Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1447–1456
DOI : 10.47974/JDMSC-1770

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

Syam Machinathu Parambil Gangadharan [†]
Department of Engineering
Liverpool John Moores University
U.S.A.

K. Arumugam [§]
Department of Computer Science
Karpagam Academy of Higher Education
Coimbatore
Tamil Nadu
India

Shaziya Islam [‡]
Department of Computer Science and Engineering
Rungta College of Engineering and Technology
Bhilai
Chhattisgarh
India

K. V. Daya Sagar [@]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram
Andhra Pradesh
India

Juan Carlos Cotrina-Aliaga [#]
Faculty of Engineering
Universidad Privada los Andes
Huancayo
Perú

[†] *E-mail:* **syamganga@gmail.com**
[§] *E-mail:* **aaruk.dpm@gmail.com**
[‡] *E-mail:* **shaziya.islam26@gmail.com**
[@] *E-mail:* **sagar.tadepalli@gmail.com**
[#] *E-mail:* **d.jcotrina@upla.edu.pe**

Online version of this article has been corrected with minor changes. These changes do not impact the academic content of the article.

Surendra Kumar *
Department of Computer Engineering and Applications
GLA university
Mathura
Uttar Pradesh
India

Abstract

Now a days Cloud computing isn't common sense for some Internet of things applications, fog enrolling is every now and again used. Its proper methodology keeps an eye on the necessities of IoT and present-day IoT, as well as the enormous proportion of splendid data sensors and IoT gadgets, produce, which would be extreme and drawn-out to send off the cloud for dealing with and examination. Fog enrolling diminishes the information move limit required and reduces the unstable correspondence among sensors and the cloud, which can antagonistically impact IoT execution. Fog is exceptionally conveyed and comprises a wide number of independent end gadgets, which add to the handling. In any case, the range of gadgets presented across various clients is not examined. Consequently, the security of fog computing is a main pressing issue that ought to come into thought. Thusly, to give the vital security to fog computing, there is a need to comprehend what the security concerns are with respect to fog. Fog computing is a decentralized enlisting establishment where data, handling, storing, and applications are seen as some place near the data source and the cloud. Like edge enrolling, murkiness figuring brings the advantages and power of the cloud closer to where data is made and circled back to. With fog computing, close-by data amassing and examination of time-delicate data become more direct. With this the aggregate and the distance of data passed to the cloud are diminished, thus lessening the impact of well-being and security issues.

Subject Classification: *Primary 93A30, Secondary 49K15.*

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

1. Introduction

Fog enlisting is a decentralized handling structure wherein data, figuring, storing, and applications are seen as some place near the data source and the cloud as shown in Figure 1. Like edge handling, fog figuring brings the advantages and power of the cloud closer to where data is made and circled back to[1-3]. This little limit and estimation of data before sending it over to the cloud is fog-enrolling. Fog figuring incorporates the utilization of contraptions with lower taking care abilities to share a part of the cloud's pile[4,5].

* *E-mail:* **kumar.surendra1989@gmail.com (Corresponding Author)**

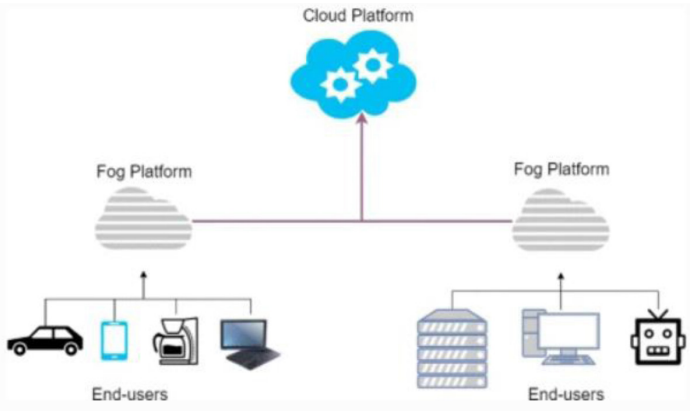

Figure 1

Devices that can communicate with the Cloud using Fog computing [7]

