

A holistic mathematical cyber security model in fog resource management in computing environments

Prabhat Kumar Srivastava [#]

Department of Computer Science and Engineering

IMS Engineering College

Ghaziabad

Uttar Pradesh

India

Ashish Kumar Srivastava ⁺

Department of Computer Science and Engineering

Galgotias University

Greater Noida

Uttar Pradesh

India

Raja Rao Budaraju [§]

Oracle

3990 Scottfield street

Dublin 94568

CA

U.S.A.

Rama Krishna Yellapragada [†]

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation Green Fields

Vaddeswaram

Andhra Pradesh

India

[#] E-mail: sri_prab@rediffmail.com

⁺ E-mail: akshere.ashish@gmail.com

[§] E-mail: rajaraob@yahoo.com

[†] E-mail: yramakrishna@kluniversity.in

Sasidhar Attuluri [@]

Savin Technologies Inc.

Suite # 2070, 9901 East Valley Ranch Parkway

Irving

TX 75063

U.S.A.

Smaranika Mohapatra ^{*}

Department of Information Technology

Manipal University Jaipur

Jaipur

Rajasthan

India

Abstract

In the evolving landscape of computing environments, fog computing has emerged as a pivotal technology for handling the increasing demands of Internet of Things (IoT) applications. Fog computing, with its decentralized approach, brings computational power closer to IoT devices, reducing latency and bandwidth constraints. However, this distributed architecture poses significant cybersecurity challenges, necessitating a holistic mathematical model to ensure the security and integrity of fog resources. This review presents a comprehensive mathematical cyber security model that is tailored to fog resource management in computing environments. The models generally encompass a wide array of security aspects, including data confidentiality, integrity, availability, and authentication. Leveraging advanced mathematical techniques, the models offer a robust framework for assessing and enhancing security in fog computing systems. The key components include threat modeling, risk assessment, and dynamic resource allocation strategies. By systematically analyzing potential threats and vulnerabilities specific to fog computing, these models assist in devising effective countermeasures and security policies. Moreover, there is a need to incorporate an adaptive resource allocation algorithm to dynamically allocate computing resources based on security priorities and real-time threat assessments. This review demonstrates the effectiveness of the mathematical cyber security model in bolstering the resilience of fog computing environments. The review highlights the need for safeguarding the next generation of fog computing systems against cyber threats, fostering the continued growth and adoption of transformative technology.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Fog computing, Resource management, Resource security system, Fog applications, IoT tools, Security.

[@] E-mail: sattuluri@savintechologies.com

^{*} E-mail: smaranikka.88@gmail.com (Corresponding Author)

1. Introduction

Edge and fog computing have become more prevalent in recent years, triggering a significant change in the landscape of computer environments. These decentralized methods place processing power closer to the data sources, which has the potential to improve latency, boost real-time processing, and maximize resource utilization [1-3]. The imperative need to adequately handle cybersecurity challenges is an essential part of this development. There is a growing need to develop a holistic mathematical model for security in fog resource management as the lines between cloud, edge, and fog computing begin to blur.

As edge computing empowers businesses and industries, fog computing offers the same by making it easier to perform data processing, storage, and application deployment at the network's edge. However, there is a unique set of cybersecurity vulnerabilities and threats that arise due to this closeness to the data source [4,5]. Fog computing differs from conventional cloud-centric models in that it uses a wide variety of devices, some of which may have little processing power, to carry out computational tasks. A reevaluation of cybersecurity strategies is essential considering the implications of this dissemination. Figure 1 shows the architecture of the devices that can communicate with the cloud using Fog computing.

Focusing on the development and implementation of a comprehensive mathematical model, this review paper explores the complex field of fog computing cybersecurity. This review aims to provide a holistic framework for assessing, mitigating, and preempting cyber threats in fog computing environments by considering the entire spectrum of fog resource

