DESIGN AND IMPLEMENTATION OF DEEP LEARNING ALGORITHM USING FOG COMPUTING FOR SECURE IOT ENVIRONMENT

First A. Deepak Kumar Yadav†

Research Scholars, Department of Computer Science and Engineering, SAGE University, Indore, Madhya Pradesh, India,

Second B. Manoj Kumar Ramaiya

Associate Professor, Institute of Advance Computing, SAGE Unviersity, Indore, Madhya Pradesh, India,

Abstract

Because there are now more connected devices than ever before in important industries like healthcare and the power grid, the definition of what is considered "critical infrastructure" has changed. As the world becomes more mobile and connected, new critical industries are becoming more and more connected to each other. This is because more and more people want information that can be accessed easily and quickly. Because of this, it is important to understand the challenges that must be overcome to secure the future digital infrastructure while it is still being built.

After showing the framework that makes big data, the functionality-based fog architecture is then built. Also, an in-depth look at the security requirements that IoT systems that use fog technology must meet is given here. After that, we look closely at the issues of data security and trust that come up when fog computing makes the Internet of Things possible. This study lays out the rules for the current task, comes up with rules for protecting a lot of data, and sorts the possible threats to Internet of Things (IoT) fog installations into groups.

Keywords : Deep Learning , IoT Environment , Fog Computing

Introduction

More and more people are talking about the Internet of Things (IoT), which is a topic that is interesting in many different fields, including business and academia. Most people think that the Internet of Things (IoT) is a network of connected electronic devices (or "things") that can talk to each other, share information, and do tasks either on their own or together through remote servers (the "cloud"). By sending information to the cloud, these "smart" objects are better able to interact with and adapt to their surroundings.

With the rise of Internet of Things technologies in service-oriented computing, software companies that focus on giving their users a variety of real-time services have found that they have a lot of room for growth. This option is available in a wide range of settings. Supporters of the Internet of Services (IoS) say that current Internet of Things (IoT) apps should collect and analyse user data to make services that are highly personalised and aware of their context. For the process to work, devices and the cloud will need to talk to each other. The "cloud computing" method, which is popular right now, has been shown to be useful in many different ways. One of the benefits is that you can "pay as you go" for high-volume server, storage, and network resources. This can help people and businesses lower their overall costs. By moving their most important apps to the cloud, users can take advantage of cloud computing's flexibility, low cost, and reliability when it comes to application management.

But new Internet of Things applications have stricter latency requirements and usually need a response right away. This is something that was not a need before. Waiting for the move to the cloud is no longer a good or helpful option, since there are still problems with both moving services to the cloud and delivering them. Also, it might be hard to keep customers' information private and stop people from getting to it without permission. Internet of Things programmes that run in the cloud usually break users' privacy expectations when storing and retrieving sensitive information. This is done to provide a better level of service. Unfortunately, putting in place privacy protections can have unintended side effects, such as using too much bandwidth and power. With all of these problems, it shouldn't be a surprise that the traditional ways of managing IoT in the cloud are not enough. Because of this, it is very important to develop a new way of thinking about computers that can bring people together.

In order to solve these problems and get around the limitations of cloud computing, a new strategy called "fog computing" has been created. "Fog computing" is a new way for computers to work that was first suggested by Cisco. If it achieves its main goal, which is to allow processing right at the edge of the network, it will be able to host and support a wide range of Internet of Things applications. In this situation, a fog node will definitely be connected to a nearby router or a privately owned and run data centre. People usually think of it as an extension of the cloud at the edge of the network. Its main job is to "offload" work from the cloud. Fog nodes have the processing power, storage space, and networking services that are usually associated with the cloud. This makes it possible for them to serve a wide range of Internet of Things use cases (IoT). This means that these applications can be used in

more places than just the cloud and low-resource Internet of Things devices. With the combination of cloud computing and fog computing, users can now always get to the services they use. An ecosystem for the Internet of Things that uses a basic multi-tier fog set up. As the number of Internet of Things (IoT) sensor applications has grown, so has the amount of data. This has made it necessary to come up with more complicated ways to analyse the data. But the protocol limits set by the different IoT infrastructures and the IoT Sensor device layer make it hard to build intelligent Internet of Things (IoT) Sensor Applications. Because of these limits, the Internet of Things sensor systems that were already in place couldn't support other Internet of Things sensor applications.

