ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

AN INVESTIGATION OF INTEGRATING THE EDGE OF THINGS, IOT AND CLOUD IN A DISTRIBUTED COMPUTING ENVIRONMENT

V Ravi Kumar* and Dr. Kailash Patidar
Department of Computer Science Engineering, Dr. A. P. J. Abdul Kalam University, Indore (M.P.), India 452016

ABSTRACT
Business 4.0, usually referred to as the fourth industrial revolution, aims to achieve automation, dependability, and control in industrial production and manufacturing environments by promoting the mass adoption of smart computing and network technologies. It entails developing an Industrial Internet of Things system. (I-IoT). I-IoT is concerned primarily with deploying the Industrial Internet of Things (IoT) in the industrial system environment to enable connectivity of everything, everywhere, and at any time in order to boost productivity, efficiency, safety, and awareness . These techniques could potentially broadcast into additional difficulties and problems related to network dynamics, increasing latency and traffic as well as the networking reaction time overhead. A paradigm shift dubbed edge computing (EC) is offered to open the door for the development of modern apps and services in order to avoid these connection issues and achieve the greatest degree of resource utilization. Several Iot systems, including smart grid, smart traffic lights, smart cities, and smart cars, are qu ickly upgrading their applications using EC, which vastly improves reaction time and saves internet bandwidth. Despite the fact that that EC moves workloads from a cloud architecture to the edge, research is still being done on how EC and the cloud compare in terms of aspects like resources development and compute performance. The application of pattern recognition in a I-IoT environment, as well as unique problems and the need for more study in the areas of computing, networking, and control systems, are what we highlight in our findings.

Keywords: Network technologies, manufacturing environments, Internet of Things, industrial system environment, edge computing (EC), cloud architecture, machine learning, I-IoT setting.

1. INTRODUCTION
The surveillance and control capabilities of physical systems can be improved by using contemporary information and communication technologies (computation, control, communication, etc.) IoT depends on the sophisticated networking of hardware, software, and services that spans several protocols, domains, and use cases. As well as permitting state of the art applications like Smart Environments, it is expected to acquire mechanization in practically all enterprises. As another worldview for IoT, a decentralized organization of helpful brilliant items (SOs) is arising (Alaba, 2017). As they move freely, cooperate, and trade information with different sorts of electronic gadgets and human clients, SOs can detect/activate, store, and decipher data created inside themselves and encompassing the close by outside climate where they are situated. Because of its remarkable presentation in offering constant information examination, modest functional expenses, extraordinary versatility, diminished dormancy, and improved nature of administration, EC has cut itself a situation in the specialized world (QoS). Because of its uncommon handling power, EC will change various businesses, including online business, interpersonal organizations, medical care, training, and transportation. By 2020, there will probably be in excess of 20 billion arranged or connected IoT gadgets, as per concentrate on information from Gartner Inc. The McKinsey Global Institute has predicted that by 2025, the combined economic effect of IoT and EC gadgets will be $11 trillion (Alsubhi Khalid, 2012).

1.1 Internet of Things
The Internet of Things (IoT) is a concept that uses wireless sensor networks and the Internet as its main technologies to create a virtual network that communicates with the physical world. IoT is also known as a worldwide network of "things" that have sensors, electronics, and software built into them. It links the gadgets whose IP addresses may be used to uniquely identify them. IoT makes it possible for these online, linked gadgets to detect, gather, and interact with one another to enhance quality of life (Barroso,

2013). In order to create a pervasive environment and a ubiquitous experience, intelligent sensors and actuators will be deployed. IoT is expanding quickly to offer a new level of services that boost societal and economic development. As demonstrated in Figure 1. IoT enables connectivity with anything or anybody at anytime, anywhere, by any network, for any service. with different administrations like the haze of incorporated data places.