All around, called Edge Figuring or starters, dimness enlisting stays aware of the improvement of Fog/cloud, taking care of, and frameworks affiliation relationship between end contraptions and conveyed overseeing server ranches. Murkiness enrolling is a gifted figuring perspective that loosens up conveyed dealing with to the edge of plans/affiliations. Dimness figuring utilizes different focuses between the cloud and the end gadgets wherein understanding can be found[7-9]. These assigned insightful focus address base stations or passages [5]. By bringing data from the cloud, haze figuring can deal with the IoT information in closeness to the information sources. In a little while, it can involve assets from the cloud in a more surprising mode than through individual gadgets. For example, darkness figuring can move the data to a Nearby circumstance in the affiliation plan and in this manner offer help with information taking consideration in a haze community or an IoT entryway [6].

2. Related Work

Fog computing is a promising reaction for work on the presence of mind and reduces the information volume shipped off the cloud checking on overseeing and dealing with limits of edge in a huge manner. The passing considered Haziness figuring wants to execution of significant streamed assets in the board structures as discussed in Figure 2. In this paper, we address asset pioneers in lack of clarity the executives and endeavor to find the briefest course to assets in a dissipated way by applying underground bug region refreshes[11]. Mist Selecting merges an

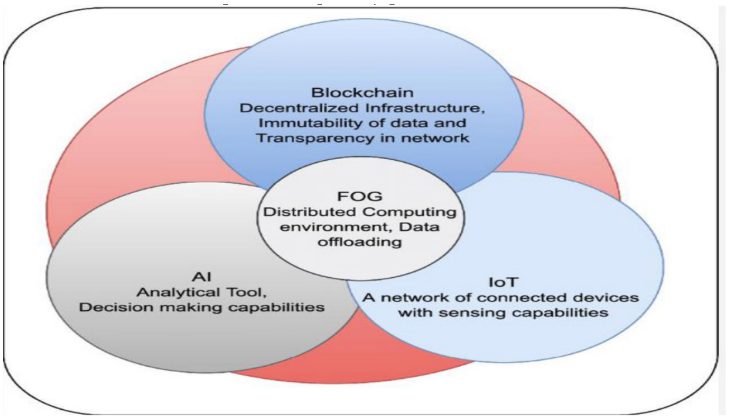

Figure 2

Classification of Fog Computing configuration

incorporated point of view where fog nodes offer cloud-like connections inside the area of gadgets that produce the information. The closeness of lack of clarity focuses accomplishes speedier evaluation, aggregation, and information for pioneers. Dinkins's focus focuses can be figured out in any spot in the IoT-to-Cloud way. As a basis, a multitier application plan is conceivable [4]. As idleness and watchful assessment are required for IoT applications, legitimate closeness other than changes into a central variable [5]. Considering this closeness shadowiness figuring better take the excellent thought of the necessities of IoT applications curiously, with other indistinct models. Making, transportation, clinical advantages, and keen metropolitan affiliations are brilliant to use events as per an irregularity point of view [12].

The researchers had [7] defined, large information is high-volume, high-speed, and high-assortment informational collections that request financially savvy novel information examination for independent direction and to deduce helpful bits of knowledge. As of late, the center difficulties of large information have been generally settled [15]. These are held inside the Versus large information volume, speed, assortment, veracity, and worth. Be that as it may, such a definition overlooks another significant perspective: dimensionality," that

3. Various security challenges

Inconsistency disclosure is a system used to perceive something that doesn't fit the commonplace approach to acting of a dataset. By the day's

end, characteristic ID tracks down information of interest in a dataset that strays from the other data.

- the local thickness deviation of a given snippet of data with respect to its neighbors. It considers as special cases the models that have an essentially lower thickness than their neighbors [17].

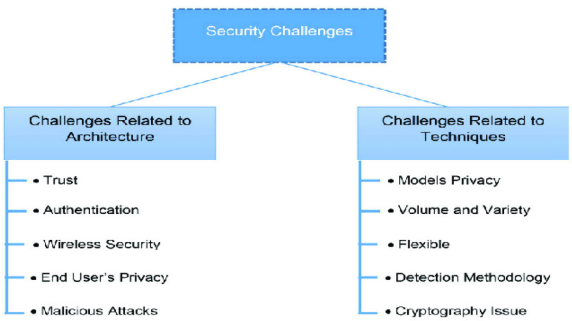

Figure 3

Structure of Security Challenges

- Point irregularities - if a data point is unreasonably distant from the rest, it falls into the class of point abnormalities. The above delineation of a bank trade frames points of eccentricities.
- Legitimate irregularities - If the event is unpredictable for unequivocal circumstances (setting), we have setting-focused anomalies. As data ends up being progressively stunning, including irregularity acknowledgment systems for the setting is crucial. This anomaly type is ordinary in time-series data [18].
- Total irregularities: The total peculiarity shows a combination of odds concerning the whole dataset, but not individual things. Model: breaking beat in ECG (Electrocardiogram).

