RESEARCH ARTICLE OPEN ACCESS

Fog Security Review: Threats, Countermeasures, and Future Research Directions

Arushi Shrivastava, Khushboo Panjwani, Goldi Soni

MCA 1st Semester, Amity University, Raipur
MCA 1st Semester, Amity University, Raipur
Assistant Professor, Amity University, Raipur

ABSTRACT

A key component of processing data closer to the network edge is fog computing, an extension of cloud computing that offers improved scalability, real-time processing capabilities, and reduced latency. But as fog computing becomes more widely used, so do the security issues that come with it. This paper provides an extensive overview of the risks that fog security is now facing, from denial-of-service assaults and data breaches to privacy issues in dispersed environments. It examines current defences against fog's distinct architecture, such as intrusion detection systems, access control methods, and encryption protocols. Additionally, the decentralized nature of fog computing makes it more difficult to guarantee security across a variety of environments and devices, which makes threat mitigation efforts much more challenging. This review also examines the gaps that exist between the state-of-the-art security solutions and the rapidly changing fog computing world, highlighting areas that require more investigation. Improving privacy-preserving methods, creating strong authentication systems, and resolving the scalability issues related to extensive fog deployments are important future directions. The need for creative, adaptable security solutions will only grow as fog computing develops, demanding ongoing attention from both academics and business. The purpose of this study is to give researchers and practitioners who are working to secure fog computing infrastructures, a basic understanding.

Keywords: Fog Computing, Fog Security, Distributed Architecture, Threats and Countermeasures, Privacy Preserving Techniques, Intrusion Detection Systems

I. INTRODUCTION

Fog computing has become an essential component of cloud computing due to the Internet of Things' (IoT) explosive growth and the growing need for real-time data processing. Fog computing, as opposed to centralized cloud models, moves intelligence, processing, and data storage closer to the network's edge, lowering latency and facilitating more responsive applications, particularly in latency-sensitive industries like healthcare, smart cities, and driverless cars. However, the traditional cloud security solutions are unable to adequately handle the new security vulnerabilities brought about by fog computing's decentralized and distributed nature.

Operating at the edge of the network, fog nodes are frequently very heterogeneous, geographically distributed, and resource-constrained, which makes them appealing targets for cyberattacks. Data breaches, unauthorized access, denial of service (DoS) assaults, and privacy violations are among the main security problems in fog environments. Moreover, creating standardized security solutions is made more difficult by the variety of hardware and software configurations found in fog systems.

The objective of this review paper is to conduct a thorough analysis of the existing dangers confronting fog computing infrastructures and the strategies used to reduce these risks. Through an examination of the advantages and drawbacks of current remedies, this paper underscores the persistent difficulties in safeguarding fog environments and pinpoints the future research paths required to progress in this area. As fog computing advances, the demand for strong, expandable, and flexible security solutions becomes more and more crucial.