The I-IoT organization, a regular CPS, is comprised of both physical and digital frameworks. Digital frameworks' control, systems administration, and processing foundations empower the activity, knowledge, and correspondence of modern frameworks. Actual frameworks are assembling and computerization frameworks that utilize modern hardware to do specific creation and robotization undertakings. Different I-IoT research drives have been done as of late (figuring out the I-IoT framework as a general rule, exploring explicit issues in I-IoT, utilizing cutting edge strategies for I-IoT, and so on.). Involving an enormous drug mind boggling as a contextual analysis, for example, one review took a gander at the issues and exploration holes in I-IoT information the board. In their examination of a particular I-IoT issue, Sun et al. likewise tended to the trust issues in asset distribution while utilizing sell off based procedures to deal with the figuring asset allotment issue. Various examination projects have likewise utilized state of the art I-IoT correspondences innovation incorporate 5G and programming characterized organizing (SDN) (Lin J, 2017).

1.2 Again, for Iot Technology, Enable the Right-Provisioned Microcontroller Technology.

A variety of modern embedded system microprocessors' microarchitecture features are analysed, and the microprocessors' suitability for IoT computing is assessed using several assessment criteria. Due to the anticipated rise of the IoT, an increasing quantity of study is focused on comprehending and discovering insights into numerous IoT features. The processing power and hardware of the edge nodes must be taken into account in the context of edge computing. A virtual platform called fog computing is suggested as a way to connect edge nodes and cloud computing data centres for networking, computation, and storage. Fog computing reduces latency and bandwidth bottleneck by relocating calculations closer to the edge nodes. If the edge nodes have sufficient computational power, data transmission will be minimized, resulting in a decrease in latency, power consumption, and bandwidth bottleneck. Edge mining has the ability to decrease the quantity of data transferred, which will decrease the amount of power used and the amount of storage needed (Amin SO, 2009).

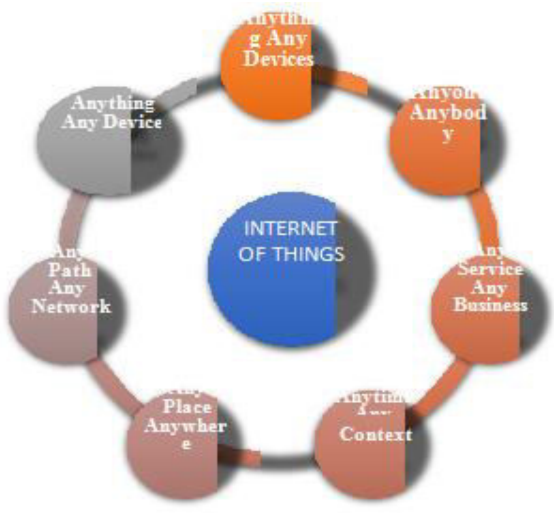

Figure: 1 Connectivity in internet of things Currently, traditional methods for providing EC services seldom concentrate on the applications' manageability, robustness, efficiency, and scalability. The new writing assessments on EC centre for the most part around the calculation and engineering of the method as opposed to on the exhibition of EC. A study on programming characterized organizing and its application is completed in a joint effort with Tc (Bonomi, 2012). A portrayal of versatile edge networks is given, alongside subtleties on their ability for imparting and registering. Different investigations have been done that examine the design of EC, yet they just spotlight on its principles and difficulties; not a solitary one of them explicitly talk about how well EC functions

1.2.1 IoT Application's Functions Classifications:

Several application domains are offered computing potential by the IoT. The application domains include healthcare, logistics and transportation, smart environments, social and personal domains.

- Sensing
- Communications
- Image processing
- Compression
- Security
- Fault tolerance

1.3 Cloud Computing Technologies and Systems

This section will present the systems and technologies that serve as the foundation for cloud computing solutions as well as the function that communication networks play in such solutions. A brief overview of programs targeted at the development of cloud computing solutions is presented, and the timeliness of the proposed notion of cloud communications is explained. Additionally, technologies like operating systems, grid computing, and communication features like IPv6 networking are assessed. Delivering computer and storage resources as a service to a group of end customers is known as cloud computing. By fusing user data, software, and on-demand computational resources over a network, cloud computing further broadens the idea of IT services. Similar to a utility (like the power grid), it depends on resource sharing to create coherence and economies of scale over a network (typically the Internet). The broader idea of integrated infrastructure, virtualization, and shared services forms the basis of cloud computing (Ammar, 2018). The layer - based technique verifiably accepts that exceptionally huge server ranches, which are intended to convey ideal productivity through economies of scale and computerization, are utilized to make the IaaS layer of Public Clouds. Expensive Storage Area Networks (SAN) gear naturally maintains the IaaS layer of Private Clouds. A couple of drives are underway, including the Open Cloud Computing Interface working party of the Open Grid Forum, the Distributed Management Task Force (DMTF) Open Cloud Standards Incubator, and the Cloud Storage Technical Work Group of the Storage Network Industry Association. The principal Open Source Cloud Computing Stack, which incorporates IaaS, PaaS, and SaaS with a normalized set of advances outfitted at elite execution and crucial applications, is upheld in France by the Free Clouds Alliance.

