Anomaly Detection in IoT Devices using Federated Learning

*

Jithin T Chandran
UG student, Dept. of CSE
NSS College of Engineering
Palakkad, India
jithintchandran123@gmail.com

Pranoy P Sundar
UG student, Dept. of CSE
NSS College of Engineering
Palakkad, India
pranoyabc@gmail.com

Sidheeque Fasal C P A
UG student, Dept. of CSE
NSS College of Engineering
Palakkad, India
fasalcpa321@gmail.com

Jaseem C K
UG student, Dept. of CSE
NSS College of Engineering
Palakkad, India
jaseemckclt@gmail.com

***Abstract*—Cyberattacks in the Internet of Things(IoT) platform is a rising concern in the domain of IoT. IoT devices are increasingly used in smart homes, autonomous vehicles and smart appliances these days. Confidential data's are involved in these applications. Hence the threats and attacks can have serious consequences. Federated learning (FL) is a family of Machine Learning algorithms introduced by Google in 2016. In a network that consists of edge nodes connected to the central server, each of the nodes trains a local model and only that model is shared with the server, not the data. This is the core idea of federated learning. Hence privacy is preserved. The concept of federated learning can ultimately transform the ideology of privacy in the internet. This paper revolves around the role of Federated Learning in the security of IoT platforms and the added advantages of using the same in modeling the anomaly detection system.**

***Index Terms*—Internet of Things(IoT), Machine Learning(ML), Federated Learning, Anomaly Detection, Edge devices**

I. Introduction

The Internet of things(IoT) is a system of interconnected and related devices capable of transferring data over a network. Recent years had witnessed a sudden uprise of IoT device consumption around the world. People are increasingly preferring IoT devices and smart appliances. Apart from that IoT infrastructures are widely used in the health sector, automobile industry, and industrial automation. According to IHS Markit, it is estimated that by 2030, there will be more than 125 billion IoT devices worldwide. Cybersecurity, in general, is a challenge that experts have been dealing with for decades. But security in IoT platforms only recently came into the mainframe of cybersecurity. The rush-to-market mentality of manufacturers had made security a secondary issue. Many IoT devices used today are dealing with confidential data and private materials. So it is bound to have a strong security. Any vulnerability or loophole in the security can be of tremendous consequence.

Anomaly detection is a method used to tackle this issue of security in general. It detects the pattern or up normal behavior in the network traffic. This eventually can help the system to detect some of the attacks. Some attacks can also be identified by training a model with some labeled datasets. Traditional Machine Learning(ML) algorithms such as Logistic Regression(LR), Support Vector Machine(SVM), Decision Tree(DT), Random Forest(RF) can be used to implement this model [1].

Many of todays IoT devices take advantage of cloud computing. But some are starting to discover the benefits of doing more compute and analytics on the devices themselves. This ability to do on-device computation is known as 'edge computing'. More and more IoT devices are turning to the edge platform each year. This method of computation can help reduce latency for critical applications and manage the huge amount of confidential data generated. Security and privacy of the data can also be improved with edge computing by keeping sensitive data within the device itself. Standard machine learning approaches requires centralize the training data on one machine or in a datacenter [2]. That is the data has to be sent to a centralized cloud for training. This gives a perception of 'One of the either' - Machine learning or Privacy to the users. Federated learning is a Machine learning algorithm introduced by Google in 2016. This is capable of training the model locally at the edge. This can eventually secure the IoT platform from cyberattacks.

This paper is organized as follows. Section II presents the background. Section III investigates the previous attempts and works done in this field. Section IV introduces Federated Learning and it's application in the security of IoT platform. Section V provides details of our model and show the experimental results. Section VI discusses the potential future directions in this domain. Section VII concludes the paper with the summary and remarks.

II. Background

Internet of Things is one of the most popular and widely expanding platforms of the current era. This shift in trend has created a lot of changes in our day-to-day routines. IoT devices play a major role in the automation field. Everything from our home to the car is automated. This is a major breakthrough by

the modern-day technology. But along with this comes many issues and concerns.