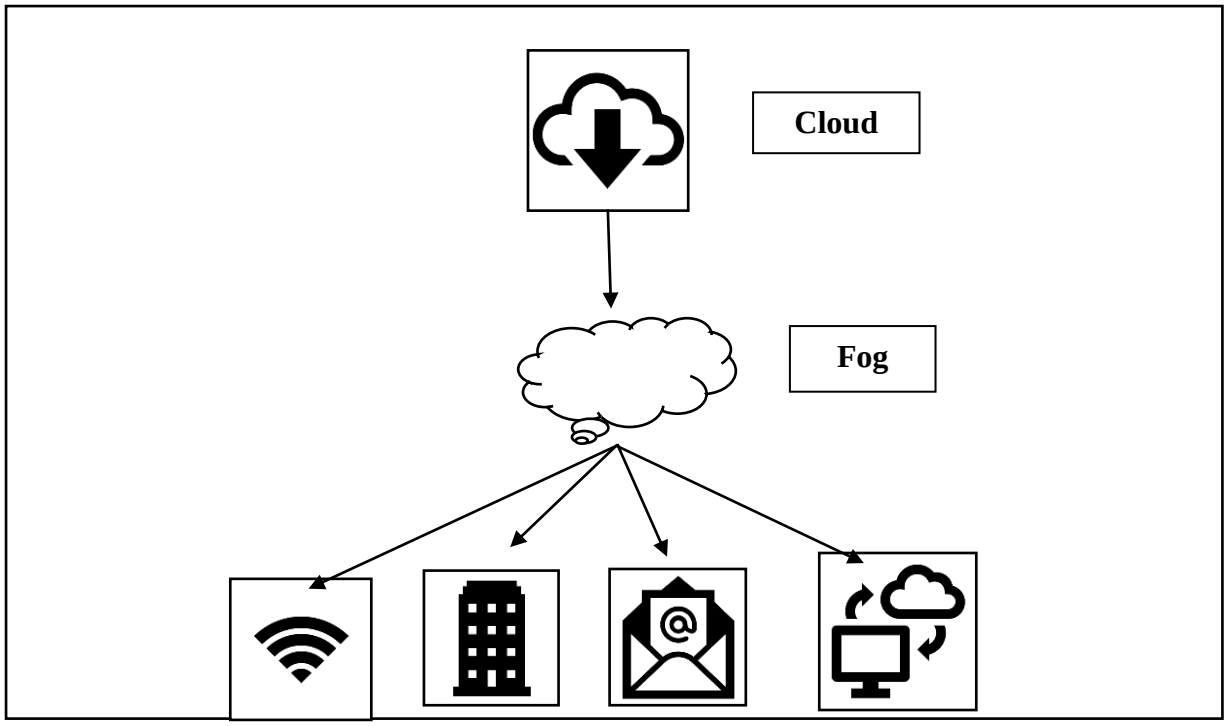

Fig 1. Fog computing

II. LITERATURE REVIEW

(Jianbing Ni et al., 2018) [1], provides a brief of the privacy concerns in the realm of fog computing, particularly when implemented in IoT environments. Notable challenges include the decentralized nature of fog nodes, which gives rise to vulnerabilities like detecting rogue nodes, exposing data privacy, and leaking location privacy. The paper also examines various remedies tailored for fog environments, including encryption, authentication, and access control mechanisms. It stresses the importance of adaptable and scalable security protocols that can function in real-time to accommodate the ever-changing nature of IoT networks. In addition, the research delves into different security frameworks and architectures presented by both the corporate sector and educational institutions. This includes Cisco's IOx service and the OpenFog Consortium, which have the objective of establishing standardized fog computing practices. The potential of integrating fog with other innovations like 5G and edge computing to improve the performance and security of IoT applications is also examined.

(Nadeem Abbas et al., 2019) [2], delves into the potential of fog computing in mitigating security issues within IoT (Internet of Things) settings. With IoT devices constrained by resources and traditional cloud-based security solutions falling short, the authors advocate for a security approach based on fog computing to bolster IoT security. The paper emphasizes how the fog provides localized processing and data storage, and how to provide a decrease in delays and risks related to centralized cloud infrastructure. It considers the main security issues, such as certification, confidentiality, integrity, and accessibility. The proposed mechanism counters several common attacks on these attributes, providing a lighter and more scalable solution than existing public key infrastructure (PKI) systems, which often incur high computational and memory overhead.

(Xiuzhen Cheng et al., 2017) [3], explores how fog computing might help with important digital issues in IoT settings. The authors draw attention to the shortcomings of conventional cloud models for the Internet of Things, highlighting the ways in which fog computing can improve data security and lessen attacks such as Denial of Service (DoS) by allocating computing resources closer to the network edge. Additionally, they suggest a fog-based certificate revocation technique that enhances IoT security efficiency by lowering communication overhead and speeding up reaction times.

(Yehia I. Alzoubi et al., 2020) [4], provides a thorough analysis of the digital issues related to fogging in IoT contexts. It demonstrates how fog computing, which runs close to the network edge, lowers latency and speeds up IoT applications' reaction times. The study also highlights the main security issues brought on by fog nodes dispersed and resource-constrained design. The study highlights that although fog computing provides localized security advantages including data encryption and real-time threat detection, its decentralized architecture also creates new threats. The authors examine a number of risk-reduction strategies, such as improved intrusion detection systems and access control mechanisms and came to the conclusion that, in spite of notable progress, fogging is still in developing and that much more has to be done to adequately handle the constantly changing threats.