1.4 Distributed and Decentralized Systems

Because most of the concerns discussed by strategic planning algorithms have previously been resolved or can be avoided at the implementation level, the development of cloud- based computing systems is based on research conducted over many years in the fields of parallel and distributed computing (u G, 2017). The accompanying ideal models are extended by the cloud framework, which is a development of conveyed registering frameworks:

A. Grid computing systems,

B. Useful computing (Computer processing systems as utilities),

C. Autonomous computing systems, Internet computing (systems that use the Internet for calculations),

D. Edge processing (Computing systems at the network perimeter),

E. Green technology (Computing systems with low environmental impact).

The problem of communications and the change of existing programs to adapt these to the SaaS is another crucial element. The P2P volunteer hardware and computer helped to establish distributed computing systems and something via, as we shall explain in the following section.

2. **NETWORKING SYSTEMS IN I-IOT** Machinery may gather and share data among themselves to support a variety of smart-world systems, including the smart grid, smart manufacturing, and many more, as shown in fig.

2. These machine gadgets' association is alluded to as M2M collaboration, otherwise called machine-type correspondence, which maintains unpreventable accessibility between machine contraptions without human participation. M2M has been recognized as an essential development for the inevitable destiny of correspondence, nearby imaginative work on the Long-Term Evolution (LTE) and Long-Term Evolutionary Advanced (LTE-A) standards by the Third Generation Partnership Project (3GPP) and the fifth-age remote organization (5G).

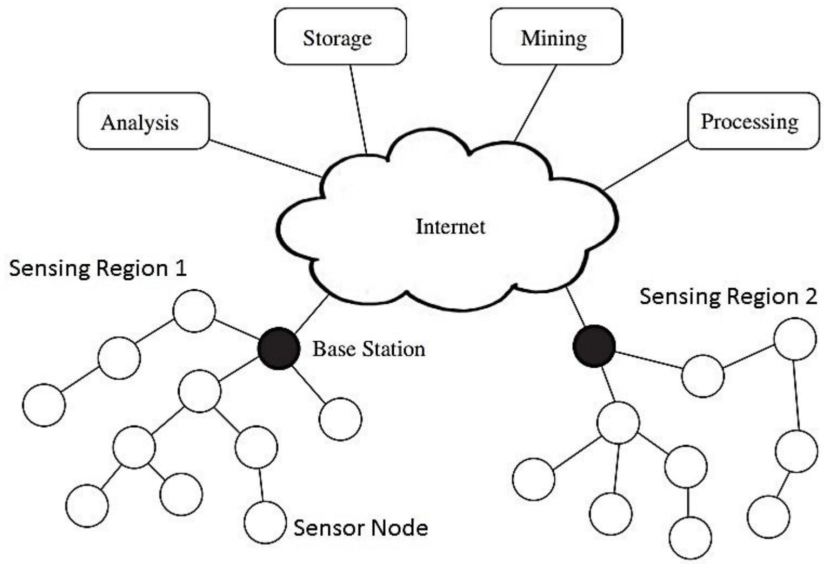

Figure: 2 Communication in I-IoT Nomenclature

2.1 Computing Systems in I-Iot

2.1.1 Overview

The advancement of processing framework that can give huge information figuring and stockpiling for machine gadgets as the need might arise for savvy world frameworks, including shrewd assembling frameworks, is pivotal according to the point of view of registering foundation since machine gadgets have restricted computational and stockpiling limit (Lu Y, 2017). The utilization of distributed computing to machine gadgets is compelled by a unified design for two reasons. Initial, a sizable measure of information created by a few machine gadgets scattered across various geological regions will be moved to a focal cloud, possibly overpowering the organization framework. Second, there might be significant inactivity during information transmission on the grounds that the brought together cloud is regularly arranged a long way from machine gadgets. for different frameworks in the shrewd world. portray in figure 3.

