An Enterprise of Cognitive Fog Computing For Disturbance Recognition in Internet of Things

Prashant Kumar Shukla

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur - 522302, Andhra Pradesh, India

Email: prashantshukla2005@kluniversity.in

https://orcid.org/0000-0002-3092-2415

Abstract

The Internet of Things (IoT) is a cutting-edge piece of cybernetic infrastructure that will eventually link all manner of previously disconnected physical objects to the web. The IoT is rapidly expanding into many facets of human life. IoT's attack surface has grown as a result of the technology's hyper-connectivity and inherent heterogeneity. In addition, IoT devices are used in both managed and unmanaged settings, leaving them open to innovative attacks. Fog computing is used in the proposed intrusion detection system for IoT applications to implement intrusion detection in a decentralised manner. Attack detection at fog nodes and summarization on a cloud server make up the proposed system's two parts. The local fog nodes in the IoT environment examine the traffic, and then they send a report to the cloud server that summarises the current global security state of the IoT application. According to the results of the experiments, the fog nodes are able to identify the attack 27% more quickly while also reducing the number of false alarms. The work that has been recommended provides a beginning point for the creation of a fog-based intrusion detection system that can be used for applications related to the IoT. The proposed system has a false alarm rate of only 0.32% and an accuracy of 98.15 percent. The proposed method can only identify attacks that conform to specific patterns.

Keywords: Fog; IoT; ANN; OSELM.

1. Introduction

The Internet of Things (IoT) is a network of interconnected computing devices, services, and people that is built around the use of wireless sensor networks and the Internet. You might think of the IoT as a worldwide network of 'things' that have electronics, software, and sensors built right in. It links together any gadget with a distinct IP address [1]. IoT allows these Internet-connected gadgets to sense, collect, and communicate with one another to enhance human well-being. The goal of the IoT is to place networked, self-aware sensors and actuators everywhere, creating a seamless, seamless user experience. The IoT is expanding rapidly to offer novel services that boost economic and social development. The IoT makes it possible to link any device, anywhere, to any other device, via any network, to provide any service [2].

RFID (Radio frequency identification), M2M (machine-to-machine communication), and WSN (wireless sensor networks) are not ground-breaking technology, but they form the backbone of the IoTs. Wireless sensor networks (WSNs) collect data from the environment via wireless sensors and transmit that data to a collector node, also known as a sink node. After that, an IP address is used to remotely access and administer each sensor node [3]. Internet Protocol later enables direct communication between nodes without the need for intermediary sink nodes. Machine-to-machine (M2M) communication describes the shift towards decentralised, peer-to-peer interactions between devices. While M2M is limited to localised scenarios like home automation and energy management, IoT opens the door to global connections and a plethora of new

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

service possibilities [4]. The integration of various technologies to deliver worldwide service is the revolutionary change brought about by the IoT.

IoT's ability to work with disparate systems and limited-capacity gadgets means it can be put to use in a wide variety of contexts. The automatic device-to-device connectivity made possible by IoT is having an impact on every area of modern life. IoT applications can be broken down into two basic categories: those aimed at consumers and those aimed at businesses [5]. Home automation, smart metres, and wearables are just a few examples of consumer applications. Enterprise software can be used to keep an eye on things like air quality and pollution, manage inventory and utilities, and more.

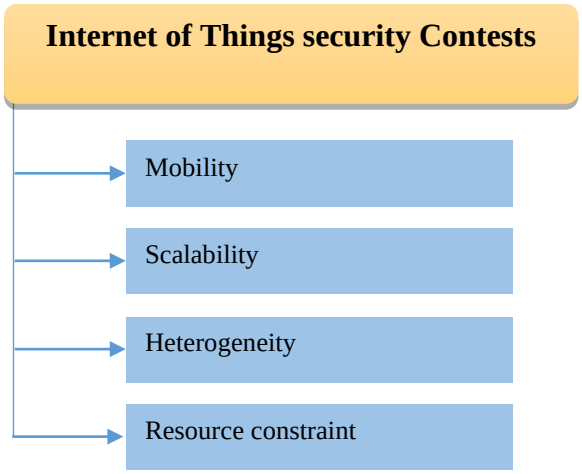

Figure 1: IoT security challenges.