The goal of this research was to build a model of fog big data analytics based on an attack pattern, analyse the data produced by IoT sensors for big data analytics, and bring attention to the problems that exist in the process of making intelligent solutions right now.

For Internet of Things sensor applications, it was necessary to use computation intelligence to sort and analyse a huge amount of data in a fog computing environment. To improve the results of our proposed method for analysing large amounts of data, we use it to analyse data from smart cities and make the most important fog applications.

Related Work

Z. Yu,, et al.[1] The widespread use of edge computing in Internet of Things (IoT) systems has elevated the importance of multi-service access control to a level that warrants immediate attention. This is a concern since the edge computing solutions that are available now do not meet the requirements of many services, which cannot afford to have any lag time. The findings of this research propose an access control mechanism for edge computing devices in IoT networks that is based on deep reinforcement learning. This gives a solution to the problem that has been identified. Within the scope of this initiative is the development of an innovative edge computing network architecture. The proposed method is developed to facilitate the delivery of granular services, in addition to enabling the adaptive distribution of resources that it makes possible. To achieve this objective, it makes considerable use of a technique known as deep reinforcement learning. The results of the tests reveal that the proposed strategy is both feasible and logical, displaying enhanced resource utilisation in scenarios where availability of those resources is limited.

M. Roopak, et al[2] As part of this research, we offer deep learning models as a way to make Internet of Things (IoT) systems more secure online. The Internet of Things (IoT) network is

an exciting new way to connect devices, both living and nonliving, all over the world. You can put these things anywhere on Earth. Even though the Internet of Things (IoT) is growing quickly, it does not have a strong enough cyber security system. This makes it vulnerable to many online threats. Users might be hesitant to use this technology if they are worried about the security of their data. Recent attacks called DDoS (distributed denial of service) have cost millions of dollars and caused a lot of damage to a number of Internet of Things networks.

Dejan Dašić et al[3] After that, the study will talk about the architectures that are used in mobile networks for deep learning. The next part of the article talks about how deep learning is used in applications and services for the next generation of mobile networks. At the end of the study, a real-world example of modulation categorization using deep learning in a key modern spectrum management application is given. As a final step, we've made a list of some interesting new areas to look into for follow-up studies.

Shaifali P et al.[4] With fog computing, processing, storage, and networking are moved closer to the users. This makes services better for the end users. In the past few years, a lot of research has been done on different architectural and algorithmic parts of fog computing. The existing literature gives a thorough look at architectural plans and how they can be used in different fields. Almost never is an algorithm looked at. In fog computing, algorithms are a very important part. The goal of this survey is to compare and contrast the algorithmic solutions that are already out there. In addition to pointing out the most important problems and promising areas for future research, this report gives a full taxonomy of the algorithms that are currently used for fog computing.

Gupta et al [5] The recent rapid progress of deep learning is mostly due to the two things we'll talk about here. (1) Training problems become much less of a problem when a lot of labelled data is used. When talking about deep learning, the word "engine" is often used in a loose way. For example, the Imagenet database has millions of examples of annotated data. (2) High-performance GPUs with thousands of cores are just one example of how fast progress in computer hardware is making it possible to train large-scale neural networks with a lot of computing power. Because of this progress, it is now possible to make AI systems that can learn new skills.

M. Kumari et al.[6] There are some security features in the cloud, like identity, authentication, and password policies, but they aren't enough to meet our requirements for security terms and conditions, and the cloud is also slower at processing real-time data. We

needed to make a new technology that we call "Fog Computing" because we have to deal with high decryption technologies or hacking issues as part of our data security. When it comes to security and safety, fog processing is the main focus of this cutting-edge technology. In passing, it's important to note that "Cloud" and "Fog" computing mean the same thing. However, "Fog" will remain the more common term because it emphasises the increased capabilities of "cloud" computing.