3. Various security challenges

Dimness handling security issues arise as there are various devices related to fog center points and at different entrances. Notwithstanding, affirmation expects a critical part in spreading out the basic plan of relations between IoT contraptions and cloudiness centers in the association this isn't sufficient as devices can persistently mess up or are

moreover defenseless to dangerous attacks. In dimness figuring, security preservation is more troublesome since fog center points could assemble tricky data. Consequently, the character of end-clients is stood out from the remote cloud server that lies in the focal association [7].

What's more, since fog centers are scattered in immense locales, brought together control is problematic. Regardless of the way that IoT is impacted, it passes various organizations on to the end clients. It really faces various security and assurance issues. IoT contraptions are related to workspaces or computers in our daily existence. The shortfall of security assembles the bet of your own information spilling while the data is accumulated and redirected to the IoT contraption. IoT devices are related to various associations. In this way, expecting the IoT device contain any security issues, might be damaging to the end-client association [9]. These issues can pursue various structures and mischief them. The foremost security issue is client information spillage in IoT devices like data, regions, etc. As relations between IoT contraptions and murkiness center points in the association expect a critical part that mitigates the impact of low torpidity and region experience with various IoT applications. Security includes stress in the online world. With close to no data on the genuine region of the server, end-clients use cloud organizations with practically zero focal points about the cycles being referred to. Disseminated figuring changes the approach in which information is made due, essentially where individual data is concerned. With conveyed processing data is taken care of in a cloud environment [16]. If security is overlooked, cloud service providers will come up short on the trust of end-clients. As shown in figure 3 we can find the following thing related to the fog computing. The persistent crimes are digital assaults by which the point is to think twice about organization's framework with the longing to take information and protected innovation. The access control issues can bring about unfortunate administration and any unapproved client having the option to procure information and authorizations to introduce programming and change designs. Figure 3 shows the working of fog system in computing environment.

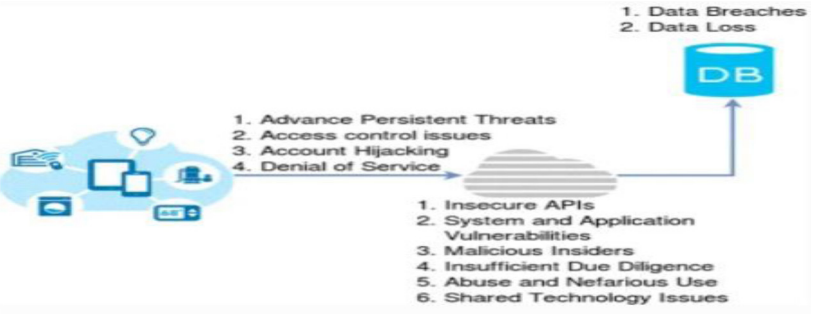

Figure 4

Proposed Methodologies [16]

4. Simulation and result Analysis

In the research review most of the security aspects has been understood by research. The figure 4 describes the market analysis of the fog computing of different applications.