The IoTs collaborates with other human-centric web services, helping the rise of the information economy and digital society through services, the media, and business [6]. There will be 16 billion IoT devices in use by the end of 2020, or roughly six gadgets for every person on the planet. There will be around 40 Zettabytes worth of data sent between users. The exponential expansion of the IoTs creates several opportunities for both consumers and producers in the form of fresh revenue streams, improved operational efficiencies, and novel business models. It will pave the way for widespread use in a variety of fields, including healthcare, inventory management, and environmental monitoring [7]. While the IoT has many potential benefits and uses, it also presents many obstacles to overcome.

The provision of transparent and wide-ranging seamless services with security is the major issue in deploying IoT. With the proliferation of IoT devices, increasing sophistication, and massive amounts of data, it has become a prime target for cybercriminals. Two minutes is all it takes for an attacker to compromise an IoT device, according to the "Internet Security Threat Report" [8]. When an IoT device is compromised, the attackers can utilise it as part of a larger botnet to launch devastating attacks. It is crucial to secure security and privacy in IoT applications as physical things regularly monitor and communicate personal data of our daily lives. If these gadgets are attacked, it might have catastrophic results [9]. Due to its reliance on wireless data transfer, IoT applications must adhere to the same stringent security standards as the Internet and device networks. Immense privacy and security dangers are introduced into IoT applications due to the anticipated pervasive entry of devices and sensors into personal places including the home, the car, and wearable devices [10].

2. Related Work Done:

The need for privacy and security in IoT has been the subject of numerous research. Perimeter defences, according to the study, are insufficient for an IoT setting. In order to develop security instincts and respond effectively to evolving threats, the IoT requires a novel security mechanism capable of analysing and interpreting the huge structured and unstructured data from IoT devices [11].

The authors investigate how current IoT communication protocols and processes fulfil fundamental safety requirements. The future security issues that will arise from deploying IoT are also addressed in this paper [12]. Researchers present an in-depth look at the IoT security and privacy needs, taking into account the network's diverse ecosystem, communication protocols, and enabling technologies. The research

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

demonstrates the importance of combining IoT and communication technologies in a safe middleware in order to meet the security requirements [13].

The effects of the IoT on users' security and privacy from a legal standpoint were examined. To address these concerns, the authors suggest a new security architecture for the IoTs [14]. The pros and cons of using a decentralised method to handle service delivery in the IoTs were investigated by the study's authors. According to their research, both centralised and decentralised methods can exist together to give a secure solution in an IoT setting.

The authors break down the IoT into its constituent parts, or "layers," and explain the unique security issues that arise at each level. In addition, the work examines the security implications of cross-layer heterogeneous integrations. A study examines IP-based IoT architecture's deployment approach and security needs [15-16]. The technological ramifications of using industry-standard IP security protocols in an IoT setting are explored in this paper.

Challenges to security and privacy in industrial IoT systems were investigated. They also offer recommendations for how to improve Industrial IoT security as a whole. A novel security model for the IoTs is proposed by the research team, and it makes use of an integrated systems approach to security and privacy [17]. Identity management, embedded security, and authorisation in IoT applications are the primary objectives of the suggested security paradigm.

Data management, identity management, trust management, and privacy were named as the four most significant obstacles to developing a safe IoTs. Also discussed is how the problems with the IoTs can be fixed by employing embedded and hardware security methods [18].

Security challenges encountered by embedded system designers are investigated. This study discusses the importance of embedded security in IoT hardware. Also covered are countermeasures to these attacks, with a focus on trusted-computing-based methods of tamper-proofing embedded devices [19]. The authors offer a systemic and cognitive strategy for protecting the IoTs. Person, technology, process, and smart item are all portrayed at the apex of a triangular pyramid that serves as a visual representation of IoT security in this work. Four planes stand in for the connections between the nodes [20]. In order to determine where the security holes in the IoT lie, we study the responsibilities of each player and the connections between them in the suggested strategy.

Experts offered a comprehensive analysis of the security challenges posed by the IoTs.In this survey, we look at why safety measures are so important in the IoT world. In addition, the list of active research projects in IoT security is included in this survey [21]. The poll concludes by noting that, due to IoT's conflicting technologies and inadequate communication protocols, no active research projects are taking into account all the security concerns raised. Researchers provided a taxonomy of IoT security attacks. This taxonomy categorises assaults taking into account device-level, protocol-level, hardware-level, and attack-strategy properties of the IoTs. Researchers can have a better grasp of the nature of the many security threats that plague the IoTs thanks to this resource [22]. The authors conducted a literature review of protecting an IoT infrastructure. In this study, we look at eight of the most prominent IoT frameworks and conduct a thorough comparison of them with regards to their suggested design, problems with developing third-party smart apps, and hardware and software compatibility for assuring security.