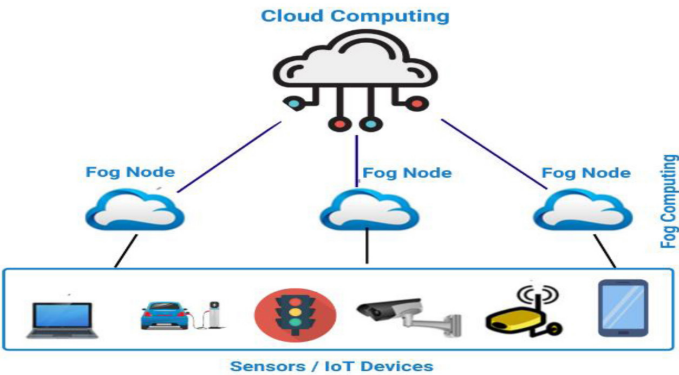


Figure 1

Devices that can communicate with the Cloud using Fog computing

management, including data, computing, storage, and application components. The review delves into the complexities of mathematical framework and investigates the fundamental principles of fog computing [6-8], to gain insight into the need for a unified cybersecurity approach in fog computing and the methods in which this novel model can provide a basis for securing the availability, confidentiality, and integrity of data and resources in a fog-enabled computing environment [9].

2. Related Works

Securing the rapidly expanding edge and fog computing ecosystem necessitates the development and implementation of a robust mathematical cyber security model for fog resource management in computing environments. Fog computing offers a viable option to improve processing efficiency and reduce the amount of data sent to the cloud, both of which are essential for edge computing. Figure 2 shows the classification of fog computing configuration Focusing on the optimization of resource allocation via the application of ant colony optimization methods [10-11], this study tackles the problems that arise from the management and processing of resources in fog computing environments. By simulating cloud-like functionality close to data-generating devices, fog nodes make computing more holistic. This geographical proximity expedites the collection, processing, and availability of data for resource managers. In order to realize a multitier application architecture [4], these fog nodes can be deployed dynamically at various points along the IoT-to-Cloud path. For Internet of Things (IoT) applications, proximity becomes crucial

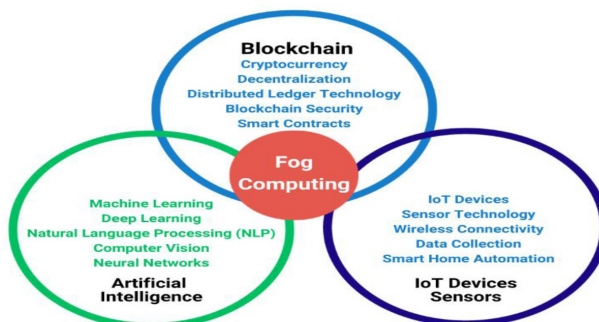


Figure 2
Classification of Fog Computing Configuration

because of the importance of low latency and efficient processing [5]. Notably, this method can have a significant impact in a wide variety of fields, from manufacturing and transportation to healthcare [12] and smart cities. There are significant benefits of incorporating fog computing into the IoT ecosystem since it promotes effective resource management and enhanced data processing.

Hence, fog computing is an ideal solution for satisfying the unique requirements of numerous IoT applications in a wide range of markets. Rohinidevi et al. [7], have characterized 'big data' as voluminous, fast-paced, and diverse datasets that necessitate cost-effective novel data analysis techniques for meaningful insights. In recent times, the primary challenges posed by big data have largely been addressed [13-16]. These challenges are encapsulated within the big data: volume, velocity, variety, veracity, and value. However, it's worth noting that this definition overlooks another crucial aspect: dimensionality.

3. Security challenges

"Inconsistency disclosure" [17] is an effective technique for pinpointing parts of a dataset that don't follow the norm. In a nutshell, it aids in identifying standout pieces of information. This method can be used to spot a number of different outliers:

- (a) Local Density Deviation: This method evaluates a data point's local density in relation to its neighboring data points. Instances with much lower density than their neighboring data points are singled out for special attention.
- (b) Point Anomalies: A data point is considered an anomaly [17] if it is significantly more or less common than the other points in the dataset. The detection of fraudulent bank transactions is a well-known instance of using anomalies to uncover unusual behavior.
- (c) Contextual Anomalies: An occurrence is said to be anomalous in context when it stands out as out of the ordinary under certain conditions. When dealing with increasingly complicated data, such as in time-series analysis, this method of anomaly detection becomes increasingly important. [18]
- (d) Collective Anomalies: These are discrepancies that appear over an entire dataset as a whole, as opposed to only a few isolated instances. Electrocardiogram (ECG) abnormalities indicative of arrhythmias are a common instance [18].