Proposed Methodology

The coefficient correlation notion that was presented for the IDS model is employed in this section of the article, and its findings are compared to those of the algorithms that are used for Fusion Deep Learning Model Classification. Therefore, the purpose of this section is to assess and demonstrate the many performance characteristics, such as runtime complexity, precision, error rate, resource utilisation, and so on. We propose an approach that, with the assistance of machine learning, can both improve the performance of the RBF kernel and boost the throughput of the Fusion Deep Learning Model Based on Fog Computing for Big Data Classification in Secure IoT Environment. This method can be found. The field of machine learning encompasses a wide variety of subfields, some of which include analysing, learning, and categorising. Because of this brilliant innovation, it is now possible to look at both labelled and unlabeled data sets at the same time. The unlabeled web structure data is derived from the web traffic data, whereas the labelled dark web data is derived from the unlabeled dark web structure data. Both sets of data are unlabeled. The processing of data that has been labelled can be done in a variety of ways, but there is no software that can explore and accurately analyse data that has not been structured. There are many different ways to process data that has been labelled. The end result of this work should be a system that is not just dependable but also spot-on accurate. This system will be utilised to perform analysis and classification on data that is not labelled (mixed data sets). In order to determine which of these various approaches has the most potential to be utilised in this kind of procedure, a comparison of the various ways things can be done is carried out. We put our suggested neural network Fusion Deep Learning Model through its paces in the real world using Fusion Deep Learning Model to evaluate how well it functions. These evaluations assist us in determining whether or not the model is successful. The efficiency of the conventional approach to classification has seen a significant boost as a direct result of the model that we have proposed for the classifier. A binary neural network classifier and an extended back propagation neural network are combined into a single, very efficient machine

learning tool thanks to the implementation of the strategy that has been provided (BPNN). The use of labelled data in conjunction with binary classification allows for significant progress to be made because it can be used to determine the likelihood that each individual item of data will be assigned to a particular categorization class. Because of this, it will be much easier to make significant headway. Following the completion of this stage, the computed probabilities are transformed into weights, which are then applied to both the completion of the classes and the training of the neural network. During the process of classification, testing data is looked at once again to locate a pattern that is similar, and the weights for the labels that are considered to be the most essential in the dataset are adjusted to reflect this. We describe a more straightforward approach that we term the Fusion Deep Learning Model. When this methodology is applied, it produces outcomes that, as a consequence of empirical investigation, have been demonstrated to be accurate. Our method of organising data into groups is superior to other similar methods, such as distributed or parallel research in two crucial respects. In order to construct a classifier function, we make use of deep learning backpropagation neural network classification in conjunction with Fusion Deep Learning Model which is an innovative method for training neural networks. Second, by utilising a wider variety of feature engineering techniques, the accuracy of the system can be improved to be even greater than it already is.

According to the findings of our study, using our method led to a significant increase in the precision of large amounts of data as well as a reduction in the difficulty of the categorization issue that is posed by online applications. Both of these components are becoming more significance as the usage of big data becomes more widespread. S3 virtual machine for information suggestion based on user interest, using a minimum categorised web structure data in a raw data set, applying training and testing to generate a large training sample and a small testing sample by applying training and testing to generate a large training sample and a small testing sample by applying training and testing to generate a large training sample and a small testing sample.

According to the model that we present, the manner in which unlabeled large-scale events are transformed into labelled ones is contingent upon the fusion level . The primary objective of fusion-based future selection algorithms is to attain the best feasible level of accuracy while simultaneously maximising their rate of execution. We have improved the usefulness of the map-reduced model by simulating it on a data set taken from the real world, and we have demonstrated that this can be accomplished successfully.

Results Analysis

Parameters of Evaluation Used to Measure Performance. To assess the efficacy of the various algorithm, we used True Positive Rate (TPR), False Positive Rate (FPR), Precision, and Precision. ,e following definitions are TPR, FPR, Accuracy, and Consistency. represents how accurate the results are, and the equation can be used to figure out the margin of error (12). True positives are samples that have been successfully recognised, and the phrase "True Positive" is used to characterise these samples. The True Negative, which is written as TN, is the total number of false-positive detections. The letter FP also stands for the number of flawed samples that were mistakenly labelled as correct (False Positive). Last but not least, the term "False Negative" (FN) refers to valid samples that were mistakenly labelled as negative. which is explained in more detail below, is easier to understand if you look at an example. Let's say it only takes 10 random checks to figure out whether or not a bank transaction involves fraud.