IoT devices are increasingly deployed in daily life. But as a matter of fact, many of these already deployed devices are vulnerable due to insecure design, configuration, and implementation. And hence, there exists many networks that already have vulnerable IoT devices that are easy to compromise. IoT devices use wireless mediums to broadcast data which makes them an easier target for an attack. Normal communication attack in the local network is limited small local domain and does not have a serious effect, but attack in IoT system expands over a larger area and has devastating effects. This was not considered a major issue some years before. But as the platform becomes increasingly used in very critical areas, it emerges as a primary concern. Many connected devices and sensors are prone to compromise in their findings. The observations can vary a lot at times that makes the analysis go completely wrong at the final step. These kinds of readings and data are anomalous. This can happen due to many reasons. Anomalies are more tend to occur in an IoT platform. Since it involves hardware, even a small setup mistake can generate misguiding data. So it is really important to detect and resolve anomalies in the platform.

Anomaly detection is a widely studied problem with a broad range of applications and a diverse set of approaches including machine learning and statistical approaches. It is the technique of identifying rare events or observations which can raise suspicions by being statistically different from the rest of the observations. Applications include network intrusion detection, fraud detection and identification of business trends in e-commerce. Anomaly detection systems are used in many platforms and fields. Anomalies are broadly classified as follows:

- Point anomalies: A single instance of data is anomalous if it's too far off from the rest
- Contextual anomalies: The abnormality is context-specific. It is seen mostly in time-series data.
- Collective anomalies: A set of data instances collectively helps in detecting anomalies.

Point anomalies concentrate only on certain instances without considering anything else. While contextual anomalies considers the context of its occurrence. The collective anomalies category is where the use-case of attack detection comes in [3].

There are many anomaly detection techniques. Simple and naive statistical methods can be used to achieve this task. But the frequent change in the definition of normal and abnormal, changing trends and noise makes this a non-reliable method as it is not capable of adapting to these scenarios. The most efficient method to detect anomalies is using the concept of machine learning. It can be divided into two:

- Supervised Anomaly Detection: In this method, the labeled dataset that contains both kinds of data, namely normal and anomalous are used to construct a predictive model to classify future data points.
- Unsupervised Anomaly Detection: In this method label are not used, instead, it assumes that only a small percentage of data is anomalous and any anomaly is statistically different from the normal samples.

Based on the above assumptions, the data is then clustered using a similarity measure and the data points which are far off from the cluster are considered to be anomalies [3].

one of the most important and featured use case that anomaly detection has is in networking. The internet is a host to various websites that are located all around the world. Unfortunately, due to the ease of access to the Internet, various individuals can access the Internet with bad intentions. With sensitive information as well as the high volumes of expected attacks every day, automation is a necessary tool to help cybersecurity professionals deal with the attacks and preserve privacy.

Generally, anomaly detection is utilized heavily in fields like medicine, finance, cybersecurity, banking, networking, transportation, and manufacturing. But it is not just limited to those fields. For nearly every case involving data collection, anomaly detection can be put to use to help users automate the process of detecting anomalies. Many fields in science can utilize anomaly detection because of the large volume of raw data collection which goes on. Anomalies that would possibly interfere with the interpretation of results or otherwise introduce some sort of bias into the data could be detected and removed efficiently, provided that the anomalies are caused by systematic or random errors.

Privacy in the IoT platform is hence a serious issue that has to be resolved. Anomaly detection systems are very important in the IoT systems as anomalies in the platform can cause devastating consequences. Various techniques and algorithms are used to enable these systems to adapt to the IoT environment securely.

III. Anomaly Detection in IoT

Many attempts and works were done in the field of anomaly detection in general and specific to the IoT platform. Most of them use deep learning techniques to achieve this task. Some works show great results using basic machine algorithms. There are also some works that use novel methods to reach the same result.

Pajouh et al [4] introduced a model for intrusion detection based on two-layer dimension reduction and two-tier classification module which was designed to detect malicious activities or attacks such as User to Root (U2R) and Remote to Local (R2L) which are seen commonly. The proposed model is using component analysis and linear discriminant analysis of the dimension reduction module to spare the high dimensional dataset to a lower one with lesser features.