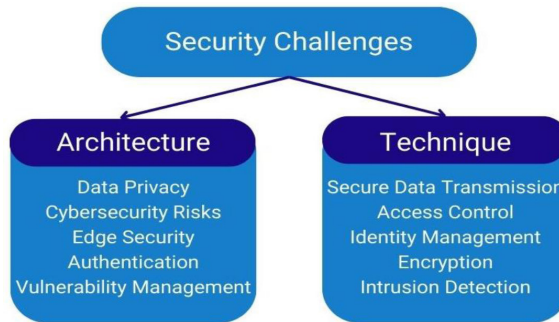


Figure 3
Structure of Security Challenges

Anomaly detection plays an important role in many domains, such as cybersecurity, fraud detection, healthcare monitoring, etc. Figure 3 illustrates the structure of security challenges associated with anomaly detection.

The numerous devices connected to fog nodes and the multiple entry points pose security challenges in fog computing. However, authentication is only part of the solution when it comes to securing communications between IoT devices and fog nodes in a network. There is still the possibility of faults or malicious assaults on devices. Because fog nodes might probe around for private information, security is more difficult to manage in the fog computing domain. This means it's more important than ever to confirm user identities before allowing access to data kept on off-site cloud servers connected to the main network [7]. Security is a particular concern in fog computing due to its decentralized nature. It requires strong procedures for authenticating devices and users and protecting data's privacy and security as it travels from the edge to the fog nodes and finally to the cloud.

Safeguarding the privacy and integrity of data in a decentralized computing paradigm like fog computing would need to tackle these security challenges as its use becomes more widespread. Because of the complexity and changeability of the environment, it is crucial that the network be protected by stringent security mechanisms and protocols. Furthermore, providing centralized control presents substantial hurdles due to the widespread deployment of fog nodes throughout extensive territories. The Internet of Things (IoT) introduces a myriad of security and privacy risks, but it also revolutionizes a variety of services for end-users. Devices connected to the Internet of Things (IoT) are already ubiquitous in our homes and places of business. The lack of strong security

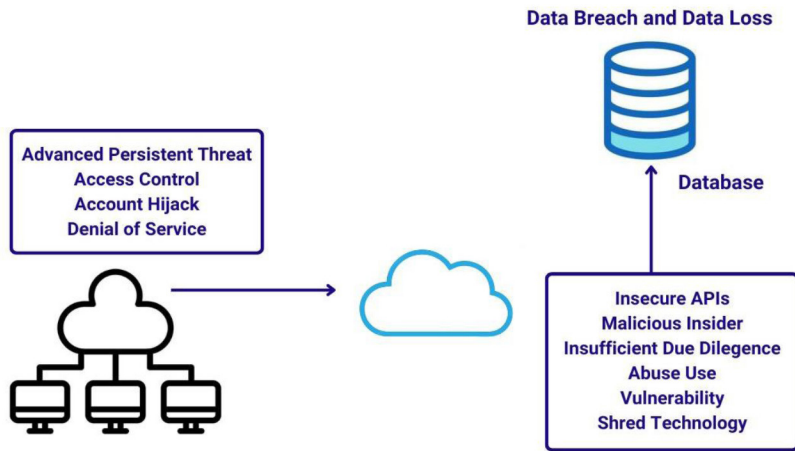


Figure 4
Fog Computing Methodology

mechanisms makes sensitive user information more susceptible to compromise as it travels among IoT devices [9]. Any security flaws in IoT devices pose a significant threat to the end-user's network infrastructure due to the devices' interoperability with a wide variety of networks. Figure 4 shows the dimensions of fog computing, including the ever-present danger of cybercrimes that try to compromise network infrastructure to steal confidential information and trade secrets.

The interaction between IoT devices and fog nodes in the network fabric is a crucial cog that reduces latency and improves the quality of location-based experiences across a wide range of IoT applications. Cloud services in particular present significant security concerns in the digital realm. Users' faith in cloud services is at risk if their security isn't properly managed. Users typically interact with cloud services without having much insight into the inner workings or physical locations of the underlying servers. Since most people's private information now resides in the cloud, cloud computing has had a profound effect on how data is stored and processed [16]. Problems with access control can lead to poor management and even provide bad actors the ability to do things like deploy software and change settings. This diagram illustrates the inner workings of the fog computing ecosystem within the larger computer environment.