(Deepak Puthal et al., 2019) [5], outlines the security concerns of fog computing, a decentralized computing infrastructure that brings cloud services to the network's edge. Although fog computing lowers latency and speeds up data processing, its distributed architecture creates new security risks for IOT (Internet of Things) devices. The sensor layer, middleware layer, and fog server are the three main levels of fog computing that are identified in the study. Every tier has unique security issues to deal with:

(i)Sensing Layer: Open to physical tampering of IoT devices, data injection, and spoofing attacks.
(ii) Threats to the middleware layer include denial-of-service (DoS) attacks, in which hostile nodes obstruct data delivery, Sybil attacks, and data interception.
(iii) Fog Server: Vulnerable to more sophisticated threats that take advantage of flaws in communication and authentication protocols, such as social engineering, DDoS attacks, and session hijacking.

The paper suggests a number of security solutions, such as intrusion detection systems (IDS), secure protocols (such as TLS and IPSec), firewall setups, cryptography, and safe programming techniques. To properly manage the enormous number of connected devices, it also highlights the necessity of privacy preservation and improved scalability solutions.

(Sourav Kunal et al., 2019) [6], offers a thorough analysis of fogging systems and the security concerns that go along with it. The study focuses on how fogging has brought cloud features or attributes to the edge, enabling low-latency applications like smart healthcare systems and Internet of Things sensors. Trust management, authentication, secure communication, privacy protection, and defense against malevolent assaults are among the security issues that have been brought to light. The authors go into a number of remedies, including authentication procedures, privacy-preserving techniques, and fog forensics. Interestingly, they examine technologies such as elliptic curve cryptography (ECC), which is thought to be more effective in fog conditions than more conventional techniques like RSA. Mutual authentication approaches and intrusion detection systems are also suggested as ways to protect fog node-to-fog communication.

The study also discusses open research difficulties, including scalability, safe protocols for dynamically joining or departing fog nodes, and cross-border data issues. Additionally, it investigates possible avenues for enhancing fog network security in the future using cutting-edge methods like user behavior tracking and decoy technologies.

(Mithun Mukherjee et al., 2017) [7], highlights the security and protection issues characteristic to mist computing, which expands cloud administrations to the arrange edge. Whereas mist computing decreases inactivity and offloads cloud information centres, its attributes—such as portability, heterogeneity, and wide ranging geo-arrangement—create noteworthy challenges that conventional cloud-based security models cannot appropriately address. The paper gives a comprehensive audit of these security concerns, counting issues related to the security of information prepared in topographically disseminated and portable situations. It moreover analyses the potential assaults and vulnerabilities particular to haze systems, such as man-in-the-middle, information spillage, and unauthorized get to.

(Aleksandr Ometov et al., 2022) [8], extensively examines the digital protection challenges present in Cloud, Edge, and Fog computing paradigms, emphasizing their distinct architectures and computing capabilities. The paper identifies critical security threats and privacy issues, particularly emphasizing the complexity of implementing uniform security measures across the diverse ecosystem. It also evaluates the similarities and differences in security vulnerabilities among the different paradigms and explores various

approaches to address these challenges, including diverse deployment strategies to enhance privacy and security measures. The paper also emphasizes how the move from conventional frameworks to disseminated computing models has expanded the requirement for vigorous security arrangements.

Rahman and Wen (2018), highlights fogging as an expansion of cloud administrations towards organize edge. It examines key applications like smart grid and healthcare, emphasizing fog's capacity to diminish inactivity by preparing information locally. The paper moreover addresses security challenges such as information security, versatility bolster, and heterogeneity, whereas proposing that mist computing underpins real-time applications more successfully than cloud models.