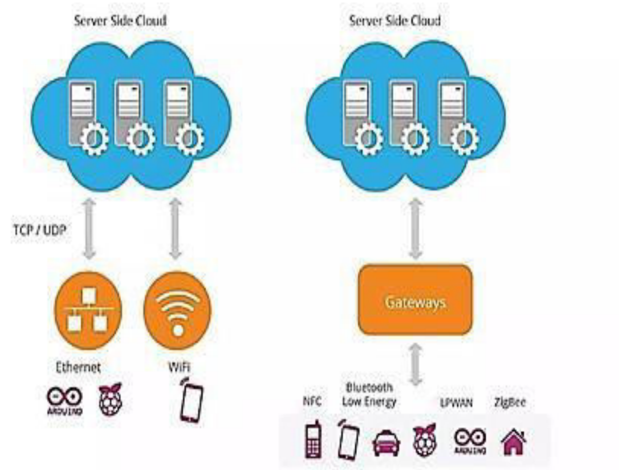

Figure: 3 Construction of Cloud Computing for I-IoT

2.2 Edge Computing

Information technology, on the contrary hand, made use of computational capabilities from network edge devices. Since they are typically situated close to end devices, edge computing can offer computing services with significantly lower latency performance when compared to cloud computing. The concentric handling thought was given regard to general edge enlisting (CCM). In the edge layer of a multi- layer designing, the CCM conveys the multi- granular reliable computational devices and systems. The introduction of contraptions and systems, the real areas of sensors, devices, servers, and server ranches, as well as the display requirements of gigantic data assessment applications, including move speed utilization, inactivity, resource viability, etc, are evidently viewed as in the arrangement of the CCM. Furthermore, the troubles of constant information streaming and examination, information investigation and joining, and security issues were investigated (Bonomi F. M., 2014).

2.3 Hierarchical Computing Architecture

We present an illustration of how to use a multi- tier edge computing architecture that is also hybrid. As illustrated in the figure, processing data from industrial facilities can be assisted by edge computing resources (such as mobile devices, edge nodes, and others). The multi-level edge registering design can proficiently bring down the inactivity of information handling by using the figuring capacities at near end gadgets. By moving some handling cycles to and from the cloud, the multi-level plan can likewise increment PC productivity. This considers the handling of high need and deferral delicate positions locally and low need and postponement lenient errands on the cloud, as found in figure 4. Reconciliation of multi-level edge and I-IoT or half breed cloud, edge registering, and I-IoT structures requires broad top to bottom exploration and reasonable testing.

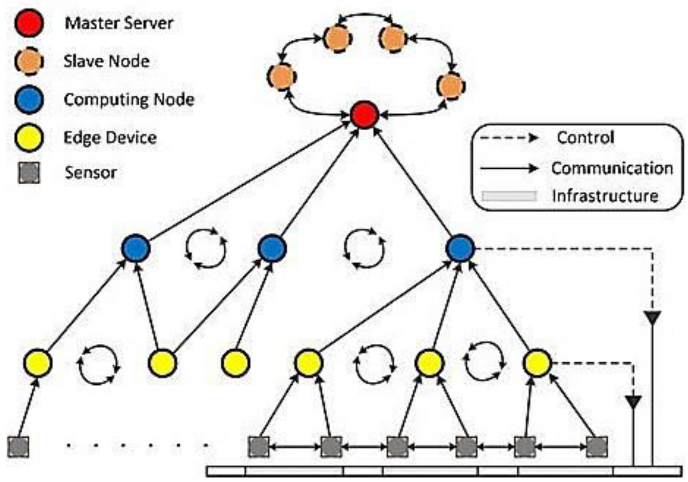

Figure: 4 Hierarchical Computing Architecture

3. REVIEW OF LITERATURE

Granjal et al. (2015) investigates how the current protocols and communication systems satisfy the fundamental security criteria in IoT communication. This work also addresses the various future security challenges involved in implementing IoT.

