ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

Federated Learning: An Intrusion Detection Privacy-Preserving Approach to Decentralized AI Model Training for IOT Security

Mohit Mittal

Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India

ABSTRACT: There are various aspects to Internet of Things security, such as guaranteeing the safety of both the devices and the Internet of Things networks to which they connect. Many other types of equipment, including industrial robots, smart grids, construction automation systems, entertainment gadgets, and many more, are included in this, despite the fact that they were not designed with network security in mind. When it comes to securing systems, networks, and data, IoT device security must be able to resist a wide range of IoT security assaults. One of the most important issues in the field of data security is the creation of intrusion detection systems (IDSs) for the Internet of Things. Client devices (edge devices) in Federated Learning utilize local data to train the machine learning model, and then send the updated model parameters to a cloud server so that they may be aggregated (rather than raw data).This paper proposes a machine learning system that employs federated learning to detect intrusions in the IoT. The FedAVG algorithm is employed to aggregate models. Models are trained locally by nodes. The models are trained and validated using machine learning methods, including Random Forest, ID3, and Support Vector Machine. The NSL KDD data set is employed to undertake experiments.

KEYWORDS: Federated Learning, Model Aggregation, TensorFlow, Machine Learning, Intrusion Detection, Internet of Things, Accuracy, FedAVG

I. INTRODUCTION

A centralized server is essential for Federated Learning (FL) to consolidate parameters. Central server malfunctions may result in single points of failure (SPoFs) and distributed denial of service (DDoS) attacks. Local model changes must be explicitly documented by FL. The capacity of a distributed system to detect and avert illegal modifications is essential to its efficacy. Ensure the security of FL systems by the use of blockchain technology. Federated deep learning and blockchain are used to mitigate the duration of poisoning and assaults. This model is designed for efficiency and performance in decentralized data training.

Modifications to machine learning models may be safely and openly documented via distributed ledgers. Due to blockchain's capacity to prevent retractions, Federated Learning can more effectively identify collaborative machine learning models and enhance system trust. This work focusses on the audibility of blockchain-federated deep learning. At the conclusion of each round, the global model is synthesized from the local models of all Federated Learning participants by Federated Averaging (FedAvg). All local models get advantages from FedAvg averaging. The inadequacy of the local model in traditional FedAvg always results in the global model's failure. Dynamic weighted updating

The Internet of Things (IoT) is a network that connects a broad variety of machines, devices, and other items that are connected to the internet through the use of wireless communication technology. A portion of the home is outfitted with hardware from the Internet of Things, which is also used in said location. An attack on the Internet or any of the systems linked with it has a substantial influence on the operating environment of the internet of things (IoT). A wide range of sensor nodes and devices, each of which makes use of a different technology, may be found at each of the Internet of Things' layers. IPv4 has a finite number of accessible locations, which is why Internet of Things devices utilize IPv6 rather than the older protocol. It is conceivable for Internet of Things devices to have smart meters, sensors,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

and sensors for use in medical care. The Internet of Things (IoT) has the potential to completely change the way services are provided throughout the world [1].

IoT's rising market share is only going to continue to increase as a result of its usefulness in a multitude of industries, including education, business, transportation, and mobility. Devices that have the capability to connect to the internet can both communicate with one another and with websites. These items or goods may communicate and share information with one another as well as with other devices and systems over a variety of different channels and in a variety of different ways. The data collected by sensors may be utilized to send information not only about the sensors themselves but also about the things to which they are linked. It is also possible to transmit information on the internal status of the devices. We are now living in a world that is more linked than ever before as a direct result of the rapid advancement of digital innovation, which has led to a society that is hyper-connected [2].

There are several facets of Internet of Things security, such as ensuring the safety of the devices themselves, as well as the Internet of Things networks to which they connect. Even though they were not developed with network security in mind, many different kinds of devices, such as industrial robots, smart grids, construction automation systems, entertainment gadgets, and many more, are included in this. When it comes to protecting systems, networks, and data, the security of IoT devices has to be able to withstand a broad variety of IoT security attacks. In the realm of data security, one of the most significant tasks at hand is the development of IDSs for the Internet of Things. IPv4 and IPv6 are two of the protocols that have been implemented to strengthen the safety of computer networks. When it comes to establishing connections with other devices, the Internet of Things makes use of a wide variety of address mechanisms. Because there is insufficient capacity for IPv4 addresses in the Internet of Things, the adoption of IPv6 is required in order to keep Internet connection [3].