In the research as shown in figure 4 are sure difficulties confronted that will frustrate the general market development. The elements, for example, an absence of a talented labor force and the shortfall of principles and conventions are restricting the market development. Likewise, complex incorporated frameworks and the joining of computer-based intelligence arrangements into the current frameworks is a troublesome undertaking that limits development. Further, the expanded potential for digital assaults because of the expansion of the organization's edge and decentralized figuring prompting intricacy in design is the potential

Figure 5

Segment Analysis of Fog Computing [7]

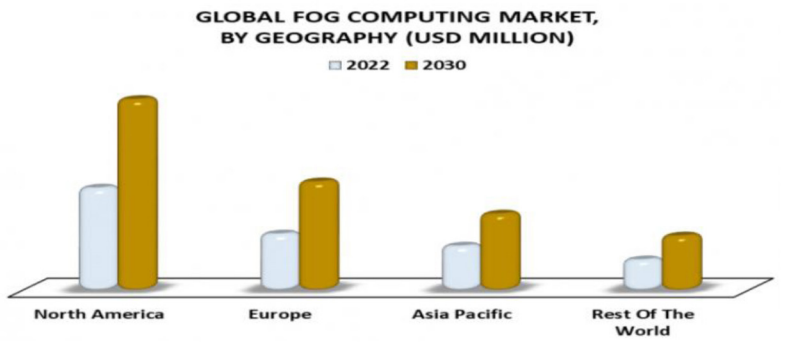

Figure 6

Global Fog Computing Market

restriction hampering the general development of the Worldwide Haze Registering Business sector. The figure 5 defines the analysis of the fog computing model. The Figure 6 shows the Global fog computing market.

In the research shown in figure 5. the Worldwide Haze Registering Business sector is characterized by North America, Europe, Asia Pacific, and the remainder of the world. North America holds the biggest portion of the overall industry. Created economies like the U.S. what's more, Canada has enormous potential for the utilization of the Web of Things. The U.S., furthermore, Canada is among the most in fact progressed nations worldwide. expanding interest in continuous exploration of the advancement of haze design will support the market in the North American district.

Conclusion and Future Work

Abnormality exposure assessments are unquestionably helpful for bending affirmation or infirmity recognizing confirmation coherent assessments where the vehicle of the objective class is astoundingly imbalanced. Peculiarity affirmation assessments are besides to in addition work on the introduction of the model by getting rid of the abnormalities from the status test. Alongside the above-examined computerized reasoning assessments, information experts can relentlessly utilize progressed certified frameworks to oversee peculiarities. Execution issue emerges because of unfortunate security and protection frameworks. In this way, these can be abstained from utilizing haze figuring which is another processing worldview to profit adaptable assets at the edge of the organization to the end-clients. Subsequently, mist registering processes

information closer to where it constructs and addresses the difficulties of increasing the information volume.

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] Rangaiah, Y. V., Sharma, A. K., Bhargavi, T., Chopra, M., Mahapatra, C., & Tiwari, A. A Taxonomy towards Blockchain based Multimedia content Security. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1-4, (2022, December) IEEE.

[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, (2022, December). IEEE.

[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, (2022, December). IEEE.

[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] Tiwari, A., & Garg, R. Orrs Orchestration of a Resource Reservation System Using Fuzzy Theory in High-Performance Computing: Lifeline of the Computing World. *International Journal of Software Innovation* (IJSI), 10(1), 1-28 (2022).

[11] Agrawal S, Agrawal J. Survey on anomaly detection using data mining techniques. Procedia Comput Sci. 60 : 708-13 (2015).

[12] Tiwari, Ashish, and Ritu Garg. "A Optimized Taxonomy on Spot Sale Services Using Mathematical Methodology." *International Journal of Security and Privacy in Pervasive Computing* (IJSPPC) 14, No. 1, 1-21 (2022).

[13] Tiwari, A., & Sharma, R. M. OCC: A Hybrid Multiprocessing Computing Service Decision Making Using Ontology System. *International Journal of Web-Based Learning and Teaching Technologies* (IJWLTT), 16(4), 96-116 (2021).

[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 (2014). Springer, Cham.

[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 (2020). Springer, Singapore.

[16] Patcha A, Park J-M. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Netw., 51(12) : 3448-70 (2007).

[17] Jiang M, Cui P, Faloutsos C. Suspicious behavior detection: current trends and future directions. IEEE Intell Syst., 31(1) : 31-9 (2016).

[18] Kaur, R., Jain, A., & Kumar, S. Optimization classification of sunflower recognition through machine learning. Materials Today: Proceedings, 51, 207-211 (2022).

[19] Kumar, S., Kumari, B., & Chawla, H. Security challenges and application for underwater wireless sensor network. In Proceedings on International Conference on Emerg, Vol. 2, pp. 15-21 (2018, October).