The development of new security mechanism for IoT environment is still an open subject, according to the state-of-the-art study on the difficulties and necessity of IoT security [23]. Because IoT devices are deployed in both the managed and the unmanaged environment, and because certain undiscovered cyber-attacks may lead to tragedy, the security mechanism for IoT must autonomously identify and defend against the cyber-attacks at a faster pace.

3. The Objective of the research Work:

1). Fog computing for distributed intrusion detection in IoTs applications.

2). The Online Sequential Extreme Learning Machine (OSELM) technique is used to construct an intrusion detection system across a network of fog nodes.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

4. The Proposed Work:

As people's relationships with technology and information grow, the IoT stands on the precipice of a data explosion from millions of linked gadgets. To detect the unknown dangers and to view a broader picture of threats in IoT applications, it is crucial to learn from these huge data to discover the security events and their relationships by correlating the internal and external information. The tremendous rate of change in IoT applications makes traditional learning algorithms inefficient.

The suggested intrusion detection system for the IoTs aims to identify cyber-attacks quickly, accurately, and with a low false alarm rate. Closer to end devices, at the dispersed fog nodes, is where the detecting method is deployed. Because fog nodes are located closer to the end devices, their intrusion detection system can identify attacks more quickly than cloud-based detection methods. In addition, OSELM is utilised in the suggested detection mechanism, which permits faster learning in parallel at remote fog nodes using streaming data given sequentially in an IoT setting. The OSELM's high generalisation power means it can quickly and effectively learn from the dynamic IoT's flowing data.