Cybersecurity is a serious issue for any sector in the cyberspace as the number of security breaches is increasing from time to time. It is said that thousands of zero-day attacks are continuously emerging because of the addition of various protocols mostly from the Internet of Things(IoT). Most of these attacks are small variants of some previously

Model	Accuracy	Precision	Recall	F1 Score
Logistic Regression	0.983	0.98	0.98	0.98
Support Vector Machine	0.982	0.98	0.98	0.98
Decision Tree	0.994	0.99	0.99	0.99
Random Forest	0.994	0.99	0.99	0.99
Artificial Neural Network	0.994	0.99	0.99	0.99

Table I. Results from Experiment [1]

known cyberattacks. The use of Deep Learning(DL) for attack detection in cyberspace could be a flexible and strong mechanism to small mutations or novel attacks because of the high-level feature extraction capability. The self-taught and compression capabilities of deep learning architectures are key mechanisms for hidden pattern discovery from the training data so that attacks are discriminated against from benign traffic [5]. The main benefit of deep learning is the absence of manual feature engineering, unsupervised pre-training and compression capabilities which enable the application of deep learning feasible even in resource constraint networks. Many works were done using deep learning methods.

Olivier Brun et al [6] use Dense Random Neural Network(RNN) for detecting attacks against IoT connected home environments. This methodology based on a deep-learning can predict the probability that a network attack is ongoing from a set of metrics extracted from packet captures. It is also observed that the results obtained in this manner are comparable to those obtained with a simple threshold detector.

Anthi et al [7] Introduces a novel predictive and adaptive IDS system tailored for IoT ecosystems. The proposed model is a real-time network-based, both signature, and anomaly-based detection system. The model is better at detecting probing attacks than it is for flood-type attacks.

Mahmudul Hasan et al [1] use various machine learning models to detect attacks in the IoT sites. The paper discusses and compares the models used to train the labeled dataset. IoT devices use a wireless medium to broadcast data which makes them an easier target for an attack. It uses naive ML model and Artificial Neural Networks to classify the threats which proves to be of high accuracy. The performance of several models were tested using IoT dataset in kaggle [8] and listed in Table I. The paper also mentions the enhanced risk of anomalies in IoT from other platforms. Thenceforth, a secured IoT infrastructure is really necessary for the protection from cybercrimes.

Joseph Schneible [9] proposes a method to implement anomaly detection on the edge. This is specific to edge devices. The approach uses autoencoders, a specialized deep learning neural network, on each edge device to identify anomalies and adjust the model by learning from new observations. This allows the system to go beyond simple threshold measurements and identify instances of anomalous behavior between correlated variables. He also experimented with Federated Learning to prove the effectiveness of merging models via averaging their weights using the KDDCUP 1999 dataset [10].

Thein Duc et al [11] introduces an autonomous self-learning distributed system for detecting compromised IoT devices. It was built effectively on device-type-specific communication profiles without any human intervention nor of any labeled data that are subsequently used to detect anomalous deviations in devices communication behavior.. It utilizes a federated learning approach for aggregating behavior profiles efficiently. Since different IoT devices can have very heterogeneous behaviors, a dedicated model is assigned to each device type. In this paper, anomaly detection models are learned using a federated learning(FL) approach in which security gateways locally collect the data from there to train local models which IoT Security service aggregates into a global model. It is a novel way and is getting popular in the IOT world.

IV. Advantages of Federated Learning

Federated learning [2] is a machine learning technique where the connected devices collect data participates in training the central machine learning model. This technique is most popular with systems deployed at scale. Federated learning is used where the data should not be shared with the cloud but requires information and analysis from the data at hand. This method is used where confidential data are involved and is ideal for edge devices. Personalized keyboards on smartphones are one of the areas where it is first implemented. GBoard application is one example. The predictive features on those personalized keyboards learn from features such as your typing patterns, usage of words, slangs to give you better suggestions in the future. But the keyboard is used to type many private and confidential data. So, it is not secure to send those data directly to the cloud. Then it would be privacy invasion and a lot of our personal stuff can be leaked and misused.