Let's say, for the sake of argument, that a sample that raises red flags is obtained. When the SVM , Random forest , Regression , BPNN, FDL algorithm is used to classify such a sample, it wrongly identifies it as a nonsuspicious one. But a smart neural network has found that this sample may have been made with bad intentions. Because of this, the SVM , Random forest , Regression , BPNN, FDL, while a deep neural network makes a TP.

Even if the tasks are done backwards, a normal transaction will still result in TN and FP. Answers that start with TP and FN are right, but answers that start with FP and TN are wrong.

$$\text{Accuracy} = \frac{TN + TP}{TP + TN + FN + FP},$$

$$\text{Precision} = \frac{TP}{TP + FP},$$

$$\text{Recall} = \frac{TP}{TP + FN},$$

$$\text{F1Score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}.$$

Table: Fusion Level Deep Leaning (Multilayer Perceptron) Perceptron

Model	Precision	Recall	F-Measure	RSME
SVM	0.890	0.865	0.977	0.0356
Random Forest	0.932	0.786	0.977	0.0876
Regression	0.932	0.834	0.977	0.0656
BPNN	0.945	0.823	0.977	0.5457
FDL	**0.965**	**0.899**	**0.977**	**0.0234**

Conclusion

Internet of Things devices can be attacked in many different ways because they don't have enough resources and have security holes in their hardware and software. This study looks into how an Internet of Things system that uses fog technology could affect the privacy and safety of its users. The main goal of this type of research is to figure out how to best protect the huge amounts of data that are created by applications that use fog computing.

First, we talked about the many applications of the Internet of Things that create a lot of data. Next, we talked about the structure of fog computing, the security needs of IoT apps that use fog, and the security problems that fog computing brings with it.

We looked at many different modern approaches to security and privacy in order to learn more about these problems and the limits they put on us.

We also looked into the many blockchain solutions that are already being used in IoT systems. This was in addition to looking into the possible benefits of blockchain technology as a new security solution for addressing security concerns in the fog-enabled IoT industry..

Reference

[1]. Z. Yu, W. Chen, J. Wang and K. Ye, "Deep Reinforcement Learning Based Access Control Strategy for Edge Computing in IoT System," 2021 IEEE International Conference on Computer Science, Electronic Information Engineering and Intelligent

Control Technology (CEI), 2021, pp. 699-702, doi: 10.1109/CEI52496.2021.9574449.

[2]. M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452-0457, doi: 10.1109/CCWC.2019.8666588.

[3]. Dejan Dašić,Miljan Vučetić, Nemanja Ilić, Miloš Stanković, Marko Beko. Application of Deep Learning Algorithms and Architectures in the New Generation of Mobile Networks. SERBIAN JOURNAL OF ELECTRICAL ENGINEERING Vol. 18, No. 3, October 2021, 397-426 UDC: 004.7:004.8 DOI: https://doi.org/10.2298/SJEE2103397D

[4]. Shaifali P. Malukani1 , C. K. Bhensdadia. Fog Computing Algorithms: A Survey and Research Opportunities. ISSN 2255-8691 (online) ISSN 2255-8683 (print) December 2021, vol. 26, no. 2, pp. 139–149 https://doi.org/10.2478/acss-2021-0017 https://content.sciendo.com

[5]. Gupta, B.B., Agrawal, D.P. & Yamaguchi, S. Deep learning models for human centered computing in fog and mobile edge networks. J Ambient Intell Human Comput 10, 2907–2911 (2019). https://doi.org/10.1007/s12652-018-0919-8

[6]. M. Kumari and A. Kumar, "A Secure Fog Computing Architecture for IoT Based Smart Manufacturing System," 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM), 2021, pp. 1-5, doi: 10.1109/SASM51857.2021.9841119.

[7]. A. Tasnim, N. Hossain, N. Parvin, S. Tabassum, R. Rahman and M. Iqbal Hossain, "Experimental Analysis of Classification for Different Internet of Things (IoT) Network Attacks Using Machine Learning and Deep learning," 2022 International Conference on Decision Aid Sciences and Applications (DASA), 2022, pp. 406-410, doi: 10.1109/DASA54658.2022.9765108.

