International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7400
***Article Received**: 02 May 2023 **Revised:** 24 June 2023 **Accepted:** 22 July 2023*

Security Issues in Service Model of Fog Computing Environment

[1]Harikrishna Bommala, [2*]Sireesha Vikkurty, [3]K. Ramesh Babu, [4]Bhargavi Peddi Reddy
[1]Department of Computer Science and Engineering
KG Reddy College of Engineering & Technology
Moinabad, Hyderabad, Telangana, India
haribommala@gmail.com, haribommala@kgr.ac.in
[2]Department of Computer Science and Engineering
Vasavi College of Engineering ,
Hyderabad, Telangana,, India
v.sireesha@staff.vce.ac.in
[3]Department of Computer Science and Engineering
Vidya Jyothi Institute of Technology
Hyderabad, Telangana,, India
krubabu@gmail.com
[4]Department of Computer Science and Engineering
Vasavi College of Engineering ,
Hyderabad, Telangana,, India
bhargavi@staff.vce.ac.in

Abstract—Fog computing is an innovative way to expand the cloud platform by providing computing resources. The platform is a cloud that has the same data, management, storage and application features, but their origins are different because they are deployed to different locations. The platform system can retrieve a large amount, work in the field, be fully loaded, and mount on a variety of hardware devices. With this utility, Fog Framework is perfect for applications and critical moments. Fog computing is similar to cloud computing, but because of its variability, creates new security and privacy challenges that go beyond what is common for fog nodes. This paper aims to understand the impact of security problems and how to overcome them, and to provide future safety guidance for those responsible for building, upgrading and maintaining fog systems.

Keywords-security; privacy; Fog Computing; Security threats; Cloud-to-fog security.

I. INTRODUCTION

Fog is an IT organization that manages and stores data within the cloud infrastructure. With the rapid development oflaptops, smart metrics, smart homes or cities, connected cars and great phone networks, everything is connected and smart. This is known as the Internet of Things (IoT) [1,2]. The cloud management system has a significant impact on the development of Internet of Things (IoT) devices, which increases the amount of data (depending on the amount, flexibility, and speed) resulting from an increase in the number of devices [3]. As you know, high-tech devices face issues related to computing power, battery life, storage, and bandwidth, which in turn affect service quality (QoS) and user experience. Fog's goal is to provide solutions to this problem. This is achieved by building a new platform that is gradually distributed between the cloud systems and between cloud systems and end-user devices [4]. The platform can filter, integrate, process, analyze and exchange data, save time and communication resources [5]. This new environment was created by Cisco and is called fog calculations. Cloud computing offers many benefits to individuals and organizations by offering the cheapest and cheapest services [6]. This white paper describes some of the security and privacy issues of fog operation, reviews existing fog management activities and related activities in the region, and identifies security and privacy issues.

II. FOG COMPUTING OVERVIEW

The definition of Fog is defined as "a situation where many distributed devices communicate with each other and work with the network to perform storage and management functions without the involvement of a third party." They can be implemented to support the network.Programmed features or new services, and applications are running in sandbox mode.Users who lease their devices to receive these services receive an incentive to perform them [1]. Most infrastructure and developers will provide ample resources to expand the network.Even though, as with all communication systems, merchants Con integrated computer devices face the threat of cyberbullying, usually provide an operating system and then additional security measures [7,8]. Many researchers have considered security, actual philosophy, or design in the development of these distribution systems, but they give system still y the baby is in danger and the security is facing the fog. I don't fully understand the challenge [9].

Fog node: The availability of scalable devices, and therefore the rapid development of standardized systems using cloud technology, has led to the implementation of cloud inflation on the market [10]. The drop could also be a new design of the fall design. This can be a good alternative to node-JS because of its ability to provide services and its proximity to network bytes [11]. As the lowest data center, Cloudlet can provide retrieval access to mobile phones near low latency and data size [12]. With cloud technology, Cloudlet can be upgraded and switched easily.

Deployment and Services: Fog computation requires predictions that cloud service delivery products will usually fall into three categories [13]. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud Security has identified 12 major security issues, including some browsers, including issues directly related to the need for cloud management, sharing and distribution [14]. Being a cloud-like environment and the same threat can affect the Fog platform (see Fig. 1).