A. Working of Federated Learning

The basic working of federated learning is as follows. Machine learning models are trained on your edge devices and then the stuff which can be either weights in neural networks or other types of machine learning models, are the only ones sent to the central server. Now the central server averages those stuff which it receives from connected edge devices and then uses them to train its central machine learning model. After it undergoes training up to some epochs, that central machine learning model is distributed back to the devices to be used for predictive purposes or for further training.

In traditional machine learning approach, training a neural network would require to have a single copy of the model and all of the training data in one place. But in reality, data is mostly gathered across an array of sensors. In those scenarios, all sensor data would have to be sent to a central server fortraining and the resulting network weights distributed back to the sensors. However, these sensors often have limited bandwidth and intermittent connections to the central server.

B. Benefits of Federated Learning

Benefits of using Federated Learning can be enlisted under these points:

- Decentralized learning
- Secure computing

Fig. 1. Initial pre-trained model send to edge devices.

Fig. 2. Each selected device computes an updated model using its local data.

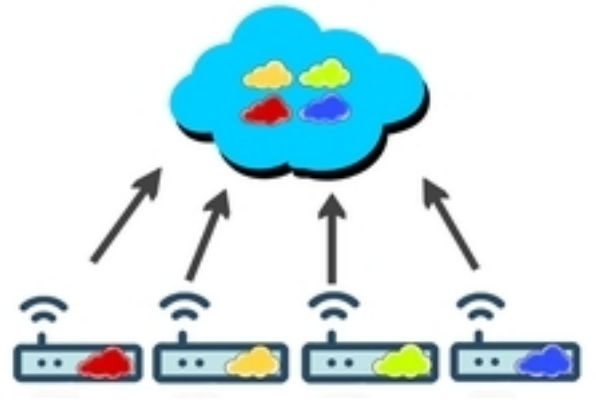

Fig. 3. Model updates are sent from the federation to the server.

Fig. 4. Server aggregates the model.

- Preserve privacy

Federated learning [12] is based on the data parallelism model. The training data is split between the copies of the network in the data parallelism model, such that each copy is trained on an independent section of data. Once all copies of the model are trained, the resulting weights are aggregated at a central repository. This is usually accomplished by averaging the weights of the independently trained models. The trained new network weights are sent to the center for aggregation, and the resulting model is then distributed or shared to the edge devices. In this way, the model in each edge device will reflect the patterns of the whole data without sending them all to the central server. This can reduce bandwidth requirements and can occur when a connection to the central server is available. Apart from the benefit of enhanced privacy, this adds to the list of benefits federated learning provides. The main advantage of introducing federated approaches to machine learning is to ensure data privacy or data secrecy. Indeed, no local data is uploaded externally, concatenated or exchanged in this method. In this way, Federated learning is ideal for anomaly detection in the IoT platform.

V. Experiment

The experiment consist of collecting and exploring a suitable dataset for anomaly and attack detection and proper preprocessing of the extracted data. A neural network is constructed to train the models in different conditions. Federated Learning method is used to train the data in a federated way which are available not in the centre, but at the edges.

A. Dataset collection and description

The open source dataset was collected from UCI database [10] provided by KDD cup 1999. This is the data set used for The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining. This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated. In the dataset, there are 48,98,431 samples and 42 features. But for the experiment, we are taking only taking 1,00,000 samples. There exists 20 distinct type of threats in the dataset. The attacks fall into 4 main categories.

- DOS: denial-of-service like syn flood.

feature name	description	type
duration	length of the connection	continuous
protocol_type	type of the protocol(tcp, udp)	discrete
service	network service on the destination	discrete
src_bytes	no. of data bytes from src to dst	continuous
dst_bytes	no. of data bytes from dst to src	continuous
flag	normal or error status of the connection	discrete
wrong_fragment	number of wrong fragments	continuous
urgent	number of urgent packets	continuous

Table II. Basic features of individual TCP connections. [10]

- R2L: unauthorized access from a remote machine, like guessing password.
- U2R: unauthorized access to local superuser (root) privileges like various "buffer overflow" attacks.
- probing: surveillance and other probing like port scanning.