The Internet of Things, sometimes known as IoT, is a rapidly developing area of internet technology that has the potential to make significant changes to the way people live their lives. There are many different applications of the Internet of Things that are used, such as smart homes, smart climate, smart cities, and health monitoring, in addition to intelligent water and environmental systems. During the process of developing an application for the internet of things, there is the potential for several issues to occur. One of the problems that has to be fixed is the lack of protection for devices connected to the Internet of Things (IoT). To be more specific, an intrusion is any operation that is not authorized or was performed maliciously and is damaging to sensor nodes. As a consequence of this, an IDS is required in order to track down the traffic on the infected network. Using an intrusion detection system (IDS), which may be either software or hardware, it is able to analyze devices with user behaviors, recognize known attack signatures, and categorize dangerous network activities [4].

When it comes to the Internet of Things, there are a multitude of applications that cross the gamut from simple home interior regulators to complex transportation systems, propelled industrial facilities, and networked financial systems. Some examples of these applications are included below. As a direct consequence of this, safety is now the top priority. Although it is impossible to achieve total security, there are other safeguards that may be taken to protect a computer network. The network is particularly vulnerable given the diverse kinds of attacks that may be conducted against it. As a consequence of this, intrusion detection systems are an essential component of the security of IoT networks. The common qualities of Internet of Things devices, such as resource limits, standards, and established protocol stacks, make it challenging to create an intrusion detection system (IDS). When it comes to detecting intrusions in the past, performance, architecture, and analytic method have all been important considerations in how it has been employed [5].

The recent emergence of Federated Learning has made it possible for the deep learning model to now successfully complete training, preserve the privacy and security of data, and effectively handle the problem of data islands. It is shown in figure 1. At its inception, Federated Learning was developed with the intention of both facilitating rapid learning across a large number of participants or computer nodes and ensuring the confidentiality of the data that was being sent. When FL is used as an edge network enabling technology, machine learning and deep learning models can be trained together, and the edge network can be optimized [6]. Client devices (edge devices) use the data that is local to them in order to train the machine learning model, and then they communicate the new model parameters to a cloud server so that they may be aggregated (rather than raw data).

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

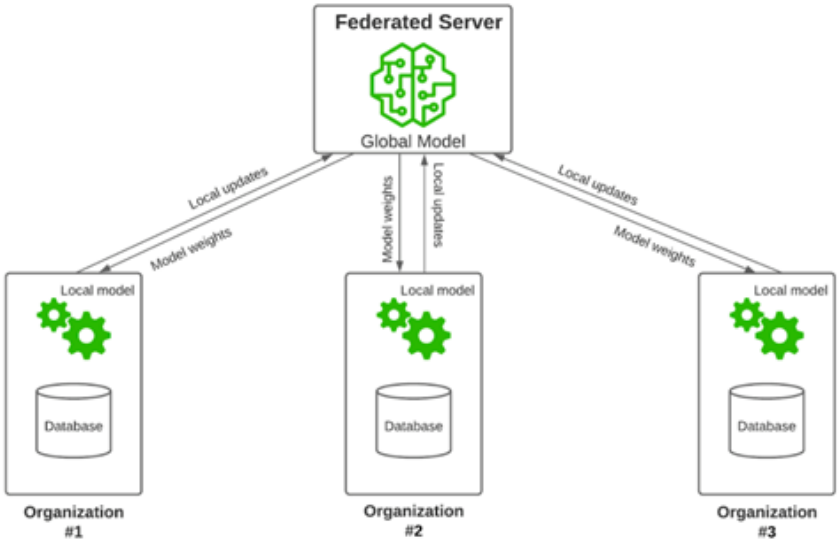

Figure 1: Federated Learning for Predictive Model

This article presents a federated learning enabled machine learning framework for intrusion classification detection in Internet of Things. FedAVG algorithm is used to perform model aggregation. Models are trained locally at nodes. Machine learning algorithms namely- Support Vector Machine, Random Forest and ID3 are used for training and testing of models.