Sicari et al. (2015) provides a detailed analysis of security and privacy requirements of IoT considering its heterogeneous environment, communication standards and technologies. The study shows the need for integration of IoT and communication technologies in a secure middleware to satisfy the protection constraints. **Sadeghi et al. (2015)** studied the security and privacy challenges in industrial IoT system. They also provide possible solutions for a holistic security framework for Industrial IoT system.

Barbar et al. (2010) proposes a new security model for IoT involving the integrated systems approach for providing privacy and security. The proposed security model mainly focuses on identity management, embedded security and authorization in IoT applications.

Ammar et al. (2018) In this survey, eight main frameworks of IoT are considered and a detailed comparative analysis is performed considering their proposed architecture, issues in development third-party smart applications, hardware and software compatibility for ensuring security.

4. RESEARCH METHODOLOGY

4.1 Introduction

The IoT's exponential expansion in connected devices has expanded the possibility for assaults. To completely tackle the capability of IoT, various state of the art advancements, including distributed computing, haze figuring, programming characterized organizing, huge information examination, and savvy sensors, have been made.

4.2 Extreme Learning Machine

Perceptron with a single invisible layer it feeds backwards (SLFN) seen in Figure 4.2 uses the quick learning algorithm ELM. Due to the lengthy iterations required for parameter tweaking, classical gradient-based learning is slow and unsuitable for real-time applications. In order to compute the output weights analytically using straightforward matrix calculations, ELM overcomes this challenge by selecting the input weights and biases at random.

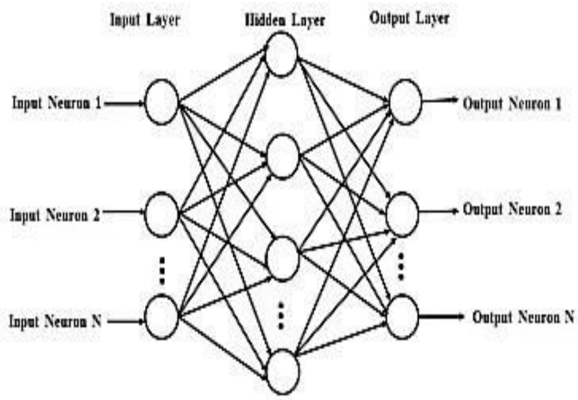

Figure: 4.1 architecture of a one-layer hidden neural feed forward network

4.3 Evaluation

This section provides the experimental setup and the dataset used to evaluate the proposed method.

4.3.1 Experimental Setup

Computer with the specifications DUAL CORE microprocessor, 1 GB RAM, and 200GB HDD are used as a Proof-of-Concept for the proposed system, As demonstrated by the fog nodes in fig. 4.3.1, the computers are connected to the Azure cloud service using 4xDual-Core AMD Opteron 2218 processors with an 8-core clock speed, 32GB of RAM, and Six X 146Mb of ram hard drives. Linux was put to use using MATLAB (R2013a).

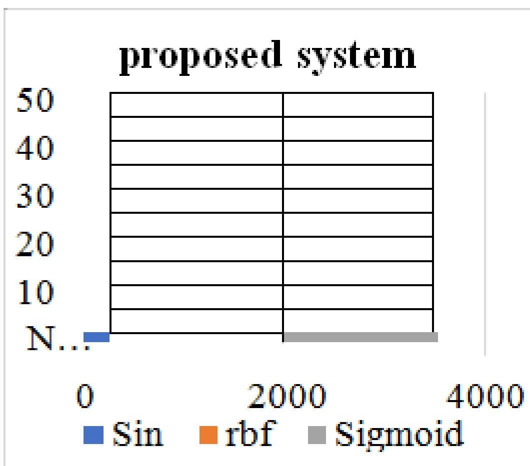

Figure: 4.3.1 Experimental Setup

Table: 1 Experimental Setup

Chunk size/	SIN	RBF	SIGMOID
Neurons	500	1000	**2000**
5	55.3	60.4	**57.1**
10	62.7	70.2	**63.4**
15	68.4	75.4	**70.5**
20	72.1	80.1	**77.6**
25	79.5	88.8	**80.1**