[8]. H. S. K. Sheth, I. A. K and A. K. Tyagi, "Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures," 2022 International Conference on

Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 476-485, doi: 10.1109/ICAAIC53929.2022.9793179.

[9]. A. Nascita, F. Cerasuolo, D. D. Monda, J. T. A. Garcia, A. Montieri and A. Pescapè, "Machine and Deep Learning Approaches for IoT Attack Classification," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2022, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9797971.

[10]. M. Abdel-Basset, H. Hawash, R. K. Chakrabortty and M. J. Ryan, "Semi-Supervised Spatiotemporal Deep Learning for Intrusions Detection in IoT Networks," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12251-12265, 1 Aug.1, 2021, doi: 10.1109/JIOT.2021.3060878.

[11]. S. Patidar and I. S. Bains, "Web Security in IoT Networks using Deep Learning Model," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 848-855, doi: 10.1109/ICSSIT48917.2020.9214114.

[12]. F. Jeelani, D. S. Rai, A. Maithani and S. Gupta, "The Detection of IoT Botnet using Machine Learning on IoT-23 Dataset," 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2022, pp. 634-639, doi: 10.1109/ICIPTM54933.2022.9754187.

[13]. R. G. Babu, A. Nedumaran and A. Sisay, "Machine Learning in IoT Security Performance Analysis of Outage Probability of link selection for Cognitive Networks," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 15-19, doi: 10.1109/I-SMAC47947.2019.9032669.

[14]. T. -Y. Ho, W. -A. Chen and C. -Y. Huang, "The Burden of Artificial Intelligence on Internal Security Detection," 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), 2020, pp. 148-150, doi: 10.1109/HONET50430.2020.9322823.

[15]. H. Qiu, Q. Zheng, T. Zhang, M. Qiu, G. Memmi and J. Lu, "Toward Secure and Efficient Deep Learning Inference in Dependable IoT Systems," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3180-3188, 1 March1, 2021, doi: 10.1109/JIOT.2020.3004498.

[16]. M. R. Nosouhi, K. Sood, M. Grobler and R. Doss, "Towards Spoofing Resistant Next Generation IoT Networks," in IEEE Transactions on Information

Forensics and Security, vol. 17, pp. 1669-1683, 2022, doi: 10.1109/TIFS.2022.3170276.

[17]. S. Abdelhamid, M. Aref, I. Hegazy and M. Roushdy, "A Survey on Learning-Based Intrusion Detection Systems for IoT Networks," 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), 2021, pp. 278-288, doi: 10.1109/ICICIS52592.2021.9694226.

[18]. T. Hasan, A. Adnan, T. Giannetsos and J. Malik, "Orchestrating SDN Control Plane towards Enhanced IoT Security," 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, pp. 457-464, doi: 10.1109/NetSoft48620.2020.9165424.

[19]. [Z. Lv, L. Qiao, J. Li and H. Song, "Deep-Learning-Enabled Security Issues in the Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9531-9538, 15 June15, 2021, doi: 10.1109/JIOT.2020.3007130.

[20]. B. Xue, H. Zhao and W. Yao, "Deep Transfer Learning for IoT Intrusion Detection," 2022 3rd International Conference on Computing, Networks and Internet of Things (CNIOT), 2022, pp. 88-94, doi: 10.1109/CNIOT55862.2022.00023.

[21]. A. Gutal, T. Bhamare, A. Mayekar and P. Deshmukh, "Automation of Society Security Using Deep Learning and IoT," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 96-102, doi: 10.1109/I-SMAC52330.2021.9640917.

[22]. S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3930-3944, 1 March1, 2022, doi: 10.1109/JIOT.2021.3100755.

[23]. A. Xu et al., "FDI Attack Detection Scheme based on Nonlinear Prediction and Deep Learning," 2021 International Conference on Intelligent Computing, Automation and Applications (ICAA), 2021, pp. 86-91, doi: 10.1109/ICAA53760.2021.00024.