEE Internet of Things Journal, Vol.3, No. 5, October, 2016, Pp. 637-646

[11] KshamataShenoy, Prachibhokare, Unnatipai,”Fog Computing: Future of Cloud Computing”, International Journal of Science and Research(IJSR), Volume 4 Issue 6, June 2015, ISSN: 2319-7064, pp.55-56

[12] PanimalarS, A., Dharani, N., Aiswarya, R., & Shailesh, P. (2017). Cloud Data Security Using Elliptic Curve Cryptography.