30	85.1	85.7	**86.3**
35	88.2	92.9	**91**
40	90.1	91.3	**91.6**
45	90.6	90.8	**89.9**
50	**91.2**	**90.6**	**90.3**

4.3.2 Dataset

Reported that Denial of Service attacks are frequently integrated within IoT ecosystem such as smart grid, smart cities etc. The attackers use the interconnectivity among the smart objects with limited protection to launch DoS attack easily. DoS attacks are usually identified by overwhelming a single node from multiple sources which can most frequently occur in IoT ecosystem. Due to this, the recommended system is investigated using the NSL KDD benchmark dataset. The collection contains assaults that normally happen in the IoT ecosystem.

Separate training and test records are included in the dataset. equipment records comprise up the training set, whereas 22,544 records with 41 features make up the test set. As demonstrated in Tables 2 and 3, the dataset may be modelled for binary classification with two classes and multi-class classification with four classes. In Figures 4.3.2 and 4.3.3, the most significant attacks discovered in the IoT context are contrasted to assaults in the NSL-KDD database.

Table 2: frequency of binary class entries

Records	Training	Test
Normal	61343	**9721**
Attack	58620	**12733**
Total	**125953**	**22545**

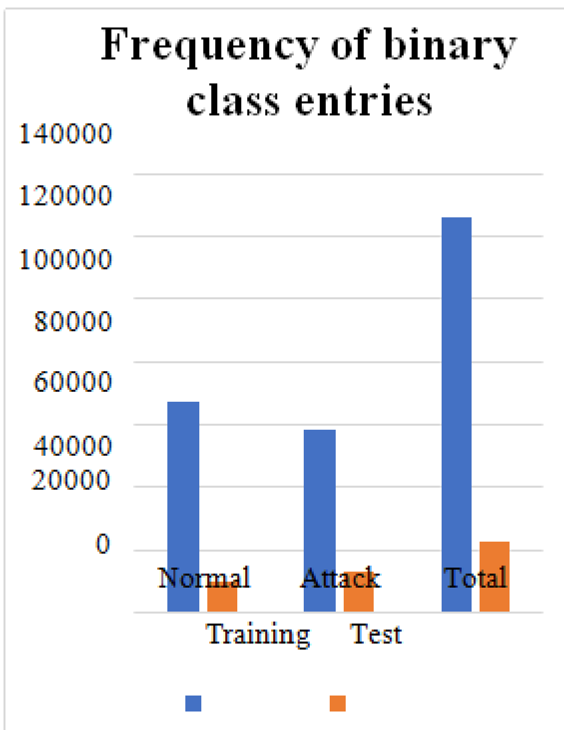

Figure: 4.3.2 frequency of binary class entries

Table 3: Total count archives for non - linear and non-categorization

Records	Training	Test
Normal	67323	**9411**
Dos	45927	**7258**
Probe	11856	**2754**
R2L	995	**2432**
U2R	42	**330**
Total	**125473**	**52544**

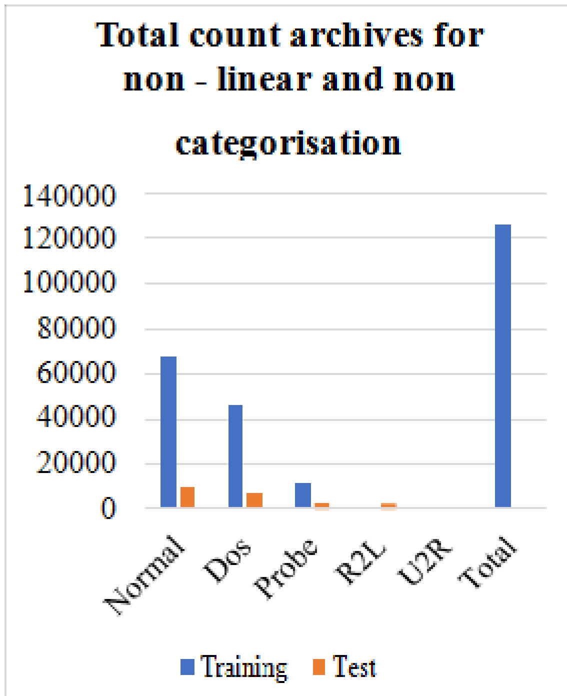

Figure: 4.3.3 Total count archives for non - linear and non-categorization

5. RESULTS AND DISCUSSION

5.1 Accuracy

Condition 5.1's precision, discovery rate, and deception rate are utilized to ascertain the proposed framework's location exactness (1,2,3). Make the use of the disarray lattice, which includes values for True Positive (TP), True Negative (TN), Untrue Positive (FP), and False Negative (FN). The recommended approach achieves 97.36% accuracy with a 0.37 percent reduction in erroneous alert rate after around 13 seconds of learning.