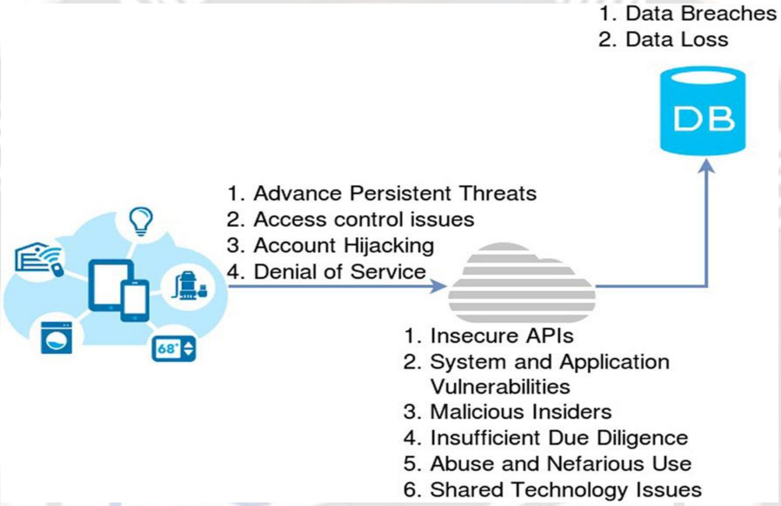
1. Data Breaches
2. Data Loss
DB
1. Advance Persistent Threats
2. Access control issues
3. Account Hijacking
4. Denial of Service
68°
1. Insecure APIs
2. System and Application Vulnerabilities
3. Malicious Insiders
4. Insufficient Due Diligence
5. Abuse and Nefarious Use
6. Shared Technology Issues

Figure 1. Potential security issues of Fog Platform inherited from Cloud computing.

The cloud platform issues may affect the Fog platform [15].

a) High Performance Threat (HPT): HPT is a cyber-attack that aims to integrate into collaboration tools with the aim of getting better data and assets.
b) Access Control Indicators (ACI): ACI enables unrestricted management and allows users to collect data and permissions to enter computer code and change settings.
c) Account Theft (AT) is a place where nurses trainers attack with the intent of stealing user accounts for malicious purposes. Stealing personal data can be a technical ploy to steal an account.
d) Denial of Service (DoS) is a place where legitimate users avoid using the system (data and applications) by flooding the system's borders.
e) Violation of Quadratic Data (VQD) after the release or interference of personal data, protection, or personal information by training nurses in charge of nursing.
f) Data Loss (DL) occurs when data is accidentally deleted (or accidentally) from a system. It does not have to be a cyber-attack; it can happen through natural disasters.
g) Unsecured Application (UA) some cloud providers are exploring application programming interfaces (APIs) for their customers to use. The protection of these applications is very important for enforcing the protection of the application.
h) Application Extended (AE) system error due to the standard computer code system used by an attacker to break into and destroy the system.
i) The Chief Business Officer (CBO) may be a user who accepts access to networks and systems but is destined to commit a crime intentionally.
j) Insufficient Efficiency (IE) usually occurs after the company accelerates support, design, and implementation of each system.
k) Abuse usually occurs after the supply of cheap equipment, and users use it to perform malicious acts.
l) Advanced Technology Solutions (ATS) are caused by shared resources, platforms, or applications. For

example, the original hardware component may not be designed to provide robust protection properties.

III. SECURITY AND PRIVACY ISSUES

A. Authentication by Trust

In cloud computing readying, knowledge centers area unit sometimes closely-held by cloud service suppliers [16]. However, fog service suppliers will be totally completely different parties.

I. Net service suppliers or wireless carriers, United Nations agency have management of home gateways or cellular base stations, could build fog with their existing infrastructures.
II. Cloud service suppliers, United Nations agency wish to expand their cloud services to the sting of the network, may additionally build fog infrastructures.
III. End users, United Nations agency own a neighborhood non-public cloud and need to cut back the value of possession, would love to show the native non-public cloud into fog and lease spare resources on the native non-public cloud.

Trust Model: Secure products are not found in e-commerce, peer-to-peer (P2P) and user reviews. Creating a fog that reflects name expression can lead to problems such as 1) how to overcome it, stubbornness, identity, 2) dealing with selfishness and mistakes, and 3) discipline and dignity. Unit-dependent solutions such as Secure Element (SE), Secure Deployment System (SDS), and Platform Module (PM) can provide reliable support for IT applications [17].