II. LITERATURE SURVEY

According to T. Eswari et al. [7], wireless sensor networks (WSNs) has several potential uses. Wireless sensor networks (WSNs) often use unsecured radio connections and sensor nodes that are incapable of withstanding elevated temperatures, since they are deployed in uncontrolled or adverse environments. As a result, WSNs are vulnerable to assaults. To protect WSN from security concerns, many different strategies were proposed. Safeguarding wireless sensor networks (WSNs) against malicious insiders is achievable with the implementation of an Intrusion Detection System. The objective of introducing this novel intrusion detection system is to protect Wireless Sensor Networks against routing assaults. The current rule-based intrusion detection systems (IDS) in wireless sensor networks (WSNs) has inherent limitations, and this framework seeks to rectify these deficiencies.

The wireless sensor network, as articulated by Yousef El Mourabit and others [8], comprises fundamental sensing devices capable of intercommunication and the detection of variations in events or other characteristics. A unique intrusion detection system design was presented. This approach combines a classification algorithm with a multi-agent system to detect breaches in a wireless sensor network.

Research conducted by Christina Ioannou and associates [9] demonstrates that the aim of attacks on wireless sensor networks (WSNs) is to reduce or eradicate the network's capacity to fulfil its designated purpose. A unique method to intrusion detection systems using anomaly detection has been presented, termed mIDS, which use the statistical tool Binary Logistic Regression (BLR). This method will ascertain if the actions of adjacent sensors are innocuous or malicious. The suggested methodology utilizes assaults on the routing layer, and the researchers demonstrated that intrusion detection systems can identify malicious activities with an accuracy ranging from 88% to 100%. According to research by Sharad A watade et al. [10], security in MANETs is mostly dependent on the capacity to detect missing packets. They propose TWOACK, ACK, AACK, and EAACK as methods to do this. EAACK

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

demonstrates superior performance relative to other approaches. The hybrid cryptography technique was devised to minimize routing overhead by identifying potentially hazardous paths, addressing the increased routing costs associated with EAACK's use of digital signatures. Prior to data transmission, confirm that both the transmitting and receiving nodes possess the shared key.

Enhancing the real-time efficacy of intrusion detection systems in IoT contexts is complicated by the need to handle and safeguard extensive data streams from the Internet of Things. In the occurrence of a cyberattack or other malicious conduct concerning the Internet of Things, these systems must respond swiftly. Thus, the suggested IDS design inside an IoT framework provides real-time functionality.

The Internet of Things (IoT) is one of the most revolutionary technological advancements in computing history, as identified by Audrey A. Gendreau and colleagues [11]. Monitoring the information flow across these extensive, diverse networks is challenging. Security in Internet of Things (IoT) networks can only be maintained if unauthorized users are identified within the constraints established by each device type or sub-network prior to any system data sharing. This article delineates the criteria for constructing an effective intrusion detection system for the Internet of Things (IoT). According to a research by Eirini A nthi et al. [12], the exponential proliferation of networked Internet of Things (IoT) devices is giving rise to new issues in safeguarding personal information and identification. This resulted in the introduction of a novel paradigm that delineates the first phases of creating bespoke Intrusion Detection Systems for the Internet of Things. The model must be capable of detecting Denial of Service (DoS) assaults.

Brojo Kishore Mishra and associates discovered that intrusion prevention and detection represent two of the most dynamic domains within cybersecurity [13]. The ongoing advancement of novel findings, functionalities, and models is the rationale behind this. Currently, much research is being conducted to visualize intrusion detection data. Future intrusion detection systems (IDSs) will include the key insights from this work, resulting in outputs that are much more effective for assessing threat magnitudes, incident element patterns, and similar metrics. Moreover, it has been shown that intrusion detection might benefit from the use of high-speed computing methodologies. Researchers Rutba Maqsood and colleagues [14] developed an Intrusion Detection System (IDS). This system's capability to identify intrusions on virtual machines (VMs), which act as a conduit for large-scale attacks, results in reduced data loss. A network intrusion detection system (IDS) is advised to safeguard against infrastructure as a service (IaaS) threats. The Advanced Encryption Standard (AES) is used to provide data safety in cloud computing settings, which presents a significant challenge. Moreover, supplementary backup and recovery systems are included to guarantee minimum data loss. No singular security measure can sufficiently protect the extensive and diverse cloud computing landscape. As the cloud continues to expand, new threats and possibilities for malicious actors to exploit will emerge. According to the report, network intrusion detection systems (IDS) can identify assaults on virtual computers. This intrusion detection system (IDS) offers protection against IaaS-based assaults. Zhijiang Chen and colleagues presented a system capable of monitoring and detecting network threats via the use of streaming data [15]. In a cloud computing context, technologies such as Flume, Sharp, and Hadoop are used for the analysis of streaming network data. Streaming k-means and Fuzzy c-means are algorithms used to cluster a stream of normal and aberrant data to mitigate potentially harmful network traffic. This prevents external forces from usurping the system.