4. Simulation and Result Analysis

In the review, most of the security aspects have been understood by research. Figure 5 describes the market analysis of the fog computing of different applications. The lack of standardized norms and protocols, as well as a paucity of skilled labor, are limiting the growth of the sector. In addition, there are significant obstacles to development caused by the incorporation of AI solutions into present frameworks and the integration of large, unified systems. Another factor that could impede the expansion of the global fog computing market is the increased risk of cyberattacks caused by the proliferation of distributed computing and the increasing complexity of network architecture. The examination of the fog computing paradigm gives a thorough comprehension of these difficulties and how they connect with the broader dynamics of the market. To ensure the long-term success of the fog computing market, it will be necessary to address not just technology advances but also legislative and workforce development concerns.

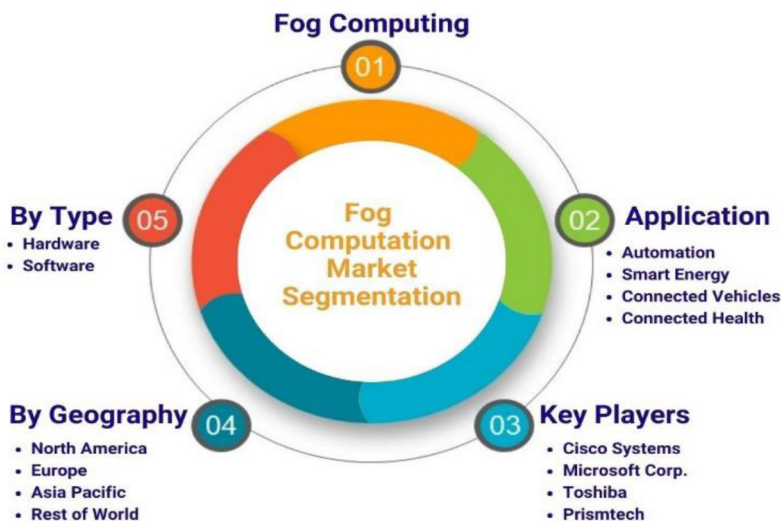


Figure 5
Segment Analysis of Fog Computing

The future trajectory of this technology and its widespread acceptance across multiple industries will be heavily influenced by efforts to alleviate these issues and establish a suitable ecosystem for fog computing innovation.

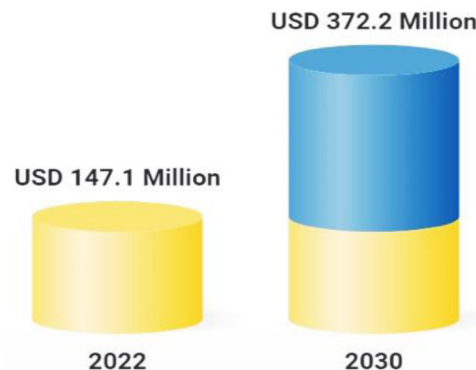


Figure 6

Global Fog Computing Market [20]

Figure 6 shows the projected Global Fog Computing Market growth in the year 2022 to 2030 and the forecast to grow at a CAGR of 12.3%. [20] North America’s position as a global leader in the adoption and innovation of fog computing is cemented by the region’s robust investments in fog computing research and the burgeoning IoT ecosystem.

Conclusion and Future Work

Securing the rapidly expanding edge and fog computing ecosystem necessitates the development and implementation of a robust mathematical cyber security model for fog resource management in computing environments. The review has highlighted the critical need for developing efficient methods for combating cybersecurity threats in distributed computing models. Providing a holistic framework for data, computing, storage, and applications, this model shows promise for increasing the robustness of fog computing infrastructures. As we continue to navigate the intricate intersection of cybersecurity and distributed computing, the proposed model stands as a crucial tool for safeguarding the integrity and availability of data and resources in this dynamic, fog-enabled era.

References

- [1] Kumar, S., Srivastava, P. K., Srivastava, Singh, D., & Goyal, D. Chaos based image encryption security in cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1041-1051 (2022).