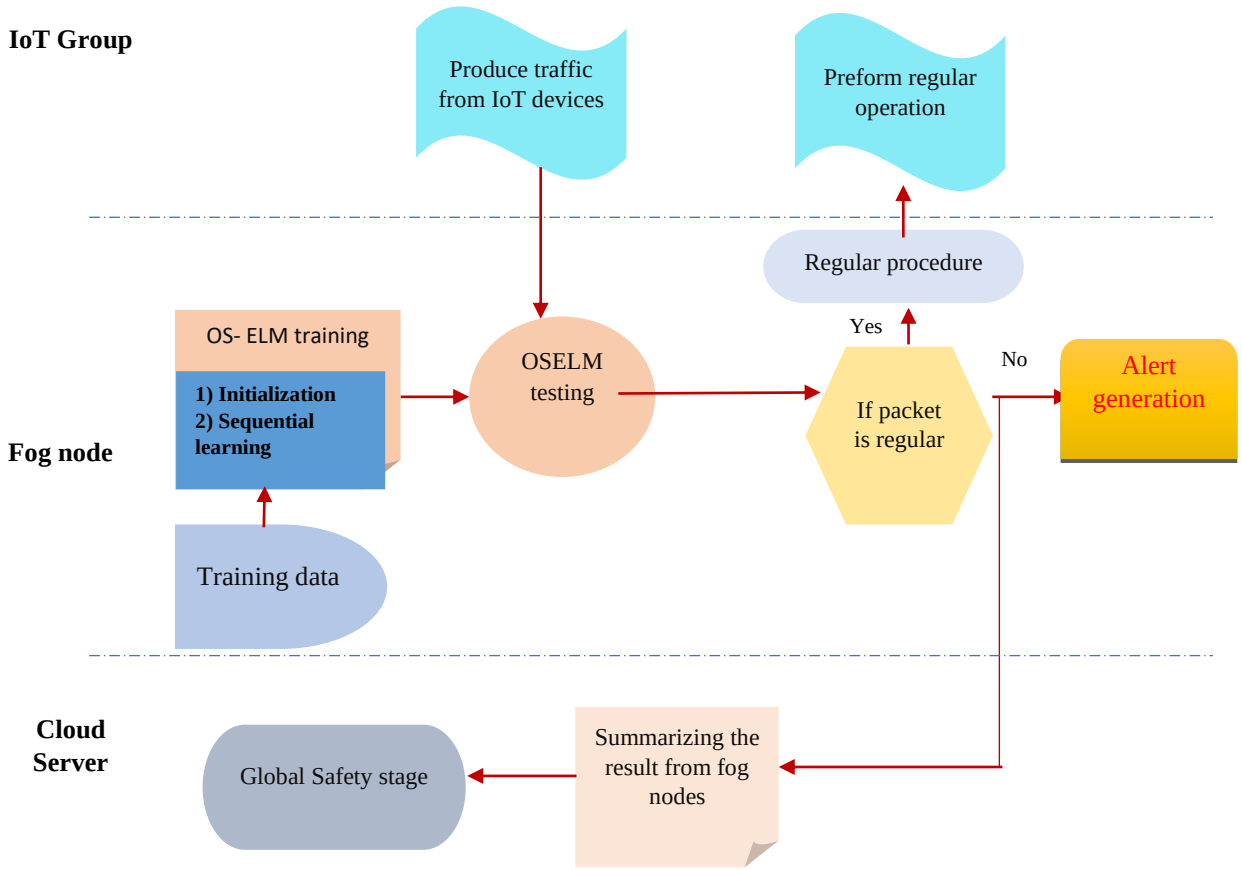

Figure 2: Enterprise process of proposed self-protection system.

Figure 2 depicts a single-hidden-layer feed-forward neural network (SLFN), which can be quickly learned with ELM. Gradient-based learning as it is traditionally practised is too time-consuming for use in real-time settings because of the iterative nature of adjusting the parameters. To get around this issue, ELM uses a random selection of weights and biases on the inputs to analytically calculate the weights on the outputs via straightforward matrix multiplication.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

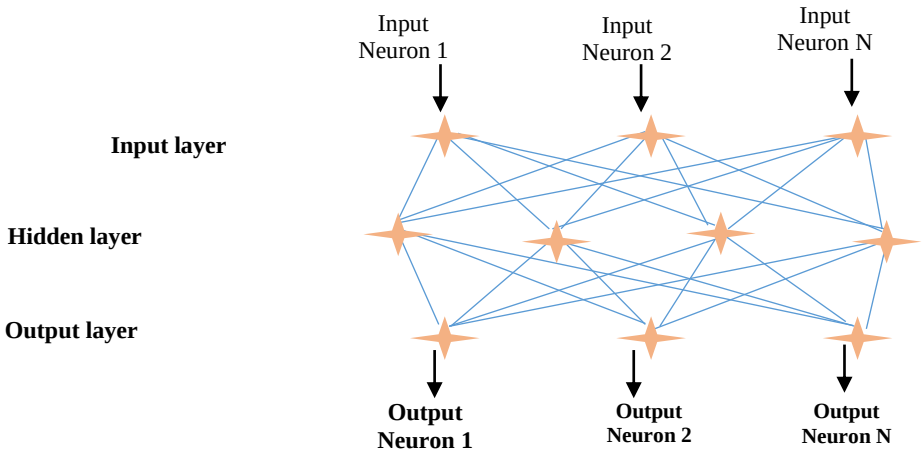

Figure 3: Solesecretedsheet feed forward NN (neural network)configuration.

Attacks in extremely dynamic environments like IoT can be detected with the help of Extreme Learning Machines (ELMs) due to their superior speed of learning. In order to detect cyberattacks in an IoT setting, the online version of the algorithm, known as Online Sequential Extreme Learning Machine (OSELM), can be employed. The cognitive models are decision-making aids that use machine learning algorithms and neural networks to replicate the way humans think. The OSELM algorithm is responsible for providing intelligence in the suggested system.