Predicted

actual	**Attract**	**Normal**	
	Normal	TN	FP
	Attack	FN	TP

$$\text{[illegible]}y = \frac{TP + TN}{TP+T[?]+FP+FN}$$

(1)

$$\text{[illegible]} = \frac{TP}{TP+FN}$$

(2)

$$\text{[illegible]} = \frac{[?]TP}{[?]T[?]+F[?]+FN}$$

(3)

5.2 Response Time

The assault identification module of the created structure is likewise sent in the Azure cloud administration as a concentrated framework to look at the exhibition of the recommended haze registering put together remote checking framework with respect to the premise of pace of response. To exhibit the impact of OS-ELM on haze figuring for interruption identification, the inertness of the proposed mist-based location framework and the ongoing cloud-based recognition are evaluated. As illustrated in

Figure 5.2, the suggested system's reaction time is contrasted with a cloud-based implementation using various network bandwidths. Due to the planned fog-based approach's greater proximity to end devices than the cloud-based implementation, the reaction time to notify a cyberattack is now about 25% lower.

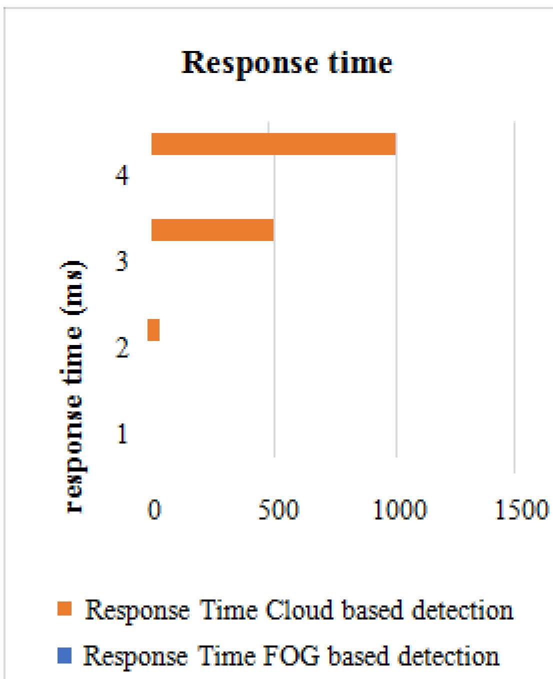

Figure: 5.2 Performance times for fog-based recognition and cloud-based detection are compared.

Table: 4 The response time to report

Response Time	
FOG based detection	Cloud based detection
0	1
5	50
10	500
15	1000

6. CONCLUSION

In this paper, the mist figuring based self- assurance framework in IoT climate was proposed. The proposed framework utilizes the critical benefit of haze figuring predominantly inactivity decrease and diminished data transmission utilization for carrying out the security framework for IoT. The proposed self- protection system in IoT using fog computing intelligently interprets attack from IoT traffic with high accuracy and efficiently recovers from the attack scenario by activating appropriate response at faster rate. The attacks with known and unknown attack signatures are efficiently interpreted by OS-ELM algorithm and distributed Gaussian Process Regression algorithms. The IoT environment's fuzzy data is used by the fuzzy-inference system to choose the best answer.

In this paper, we provide a complete analysis of I-IoT from a CPS viewpoint, concentrating on control, systems administration, and processing. Control frameworks are anticipated for a vast array of today 's technology in the Internet of Things (sensors, actuators, gear, and so on.). In industrial systems, networking systems provide for the timely transfer of data and control signals for a variety of scattered operations. Computing systems offer the computational infrastructure necessary for reliable, timely, and efficient data gathering, storage, processing, and analysis.