- [2] Kamble, S., Saini, D. K. J., Verma, S., Tiwari, A., & Goyal, D. Detection and tracking of moving cloud services from video using saliency map model. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1083-1092 (2022).
- [3] Kumar, S., Dubey, K. K., Gautam, Kumar, V., & Mamodiya, U. Detection of recurring vulnerabilities in computing services. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1063-1071 (2022).
- [4] Kumar, S., Kumar, S., Ranjan, N., Tiwari & Rafsanjani, M. K. Digital watermarking-based cryptosystem for cloud resource provisioning. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1), 1-20 (2022).
- [5] Tiwari, Ashish, and Ritu Garg. "Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems." *International Journal on Semantic Web and Information Systems (IJSWIS)* 18, no. 1 : 1-18 (2022).
- [6] Alwakeel AM. "An overview of fog computing and edge computing security and privacy issues." *Sensors*, 21(24), 8226 (2021).
- [7] Rohinidevi, V. V., Srivastava, P. K., Dubey, N., Tiwari, S., & Tiwari, A. A Taxonomy towards fog computing Resource Allocation. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-5). IEEE (2022, December).
- [8] Singh, N. K., Jain, A., Arya, S., Gonzales, W. E. G., Flores, J. E. A., & Tiwari, A. Attack Detection Taxonomy System in cloud services. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-5). IEEE (2022, December).
- [9] Tiwari, A., & Garg, R. Reservation System for Cloud Computing Resources (RSCC): Immediate Reservation of the Computing Mechanism. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1), 1-22 (2022).
- [10] Ali A, Ahmed M, Imran M, Khattak HA. "Security and privacy issues in fog computing." In *Fog Computing: Theory and Practice*, 105-137 (2020).
- [11] Apat HK, Nayak R, Sahoo B. "A comprehensive review on Internet of Things application placement in Fog computing environment." *Internet of Things*, 100866. Published on July 1 (2023).
- [12] Patil, V.; Saxena, J.; Vineetha, R.; Paul, R.; Shetty, D.K.; Sharma, S.; Smriti, K.; Singhal, D.K.; Naik, N. Age Assessment through Root Lengths of Mandibular Second and Third Permanent Molars Using

- Machine Learning and Artificial Neural Networks. *J. Imaging*, 9, 33 (2023).
- [13] Tran-Dang H, Bhardwaj S, Rahim T, Musaddiq A, Kim DS. "Reinforcement learning based resource management for fog computing environment: Literature review, challenges, and open issues." *Journal of Communications and Networks*, 24(1), 83-98 (2022).
- [14] Tiwari, A., Sharma, V., & Mahrishi, M. Service adaptive broking mechanism using MROSP algorithm. In *Advanced Computing, Networking and Informatics-Volume 2*, pp. 383-391. Springer, Cham (2014).
- [15] Tiwari, A., Sharma, R. M., & Garg, R. Emerging ontology formulation of optimized internet of things (IOT) services with cloud computing. In *Soft Computing: Theories and Applications* (pp. 31-52). Springer, Singapore (2020).
- [16] Pa Abd Elaziz M, Abualigah L, Attiya I. "Advanced optimization technique for scheduling IoT tasks in cloud-fog computing environments." *Future Generation Computer Systems*, 124, 142-154 (2021).
- [17] S. Kumar, U. Gupta, A. K. Singh, and A. K. Singh, "Artificial Intelligence: Revolutionizing cyber security in the Digital Era", *J. Comput. Mech. Manag*, vol. 2, no. 3, pp. 31-42, Aug. (2023).
- [18] S. Kumar, "Reviewing Software Testing Models and Optimization Techniques: An Analysis of Efficiency and Advancement Needs", *J. Comput. Mech. Manag*, vol. 2, no. 1, pp. 43-55, Feb. (2023).
- [19] Alrawais A, Alhothaily A, Hu C, Cheng X., "Fog computing for the internet of things: Security and privacy issues." *IEEE Internet Computing*, 21(2), 34-42 (2017).
- [20] R. and M. Ltd, "Fog computing - global strategic business report," Research and Markets - Market Research Reports, <https://www.researchandmarkets.com/reports/4845755/fog-computing-global-strategic-business-report> (accessed July. 13, 2023).