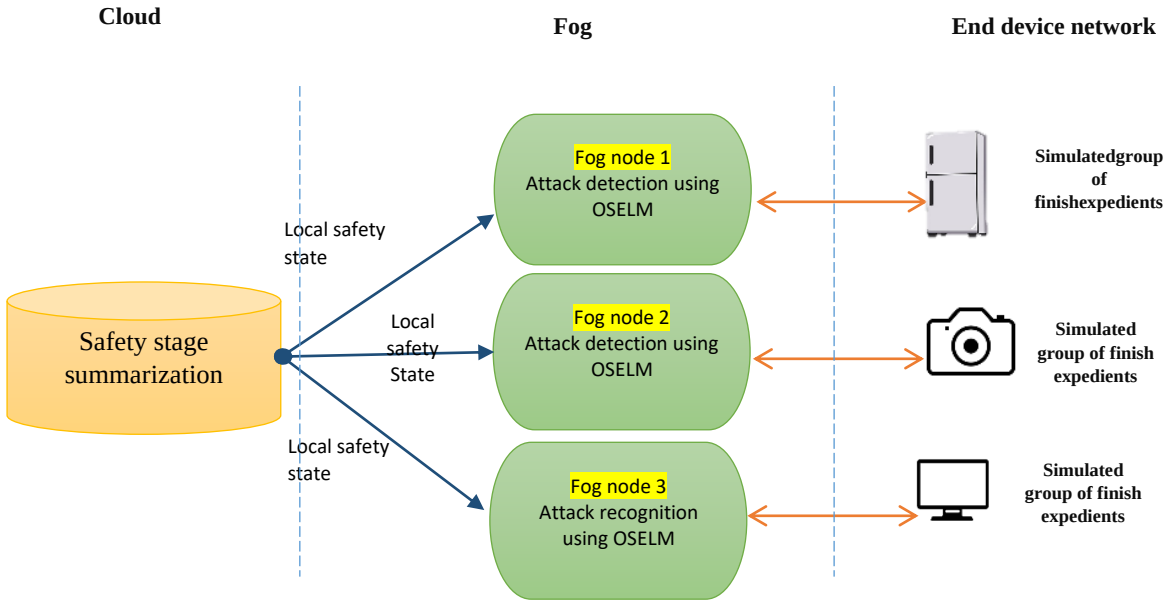

Figure 4: Fog calculatingstructural design

In order to implement intrusion detection in a distributed fashion, fog computing is used in the proposed IoT intrusion detection system. Attack detection at fog nodes and summarization on a cloud server make up the

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

proposed system's two parts. When it comes to managing web-based programmes, the online version of ELM is known as OSELM. Matrix H is used to make adjustments to the standard ELM, with the rank of the hidden neurons being taken to be rank(H) =N. Here we calculate the pseudo inverse of H:

$$H^* = (H^T H)^{-1} H^T \quad (1)$$

The estimation is given as:

$$\hat{\alpha} = (H^T H)^{-1} H^T T \quad (2)$$

The solution of OSELM is the recursive least square algorithm, which is a sequential implementation of the least-square of Equation (2). The first step in OSELM is the initialization phase, and the second is the sequential learning phase. The first stage, "initialization," is very like training in standard ELM, but less information is collected.

The cloud server receives the intrusion data from the fog nodes and uses it to create a global picture of the IoT application's security. To study and visualise the current security state of the IoT application, the cloud server compiles the results from the fog nodes. By employing attacker plan recognition techniques, it is possible to foresee the attacker's next move.

5. Result and Discussion:

Here, the experimental data are used to draw conclusions about the accuracy, reaction time, and network load of the proposed system. The effectiveness of the OSELM algorithm in threat detection is evaluated through the classification outcomes. When this algorithm is deployed to fog nodes, the reaction time for attack detection can be measured and compared to when the method is deployed in the cloud.

5.1. Accuracy:

It is a typical metric for classifying test results numerically. Increased precision indicates a more efficient system.

$$\text{Accuracy} = \frac{TN+TP}{Total\ data\ Sample} X100 \quad (3)$$

5.2. Detection Rate:

The accuracy with which the model places the test data into one of its classes constitutes the present method's sensitivity. How many true positives were successfully detected was the question it addressed. True Positive Rate is another name for it.

$$Senstivity = \frac{TP}{TP+FN} X100 \quad (4)$$

5.3. False Alarm Rate:

The False Detection Rate is defined as

$$False\ Detection\ Rate = \frac{2TP}{2TP+FP+FN} X100 \quad (5)$$

All these parameters are evaluated as compared the performance of the proposed algorithm to the existing algorithm and results are encapsulated in table 1. The accuracy of the proposed system's detection is evaluated in comparison to the accuracy of some existing techniques, such as ANN, Naive Bayes, and conventional ELM.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

Table 1: Enactmentassessment for dualisticarrangement.

Algorithm	Naive Bayes	ANN	ELM	Proposed Method
Accuracy (%)	87.56	95.34	96.12	98.15
Detection Rate (%)	92.05	96.48	97.14	97.89
False Alarm Rate (%)	13.62	5.29	3.34	0.32