(Saad Khan et al., 2017) [10], investigates the security challenges related with Fog computing, a worldview expanding cloud administrations to the edge of the arrange. Fog computing offers decentralized information handling, making it perfect for real-time, location-sensitive applications like IoT (Internet of Things). The paper emphasizes that this engineering brings critical security dangers, as Mist computing acquires numerous vulnerabilities from cloud computing, such as Advanced Persistent Threats (APTs), account capturing, and Denial of Service (DoS) assaults. The survey distinguishes common security holes in Fog applications, which are regularly driven by client usefulness requests and security measures. The paper too addresses comparable innovations like edge computing, fog, and small information centres, giving a comprehensive comparison of their security concerns. The authors concluded with recommendations for future investigate headings, highlighting the significance of joining vigorous security components into the plan of Fog frameworks to address dangers such as unreliable APIs.

Soni(2022) [11], in the paper stated that the Internet of Things (IoT) is relying more and more on big data as it offers insights into consumer behaviour, asset utilisation, and preventative maintenance. Big data can be employed in the IoT to gather, store, analyse, and act on data from connected devices, sensors, and other sources. The system may be made more effective and efficient with the use of this data, which can also give important insights into how customers behave and how assets are utilised.

III. COMPARISON OF RELATED RESEARCH WORK

The following table provides a comprehensive comparison of several research papers focused on the fog security. It outlines key aspects such as the paper titles, authors, years of publication, the primary focus of each study, the security measures addressed, countermeasures taken, methodology or approach used and the future directions proposed.

TABLE I
COMPARISON OF RESEARCH WORK

Paper Title	Author	Year	Research Focus	Security Threats Addressed	Proposed Countermeasures	Methodology/ Approach
Securing Fog Computing for Internet of Things Applications: Challenges and Solutions	Jianbing Ni et al.	2018	Focuses on safeguarding mechanisms and information integrity in fogging.	Data breaches, man-in-the-middle (MITM) attacks, and distributed denial of service (DDoS).	Proposes a one-way encryption framework for secure data sharing and authentication.	Uses a combination of cryptography and blockchain to establish a secure, decentralized framework for fog nodes.
A Mechanism for Securing IoT-enabled Applications at	Nadeem Abbas et al.	2019	Emphasizes secure access control in large-scale fog	Insider threats, DDoS, and man-in-the-browser attacks in fog	Focuses on key management schemes for secure authentication and	Proposes a hierarchical key management scheme for

the Fog Layer			networks with IoT devices.	nodes.	cryptographic protocols.	authentication in large-scale fog environments, validated with security analysis and simulations.
An overview of Cloud-Fog Computing: Architectures, Applications with Security Challenges	Sourav Kunal et al.	2019	Studies encryption techniques to safeguard sensitive data in fog and IoT environments.	Data confidentiality breaches, edge device vulnerabilities, and network attacks.	Uses homomorphic encryption and secure multi-party computation (SMC) for secure data processing and storage.	Utilizes encryption techniques optimized for edge devices and proposes frameworks for reducing the computational overhead of these systems.
Fog Computing, Applications, Security and Challenges, Review	Gohar Rahman	2018	Analyzes the intrusion detection systems (IDS) in fog computing environments.	External attacks such as botnets, insider threats, and DDoS.	Proposes a hybrid intrusion detection system using AI techniques such as machine learning for dynamic threat detection.	Incorporates machine learning algorithms for anomaly detection and pattern recognition in large fog networks.
Fog Computing Security: A Review of Current Applications and Security Solutions	Saad Khan et al.	2017	Investigates lightweight security solutions for resource-constrained fog networks.	Unauthorized access, malicious node attacks, and data privacy.	Introduces a novel lightweight encryption scheme combined with access control policies.	Introduces a distributed, lightweight encryption protocol that emphasizes low latency.

IV. CONCLUSION

Fog computing presents a transformative arrangement for overseeing information closer to the edge of systems, empowering quicker handling, and decreased inactivity. This decentralized engineering presents a special set of security challenges that got to be tended to guarantee its broad selection. This review has highlighted different dangers to fog computing, counting information breaches, denial of service attacks, and security infringement, which can compromise the astuteness, privacy, and accessibility of information.

Whereas a few countermeasures, such as encryption conventions, get to control components, and interruption location frameworks, have been created to moderate these dangers, they stay inadequately to completely address the energetic and dispersed nature of fog situations. The heterogeneity of gadgets, real-time information preparing necessities, and the scale of arrangements display progressing challenges for actualizing viable and adaptable security arrangements.