Rogue Fog Node: Low noise fog indicates that it is cool and becomes a fog device like a party alarm that connects the user with it. For example, in an insane attack, an agent may be allowed to convict a criminal offense, but that may be more than just a legitimate crime [18]. This feature demonstrates the benefits of a built-in attack on cloud computing when the gateway is at risk or has to be replaced accidentally. The presence of fake packages poses a serious threat to the security and privacy of your data [19]. This problem is difficult to solve for many reasons. 1) Complex security environment requires a reliable management system. Negative access point (AP). His method uses roaming time between DNS server users to look for client AP scams [20].

Authentication: Authentication is a major concern for the security of vulnerable PCs, as the presence of an anti-fog node poses a serious threat to users. The nodes are not authenticated at different precipitation mode levels, because of a major security issue for the deposition computer. PKI authentication is low cost and offers an inexpensive, secure, and easy-to-use solution to basic failures of basic wireless networks. Confirmation in confined spaces requires physical contact. Additionally, NFC may be accustomed to changing the authentication method in a cloud environment. Similar to the physical display on laptops and cloud computing, technology is also useful, for example for fingerprints, screens, touches, or key confirmations.

B. Network Security

Due to the prevalence of wireless fog security can be a major issue in cloud communications. Examples of attacks include accidental attacks and suicide attacks [5, 6. The attack was linked to a wireless network space outside the research center. In most cases on the network, you should always trust your management system through NetworkManager and share management traffic and business quality over the network. HIR leasing streamlines implementation and management, increases corruption, and significantly raises prices across multiple cloud sectors. Or how does SDN promote the safety of hog nets? 1) Internal Data Investigation and Protection System (IDS): Cloud-Watch uses open sources to send traffic to security-protected applications or IDSs. 2) VLAN-priority traffic and processes and malicious distribution. 3) Managed network service: An improved AN SDN access system with Open Flow support is available. 4) Network: A cloud-filled home network extends to visitors if the network and visitors are designed quickly to avoid stress [6]. We plan to launch a secure wireless service while asking the original host to perform a quality verification of the wireless area network in the cloud. Different guests are allowed and an account is required to change the guest's weight.

C. Secure Data Storage

When user data is released and the user of the UN agency uses this information to Nebel, then it poses a security threat similar to cloud computing. First of all, it is difficult to find responsibility for the data because external data is missing or accidentally changed. Second, the uploaded data is at risk for the benefits of unauthorized tools [1, 12]. To overcome this threat, data storage services are being developed that provide evidence to protect data in the cloud computing environment. With technologies such as Homomorphism Privacy Writing Privacy and Privacy Writing Principles, combined to ensure the integrity, data protection, and validation of the cloud storage system, users can store data stored on unattended servers trust them. View and facilitate the protection of cloud data protection. tests in relation to third-party investigators (TPA). Homomorphic methods and random techniques provide personal protection for garbage dumps. The system of storing content that controls corruption and managing data using text or networks to ensure responsible storage of education is a system that uses LT code, low cost, and return and data.It's fast, and the cost of communication is right [18]. This gives Maine the best summary of what you can get about cloud storage services. With Fog, there are new challenges in building efficient storage systems, achieving low latency, supporting efficient operation, and addressing cloud interactions.

D. Secure and Privacy for Data

The biggest problem with using cloud management is finding a secure personal computer to send to your cloud site. Fog allows fog users to check the accuracy of the system and gain confidence in the load on the fog area [15]. The Pinocchio system allows you to use your browser to analyze old servers created by the server. By using Pinocchio, the client generates a public authentication key for the census. The service then analyzes the computer's statistics and validates it using a test key.

Data Search: Retrieving data for privacy, end-user knowledge must be encrypted before being sent to the cloud [16]. This challenges the use of educational economy services. The most important part of the function is the keyword search key. Researchers have developed a type of hidden writing technology that allows users to search securely without limiting the confidentiality of their knowledge.

Privacy: As end-user users use services such as computer control, wireless networks, and IoT, the loss of important data such as education, location, and usability becomes important [17]. Maintaining this privacy with cloud management is very difficult because the dust cloud will stop users and can retrieve large amounts of data from distant clouds over large networks. Personal technology, along with cloud, high-speed networks, wireless networks and online social networks, are integrated into a number of events.