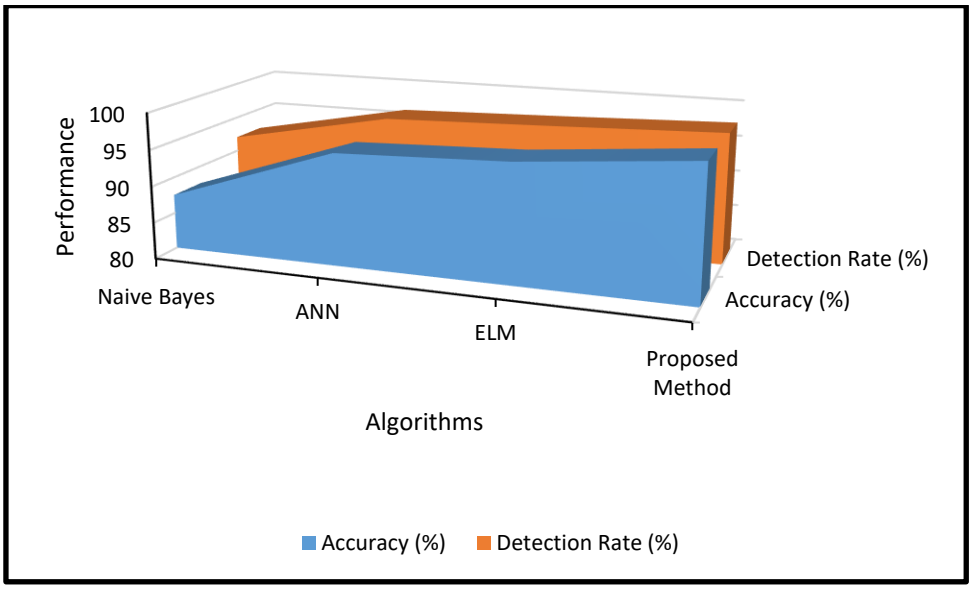

Figure 5: Performance comparison for binary classification.

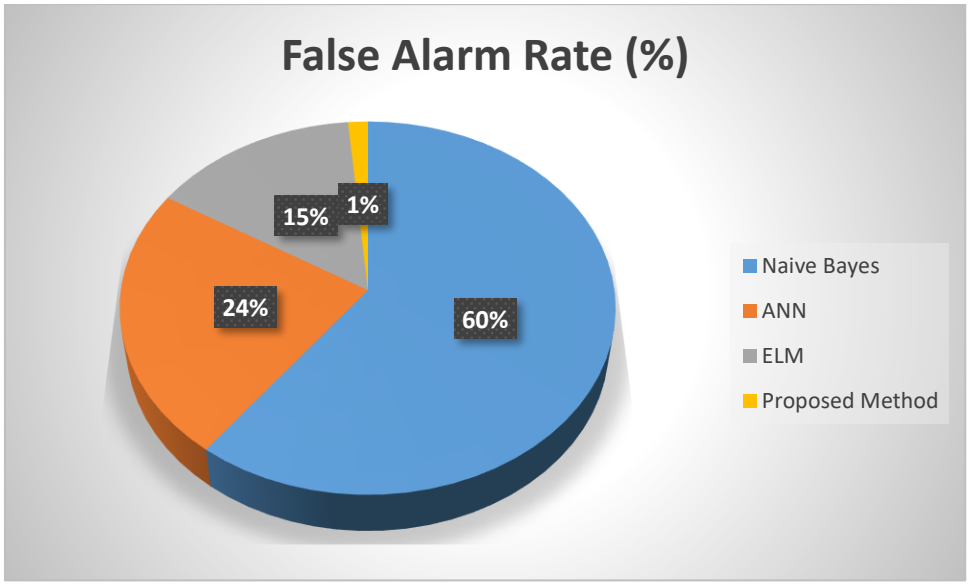

Figure 6: False Alarm Rate Comparison of the proposed method with Existing Approach.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

The proposed system has a false alarm rate of only 0.32% and an accuracy of 98.15 percent. When compared to the previous algorithms, the suggested system's main benefit is its ability to incorporate new data live for learning. OSELM's online learning features allow it to pick up on the ever-changing conditions of IoT applications more quickly. In order to provide a worldwide overview of the security status of IoT applications, local fog nodes identify attacks based on traffic generated from the IoT environment and communicate this information to the cloud server. Compared to a cloud-based version, the fog nodes are 27% more effective in detecting attacks with a much lower false alarm rate.

The assault detection module of the proposed system is also deployed in the Azure cloud service as a centralised system in order to assess the efficacy of the suggested fog computing based intrusion detection system in terms of response time. To demonstrate the effect of OSELM on fog computing for intrusion detection, we compare the latency of the proposed fog based detection system to that of the current cloud based detection.

Table 2: Comparison between fog based detection and cloud based detection in response time.