Looking ahead, future inquire about security in fog computing by upgrading privacy-preserving strategies, fortifying confirmation systems, and creating versatile security measures of taking care of large-scale and different systems. Collaboration between the educational community, industry, and government bodies is fundamental to progress in fog security and make strong systems for its secure integration into basic foundations. As fog computing proceeds to advance, so must the security procedures that secure it, guaranteeing that this promising innovation can be sent securely and successfully.

V. FUTURE SCOPE

The need for more resilient and adaptable security solutions will only grow as fog computing develops and becomes more popular across a range of businesses. Fog computing's decentralized structure and proximity to clients and Internet of Things

(IoT) devices provide special vulnerabilities that call for innovative methods of attack detection and avoidance. Future studies should concentrate on creating all-encompassing security frameworks that can handle the wide variety of fog computing-related devices, networks, and protocols.

Improving privacy-preserving methods is one interesting field for future research. It will be crucial to maintain data secrecy without sacrificing efficiency when fog nodes process enormous volumes of sensitive data. While methods like unfair privacy, privacy preserving computation, and parallel encoding present viable avenues, more development and optimization for fog situations are required.

Another key focus area is the development of lightweight, scalable authentication and access control mechanisms that can operate efficiently across large-scale, distributed fog networks. Traditional security measures designed for centralized cloud systems are often inadequate for the decentralized fog architecture. Future solutions must balance security with low-latency processing to meet the real-time demands of fog-based applications.

Moreover, there is a growing need for adaptive intrusion detection and prevention systems (IDPS) capable of handing the dynamic and heterogeneous nature of fog environments. AI-driven security models, leveraging machine learning and data analytics, could provide more accurate threat detection while minimizing false positives.

In conclusion, the future of fog security research lies in creating flexible, scalable, and intelligent solutions that can keep pace with the evolving complexity of fog ecosystems. This will require ongoing collaboration between academia, industry, and government bodies to ensure that fog computing can reach its full potential securely.

REFERENCES

[1] Jianbing Ni, Xiaodong Lin, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions", IEEE Communications Surveys & Tutorials, Vol. 20, No. 1, First Quarter 2018.

[2] Nadeem Abbas, Muhammad Asim, Noshina Tariq, Thar Baker, Sohail Abbas, "A Mechanism for Securing IoT-enabled Applications at the Fog Layer", J. Sens. Actuator Netw. 2019, 8, 16.

[3] Xiuzhen Cheng, Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, "Fog Computing for the Internet of Things: Security and Privacy Issues", IEEE Internet Computing March 2017.

[4] Yehia I Alzoubi, Valmira H. Osmanaj, Ashraf Jaradat, Ahmad Al-Ahmad, "Fog Computing Security and Privacy for the Internet of Thing applications: State-of-the-art", Security Privacy, 2020.

[5] Deepak Puthal, Saraju P. Mohanty, Sanjivani Ashok Bhavake, Graham Morgan, Rajiv Ranjan, "Fog Computing Security Challenges and Future Directions", IEEE Consumer Electronics Magazine May 2019.

[6] Sourav Kunal, Arijit Saha, Ruhul Amin, "An overview of Cloud-Fog Computing: Architectures, Applications with Security Challenges", Security Privacy, 2019.

[7] Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, Vikas Kumar, “Security and Privacy in Fog Computing: Challenges”, IEEE Access, Volume 5, 2017.

[8] Aleksandr Ometov, Oliver Liombe Molua, Mikhail Komarov, Jari Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing", Sensors 2022, 22, 927.

[9] Gohar Rahman, Chuah Chai Wen "Fog Computing, Applications, Security and Challenges, Review", International Journal of Engineering & Technology, 7 (3) (2018) 1615-1621.

[10] Saad Khan, Simon Parkinson, Yongrui Qin, "Fog Computing Security: A Review of Current Applications and Security Solutions", Journal of Cloud Computing: Advances, Systems and Applications (2017) 6:19.

[11]Goldi Soni, “Data Science: Significance of big data in internet of things” NeuroQuantology (2022) 20(21) 607-606.