The count of particular attacks are given in fig. 5. The dataset consists of higher-level features that help in distinguishing normal connections from attacks. There are also several categories of derived features. The basic features in the dataset are given in Table II.

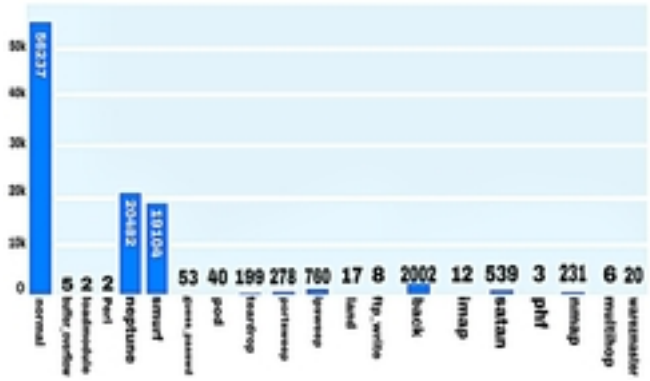

Fig. 5. Count of threats in the Dataset.

B. Data Preprocessing

Exploratory data analysis and data observation was done on the dataset. The samples taken for the experiment does not have any missing data. Steps were taken to make the dataset feed-able to any classifier. For the modeling only numerical features are taken from the dataset. Columns with constant values are also removed as it won't do any good to the model. The number of features reduced to 33 from 42 columns. The target data is also categorical. To convert this feature into integer, label encoding method is used. All the values are scaled for each column from 0 to 1. The data is split into two for each IoT gateways. The first half of the data is given to one gateway and the other half to the second gateway.

C. Experimental Setup

The experiment was done entirely using the Google Colab environment. For data analogy, cleaning and feature engineering, Pandas framework and Numpy framework; for data visualization, Matplotlib framework and Seaborn framework and for data analysis, scikit-learn framework and PyTorch framework were used. For Federated Learning experiments, PySyft library by OpenMined was used.

Model	Train Set	Test Set	True Positive	Accuracy
Edge 1	3000	2000	11235/2000	56%
Edge 2	3000	2000	15347/2000	77%
Full Dataset	6000	4000	38310/4000	96%
FL Model	6000	4000	38304/4000	96%

Table III. Result Analysis of the Experiment.

D. Implementation

Gateways are initialized with splitted dataset. The dataset is again divided into training and testing data. 40% of the data is taken for testing. A neural network is constructed with 3 layers. The input layer is of 33 neurons. There are 2 hidden layers each of 8 neurons and the output layer consist of 20 neurons, each representing an attack or normality. The learning rate used is 0.01 and 20 epochs are taken for training each of the models. The optimizer used in the model is SGD(Stochastic gradient descent). All the data are trained using this architecture. The edges are trained seperately to generate models and the performance is noted. The full dataset is trained using the same architecture and the accuracy of the model is observed. The federated learning model using the gateways are also evaluated and compared to the other models.

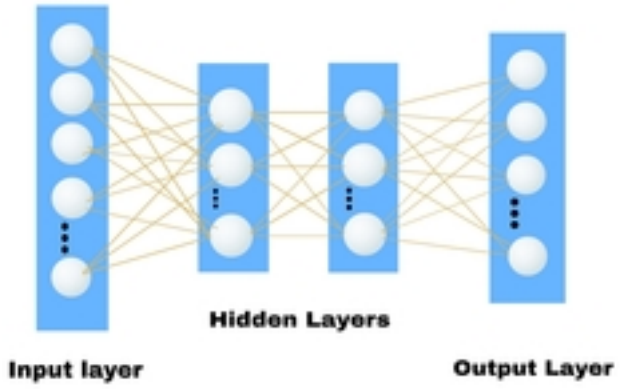

Fig. 6. Architecture of the Neural Network.

E. Result Analysis

A model was trained seperately at the edges with the data they have, another model trained with all the data centered at one place, preferably at the cloud and one model trained using the Federated Learning Technique. The performance of the model was evaluated in each case and compared to deduce inference. The comparison is given in Table III.