S. No.	Bandwidths	Response Time (ms)	
		FOG based Recognition	Cloud based Recognition
1	50	12	19
2	200	10	17
3	500	8	15
4	800	7	13
5	1000	5	10

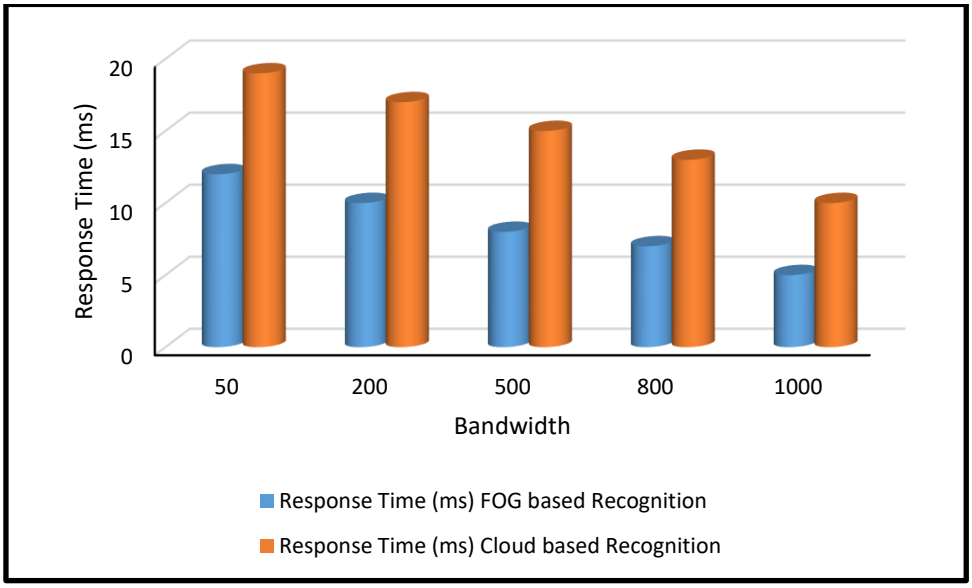

Figure 7: Comparison between fog based detection and cloud based detection in response time.

The proposed system's reaction time is measured against the cloud-based implementation's response time across a range of network throughputs. When compared to cloud-based implementation, the suggested fog-based technique shortens the amount of time necessary to alert end devices of a cyber attack by approximately 27 percent. This is due to the proximity of fog nodes to end devices.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

6. Conclusion and Future Scope

Using fog computing, the proposed IoT self-protection system accurately analyses attacks in IoT traffic and quickly recovers from attack scenarios by activating the proper response. This study reports the results of intrusion detection work done on fog nodes for IoT use. The OSELM technique was used to impart knowledge to neighbourhood fog nodes, which enabled intrusion detection. OSELM's online learning features allow it to pick up on the ever-changing conditions of IoT applications more quickly. The traffic that passes through the IoT environment is evaluated by the local fog nodes, which subsequently send a report to the cloud server that summarises the severity of the assault.

The attack is discovered by the fog nodes 27% faster than it is using the cloud-based approach, and the false alarm rate is 27% lower thanks to the fog nodes. As a first step towards building a fog-based intrusion detection system for IoT applications, the work described here is invaluable. Only attacks with specific, known signatures will be detected by the proposed method.

Towards the goal of creating an autonomous security system for the IoT ecosystem, the design of a fog computing based self-protection system is an important step. Since IoT devices are also deployed in uncontrolled contexts, the true IoT ecosystem requires an autonomic security system with self-configuration and self-managing capacity. Due to the difficulty of doing frequent security upgrades and reconfigurations in unmanaged environments, these devices are more likely to experience security breaches. As a result, the suggested system can be modified to accommodate the autonomous features of self-configuration and self-management.

References:

[1]. Alaba, FA, Othman, M, Hashem, IAT & Alotaibi, F 2017, 'IoTs security: A survey', Journal of Network and Computer Applications, vol. 88, pp. 10-28.

[2]. Diro, AA & Chilamkurti, N 2017, ‘Distributed attack detection scheme using deep learning approach for IoTs’, Future Generation Computer Systems, vol.82, pp 761-768.

[3]. Sedjelmaci, H, Senouci, SM & Al-Bahri, M 2016, ‘A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology’, IEEE International Conference on Communications (ICC), pp. 1-6.

[4]. Alsmadi, A.M.; Aloglah, R.M.A.; Abu-Darwish, N.J.S.; al Smadi, A.; Alshabanah, M.; Alrajhi, D.; Alkhaldi, H.; Alsmadi, M.K. Fog Computing Scheduling Algorithm for Smart City. Int. J. Electr. Comput. Eng. 2021, 11, 2219–2228.