Confidential Data: On cloud networks, privacy protection algorithms run between the cloud and the cloud, but the domains of these algorithms are usually limited to resources on larger devices [18]. The weak mist from the blades usually accumulates the basic knowledge provided by sensors and finishing equipment. Use techniques such as Homomorphic secret scripts to allow for the integration of protection hidden at source gateways instead of encryption. Personal information is only used when math questions are used to ensure that the confidentiality of staff with different professional opinions is not compromised by the pool of knowledge.

Secret Situation: Secret Situation In the calculation of the fog, the secret of the situation first refers to the secret situation of the buyer of the fog [19]. Fog buyers usually cease operations at the cloud nodes closest to the drop zone, so they determine that fog buyers are near and on opposite sides of the other nodes. Cloud buyers connect with important people or objects, jeopardizing the privacy of that person or object.

E. Access Control

Ensure access to enhanced security systems and user privacy. Power, management and access are often areas and are tolerated. The main solution is wrong when controlling the navigation buttons. Many of the most important public consultations are recommended to achieve total control. The search for a complete data access system depends on the material [21]. Under cryptographic policies, resource management systems rely on cloud compatibility to protect cross-site and business collaboration between different resources. With cloud computing, it is difficult to configure fogs to access cloud computing destinations and clients when limited resources are revealed.

F. Intrusion Detection

Intrusion detection technology is used to prevent attacks such as intrusions, flood attacks, port scans, and attacks on virtual machines and hypervisors [1]. It is also used in a system of expert monitors to monitor the frequency of readings and to detect the number of transients that can be damaged by an attack. Cloud computing allows you to determine tracking behavior by sending IDs to a cloud meeting team to monitor and analyze log files, location management, and user credentials. You can also send to your cloud network to look for malicious attacks such as DoS crawls and web crawls [22]. The service enhances the cloud-based security system that enables remote cloud-to-cloud delivery and provides communication between mobile devices, cloud computing, and cloud computing. Challenges also arise from the destruction of scale, the rapid and rapid fragmentation of national human organizations to meet the needs of microorganisms.

IV. CONCLUSION

The Fog system is integrated with end-user and cloud platforms to manage, store, and send large amounts of data while consuming a large amount of resources. This article addresses security and privacy issues in cloud management issues. This could be a new computer system that provides synthetic resources to the network infrastructure to include end users. This article addresses security issues such as data security, cyber security, and network security. Therefore, it is important to maintain appropriate security measures to overcome the limitations identified in this article. It also focuses on personal data issues. This may require new thinking to adapt to new challenges and changes. Therefore, decision support tools that can recommend security measures to developers can prevent the occurrence of vulnerabilities and protect the Fog platform from malware.

Acknowledgement We thank KG Reddy College of Engineering & Technology (Autonomous), Hyderabad and Vasavi College of Engineering (Autonomous), Hyderabad for the support extended towards this work.

REFERENCES

[1] Z. Wen, R. Yang, P. Garraghan, P., T. Lin, J. Xu, and M. Rovatsos, “Fog orchestration for the Internet of things services,” IEEE Internet Computing”., vol. 21, no. 2, pp. 16–24, 2017.

[2] A. Al-fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things : A Survey on Enabling Internet of Things : A Survey on Enabling Technologies, Protocols, and Applications”, IEEE communications surveys & tutorials vol.17, no. 4, pp.2347–2376, 2015.

[3] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in MCC ’12: Proceedings of of the MCC workshop on Mobile cloud computing, pp. 13–16, 2012.

[4] Ayesha Mariyam, SK. Althaf Hussain Basha, S.Viswanadha Raju. (2023). Long Document Classification using Hierarchical Attention Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 343 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2708

[5] Krishna, B. Hari, et al. "Security Issues In Service Model Of Cloud Computing Environment." Procedia Computer Science 87 (2016): 246-251.

[6] S. N. Gollaprolu Harish, B. Harish, and M. Shaik, “A Review on Fog Computing and its Applications,” Int. J. Innov. Technol. Explore. Eng., vol. 8, no. 6, pp. 358-369, 2019.