Before building and running real-time applications. for example, careful planning and testing of the computer technology must be done due to the high implementation costs.

REFERENCES

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

2. Alsubhi Khalid, Issam Aib & Raouf Boutaba 2012, 'FuzMet: A fuzzylogic based alert prioritization engine for intrusion detection systems', International Journal of Network Management., vol. 22, no. 4, pp. 263-284.

3. Barroso, LA, Clidaras, J & Holzle, U 2013, 'The datacenter as a computer: An introduction to the design of warehouse- scale machines', Synthesis Lectures on Computer Architecture, vol. 8, no. 3, pp. 1-154.

4. Bonomi, F, Milito, R, Zhu, J & Addepalli, S 2012, 'Fog computing and its role in the internet of things', Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13-16.

5. Lin J, Yu W, Zhang N, Yang X, Zhang H, and Zhao W, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

6. Amin SO, Siddiqui, MS, Hong, CS & Lee, S 2009, 'RIDES: Robust intrusion detection system for IP-based ubiquitous sensor networks', Sensors, vol. 9, no.

7. Ammar, M, Russello, G & Crispo, B 2018, 'Internet of things: A survey on the security of IoT frameworks', Journal of Information Security and Applications, vol. 38, pp. 8-27.

8. Xu G, Yu W, Griffith D, Golmie N, and Moulema P, "Toward integrating distributed energy resources and storage devices in smart grid," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 192–204, Feb 2017.

9. Lu Y, “Industry 4.0: A survey on technologies, applications and open research issues,” Journal of Industrial Information Integration, vol. 6, pp. 1–10, 2017.

10. Bonomi, F, Milito, R, Natarajan, P & Zhu, J 2014, ‘Fog computing: A platform for internet of things and analytics’, Springer International, pp. 169 -186.

11. Jeong S, Na W, Kim J, and Cho S, “Internet of Things for smart manufacturing system: Trust issues in resource allocation,” IEEE Internet of Things Journal, 2018.

12. Columbus L, “Roundup of Internet of Things forecasts and market estimates, 2016.

13. Lee I. and Lee K, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol. 58, no. 4, pp. 431–440, 2015.

14. Centenaro M, Vangelista L, Zanella A, and Zorzi M, “Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios,” IEEE Wireless Communications, vol. 23, no. 5, pp. 60–67, 2016.

15. Li B. and Yu J, “Research and application on the smart home based on component technologies and Internet of Things,” Procedia Engineering, vol. 15, pp. 2087– 2092, 2011. [Google Scholar]

16. Jie Y, Pei JY, Jun L, Yun G, and Wei X, “Smart home system based on IoT technologies,” in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013, pp. 1789–1791.

17. Santoso FK and Vun NC, “Securing IoT for smart home system,” in Consumer Electronics (ISCE), 2015 IEEE International Symposium on. IEEE, 2015, pp. 1–2. [Google Scholar]

18. Yun M. and Yuxin B, “Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid,” in Advances in Energy Engineering (ICAEE), 2010 International Conference on. IEEE, 2010, pp. 69–72.

19. Gartner ‘Gartner Says 6.4 Billion Connected ‘Things’ Will Be in Use in 2016 Up 30 Percent From 2015.

20. Mckinsey ‘By 2025 Internet of Things Applications Could Have \$11 Trillion Impact, 2015.

21. K. Cassar, White Paper: Amazon Echo: Seattle’s Sonic Boom is Felt Beyond e- Commerce, San Mateo, CA, USA:Slice Intelligence, Inc, Apr. 2016.

22. M. M. Michaels, White Paper: The Apple Watch Case Study: What We Can Learn and Apply From an Affordance Analysis, Fairfield, LA, USA, Nov. 2015.

23. B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka and T. Turletti, "A survey of software-defined networking: Past present and future of programmable networks", IEEE Commun. Surveys Tuts., vol. 16, pp. 1617-1634, Feb. 2014.

24. S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang and W. Wang, “A survey on mobile edge networks: Convergence of computing caching and communications”, IEEE Access, vol. 5, pp. 6757-6779, 2017.

25. P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading", IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1628-1656, 3rd Quart. 2017.