[5]. Yakubu, J.; Abdulhamid, S.M.; Christopher, H.A.; Chiroma, H.; Abdullahi, M. Security Challenges in Fog-Computing Environment: A Systematic Appraisal of Current Developments. J. Reliab. Intell. Environ. 2019, 5, 209–233.

[6]. Wang, J.; Li, D. Adaptive Computing Optimization in Software-Defined Network-Based Industrial IoTs with Fog Computing. Sensors 2018, 18, 2509.

[7]. Zahmatkesh, H.; Al-Turjman, F. Fog Computing for Sustainable Smart Cities in the IoT Era: Caching Techniques and Enabling Technologies—An Overview. Sustain. Cities Soc. 2020, 59, 102139. [8]. Kraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog Computing in Healthcare-A Review and Discussion. IEEE Access 2017, 5, 9206–9222.

[9]. Dar, B.K.; Shah, M.A.; Islam, S.U.; Maple, C.; Mussadiq, S.; Khan, S. Delay-Aware Accident Detection and Response System Using Fog Computing. IEEE Access 2019, 7, 70975–70985.

[10]. Sahil; Sood, S.K. Fog-Cloud Centric IoT-Based Cyber Physical Framework for Panic Oriented Disaster Evacuation in Smart Cities. Earth Sci. Inform. 2022, 15, 1449–1470.

[11]. Mahmud, R.; Ramamohanarao, K.; Buyya, R. Application Management in Fog Computing Environments: A Taxonomy, Review and Future Directions. ACM Comput. Surv. 2020, 53, 1–43.

[12]. Puliafito, C.; Gonçalves, D.M.; Lopes, M.M.; Martins, L.L.; Madeira, E.; Mingozzi, E.; Rana, O.; Bittencourt, L.F. MobFogSim: Simulation of Mobility and Migration for Fog Computing. Simul. Model. Pract. Theory 2020, 101, 188–218.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023

[13]. Javadzadeh, G.; Rahmani, A.M. Fog Computing Applications in Smart Cities: A Systematic Survey. Wirel. Netw. 2020, 26, 1433–1457.

[14]. Villegas-Ch., W.; García-Ortiz, J.; Urbina-Camacho, I.; Mera-Navarrete, A. Proposal for a System for the Identification of the Concentration of Students Who Attend Online Educational Models. Computers 2023, 12, 74.

[15]. Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog Computing Security and Privacy Issues, Open Challenges, and Blockchain Solution: An Overview. Int. J. Electr. Comput. Eng. 2021, 11, 5081–5088.

[16]. Khan, S.; Parkinson, S.; Qin, Y. Fog Computing Security: A Review of Current Applications and Security Solutions. J. Cloud Comput. 2017, 6, 1–22.

[17]. Roy V. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 ,PP. 42-52.

[18]. Zhang, P.Y.; Zhou, M.C.; Fortino, G. Security and Trust Issues in Fog Computing: A Survey. Future Gener. Comput. Syst. 2018, 88, 16–27.

[19]. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues. J. Netw. Comput. Appl. 2017, 98, 27–42.

[20]. Abdali, T.A.N.; Hassan, R.; Aman, A.H.M.; Nguyen, Q.N. Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues. IEEE Access 2021, 9, 75961–75980.

[21]. Margariti, S.V.; Dimakopoulos, V.V.; Tsoumanis, G. Modeling and Simulation Tools for Fog Computing-A Comprehensive Survey from a Cost Perspective. Future Internet 2020, 12, 89.

[22]. Joseph B. Awotunde , Hrudaya K. Tripathy , Anjan Bandyopadhyay, Hybrid Particle Swarm Optimization with Firefly based Resource Provisioning Technique for Data Fusion Fog-Cloud Computing Platforms, Fusion: Practice and Applications, Vol. 8 , No. 2 , (2022) : 25-35 (Doi : https://doi.org/10.54216/FPA.080203)

[23]. Tuli, Shreshth & Mirhakimi, Fatemeh & Pallewatta, Samodha & Zawad, Syed & Casale, Giuliano & Javadi, Bahman & Yan, Feng & Buyya, Rajkumar & Jennings, Nicholas. (2023). AI augmented Edge and Fog computing: Trends and challenges. Journal of Network and Computer Applications. 216. 103648. 10.1016/j.jnca.2023.103648.

DOI: https://doi.org/10.54216/IJWAC.070102
Received: January 13, 2023 Revised: April 15, 2023 Accepted: May 14, 2023