The model performs better with more training data given, which was expected. The merged model and the federated model have similar accuracies, which proves that the federated model does not compromise accuracy or performance for the enhanced security. By using this method, the load on central

server can be reduced to a reasonable rate as the training data doesnt requires to be at the server. As the federated learning gives back the global model to the edges, the better performance of classification reflects in all the edge devices alike. This secures the data of the edge devices as they are only sending the weights of their local model and not the data itself.

VI. Future Direction

Federated learning is one of the novel methods used in edge devices. It was introduced only by the end of the year 2016. It is still in its early stages. But the innovation it brings in is huge and as a result, it is starting to get implemented in many areas where privacy is a concern. Some of the challenges that this method faces are inference attack and model poisoning. There are some works that attempt to tackle these issues. These issues should be resolved in order to ensure the security of the data.

This accuracy of the model depends on the dataset to some extend. But it can be enhanced using more complicated and apt algorithms. More challenges and issues are prone to occur as the technique is used in various environments. Future research steps should be taken to adapt to all those platforms.

VII. Conclusion

This paper discusses the benefits and advantages of using federated learning to detect anomalies in the IoT platform. Various methods are used for anomaly detection in general. Many techniques are specifically implemented in order to detect anomalies in the IoT platform too. We also explored some of the previous attempts and works done in this field.

Federated learning is a novel method used for this application. From the experiments, it can be inferred that federated learning performs well inspite of not seeing the entire data. There are many challenges and limitation that the method faces currently. This is an active research area. To conclude, federated learning is a method that enhances the security and privacy of data, which is very critical in the IoT platforms.

References

[1] M. Hasan, Md. M. Islam and Md. I.I. Zarif et al, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things 7, 2019.

[2] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson and Blaise Agera y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," Google, 2016.

[3] Pramit Choudhary, "Introduction to Anomaly Detection", 15 February 2017. [Online]. Available: https://blogs.oracle.com/datascience/introduction-to-anomaly-detection [Accessed 24 February 2020]

[4] Hamed Haddad Pajouh, Reza Javidan, Raouf Khaymi, Ali Dehghantanha and Kim-Kwang Raymond Choo, "A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," Transactions on Emerging Topics in Computing, 2016.

[5] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Generation Computer Systems, 2017.

[6] Olivier Brun, Yonghua Yin and Erol Gelenbe, "Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments," Procedia Computer Science 134, 2018, 458463.

[7] Eirini Anthi, Lowri Williams and Pete Burnap, "Pulse: An Adaptive Intrusion Detection for the Internet of Things," School ofComputer Science and Informatics, Cardiff University, 2017.

[8] M.-O. Pahl, F.-X. Aubet, DS2OS traffic traces, 2018, (https://www.kaggle.com/francoisxa/ds2ostraffictraces). [Online; accessed 8-June-2020].

[9] Joseph Schneible and Alex Lu, "Anomaly Detection on the Edge," Cyber Security and Trusted Computing, 2017.

[10] KDD CUP 1999 data [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed 24 February 2020]

[11] Thien Duc Nguyen,Samuel Marchal,Markus Miettinen and Hossein Fereidooni, "A Federated Self learning Anomaly Detection System for IoT," 39th IEEE International Conference on Distributed Computing Systems(ICDCS), 2019.

[12] Ying Zhao, Junjun Chen, Di Wu, Jian Teng and Shui Yu, "Multi-Task Network Anomaly Detection using Federated Learning," SoICT: Proceedings of the Tenth International Symposium on Information and Communication Technology, December 2019, Pages 273-279.

[13] Davy Preuveneers, Vera Rimmer 1, Ilias Tsingenopoulos, Jan Spooren, Wouter Joosen and Elisabeth Ilie-Zudor, "Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study," Applied Sciences, 2018.

[14] Tuhin Sharma and Bargava Subramanian, "Anomaly Detection in Smart Buildings using Federated Learning", Oreilly AI London 2019, 17 Oct 2019.