[7] X. Xu., Fu, S., Cai, Q., Tian, W., Liu, W., Dou, W., & Liu, A. X.,”.Dynamic resource allocation for load balancing in fog environment”. Wireless Communications and Mobile Computing, pp. 1–15, 2018.

[8] Mr. Kaustubh Patil. (2013). Optimization of Classified Satellite Images using DWT and Fuzzy Logic. International Journal of New Practices in Management and Engineering, 2(02), 08 - 12. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/15

[9] Bommala, H., Kiran, S., Pujitha, M., & Reddy, R. P. K. (2019). Performance of Evaluation for AES with ECC in Cloud Environment. International Journal of Advanced Networking and Applications, 10(5), 4019-4025.

[10] Chiang and T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, 2016.

[11] P. Hu, S. Dhelim, H. Ning, and T. Qiu, “Survey on fog computing: architecture, key technologies, applications, and open issues,” J. Netw. Comput. Appl., vol. 98, pp. 27–42,2017.

[12] Harikrishna, B., Kiran, S., & Deep, K. M. (2018). Network as a service model in cloud authentication by HMAC algorithm. International Journal of Advanced Networking and Applications, 9(6), 3623-3631.

[13] W. Jiafu, “Fog computing for energy-aware load balancing and scheduling in smart factory." IEEE Transactions on Industrial Informatics, vol. 14, pp. 4548-4556,2018.

[14] Bommala, H., Kiran, S., Deep, K. M., &Babu, V. S. (2019). Client Authentication as a Service in Microsoft Azure. International Journal of Engineering and Advanced Technology (IJEAT), 8.

[15] S. Agarwal, S. Yadav, and A. K. Yadav, “An architecture for elastic resource allocation in Fog computing,” Int. J. Comput. Sci. Commun., vol. 6, no. 2, pp. 201–207, 2016.

[16] Bommala, Harikrishna, and S. Kiran. "Sensitive Information Security in Network as a Service Model in Cloud-IPSec." International Conference on Emerging Trends in Engineering. Springer, Cham, 2019.

[17] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, “Optimal workload allocation in fog- cloud computing toward balanced delay and power consumption,” IEEE Internet Things J., vol. 3, no. 6, pp. 1171–1181, 2016.

[18] L. F. Bittencourt, D.-M. J., R. Buyya, O. F. Rana, and M. Parashar, “Mobility-aware application scheduling in fog computing,” IEEE Cloud Comput., vol. 4, no. 2, pp. 26–35,2017.

[19] Jones, D., Taylor, M., García, L., Rodriguez, A., & Fernández, C. Using Machine Learning to Improve Student Performance in Engineering Programs. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/101

[20] Bommala,Harikrishna, et al. "Survey on Machine Learning with Cloud Technology Preserving Privacy: Risks and Keys." Solid State Technology 64.2 (2021): 3135-3150.

[21] S. K. Mishra, D. Putha, J. J. Rodrigues, B. Sahoo, and E. Dutkiewicz, “Sustainable ServiceAllocationusing Metaheuristic Technique in Fog Server for Industrial Applications,” IEEE Trans. Ind. Informatics, vol. 14, no. 10, pp. 4497–4506, 2018.

[22] Sahoo, D. K. . (2022). A Novel Method to Improve the Detection of Glaucoma Disease Using Machine Learning. Research Journal of Computer Systems and Engineering, 3(1), 67–72. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/44

[23] R. Mahmud, R. Kotagiri, and R. Buyya, “Fog computing: A taxonomy, survey, and future directions,” in the Internet of everything, Singapore: Springer, pp. 103–130,2018.

[24] X. Q. Redowan Mahmud, KotagiriRamamohanarao, RajkumarBuyya, “Latency-aware Application Module Management for Fog Computing Environments”, ACM Transactions on Embedded Computing Systems, vol. 9, no. 4, pp. 1-21.2018.

[25] Pham and E. N. Huh, “Towards task scheduling in a cloud-fog computing system.,” in 18th Asia-Pacific network operations and management symposium, pp. 1–4, 2016.

[26] X. Masip-Bruin, E. Marín-Tordera, A. Alonso, and J. Garcia, “Fog-to-cloud computing (F2C): The key technology enabler for dependable e-health services deployment,” in 2016 Mediterranean ad hoc networking workshop (Med-Hoc-Net), pp. 1–5, 2016.