III. METHODOLOGY

This section presents a federated learning based methodology for intrusion classification and detection in Internet of Things. Methodology consists of machine learning algorithms- SVM, RF and ID3 algorithms. In this methodology, training of model is performed locally at individual nodes. Aggregate algorithm is used to accumulate all node level model trainings in a central cloud storage. In this way, model aggregation is performed using the FedAVG algorithm [16].

Support vector machines (SVMs), often referred to as support vector networks (SVMs), are supervised models that assess data and may be used for classification and regression analysis. These models share common evaluation methodologies. A non-probabilistic binary linear classifier is produced by the SVM training process. This classifier is

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

based on the set of training examples and assigns new instances to one of the two categories. For the purpose of illustrating SVM models, mapped example locations in space are utilized. These models divide occurrences into various categories by a distance that is as great as is practically possible. In this same space, fresh instances are mapped and projected to belong to a certain category based on which side of the gap they fall in with regard to. This mapping and projection takes place in real time. By implicitly converting their inputs to high-dimensional feature spaces, support vector machines (SVMs) have the potential to successfully conduct non-linear classification of the trick in addition to linear classification [17].

The algorithmic architecture of Random Forest is founded on the idea of bagging as its primary conceptual underpinning. In order to accomplish classification in this system, decision trees are used on a main basis. The following procedures were used in order to produce each tree in Random Forest: This kind of sample is referred to as a bootstrap sample when the number of records in the training set is N and N records are selected at random while maintaining the same number of records in the set. The growth of the tree will benefit from this sample being used as a training set for its development. If there are M input variables, then each node is divided by finding the optimum possible split based on these m attributes. In the event that there are M input variables, a number between 1 and M will be chosen. Despite the growing size of the forest, m has not changed. Every tree is provided with as many chances as possible to realize its full potential. There will be no cutting done here.

J. Ross Quinlan developed the ID-3 approach, often known as the Iterative Decision Tree-3. This was the first method to use decision trees for monitoring evolution. This strategy uses both entropy and the information gain measure. A nodule acts as the first reference for a recursive assessment of the entropy of the functional characteristics. The theories of entropy and information gain characterize split attributes as datasets separated based on the subset exhibiting the lowest error rate (entropy). The approach systematically analyses each data subset repeatedly due to the absence of explicit categorization of the target classes. The nodes at the extremity of a branch are referred to as terminal nodes. In a tree structure including non-terminal nodes, the split attribute may be used to identify them.

IV. RESULT AND DISCUSSION

For this experiment, the machine learning model was constructed using TensorFlow federated. Secure machine learning is enabled by TensorFlow. Jupiter notebook was employed to conduct the investigation. This assesses the effectiveness of the model. The efficiency of the qualitative model is assessed in terms of true positive (TP), false positive (FP), and false negative (FN). Accuracy, precision, and recall were computed. In this investigation, the Accuracy, multiclass performance measure is employed to evaluate the real model's performance.

In the course of carrying out this experiment, the collection of data represented by [18] serves as an input. Within the NSLKDD dataset, there are a total of 25192 records that are considered to be testing data, and the remaining data (around 80 percent) is considered to be training data (100781 records). In this line of work, the creation of decision rules only makes use of twenty percent of the training data.

In this methodology, training of model is performed locally at individual nodes. Aggregate algorithm is used to accumulate all node level model trainings in a central cloud storage. In this way, model aggregation is performed using the FedAVG algorithm [19].

The researchers that worked on this study used the performance criteria of accuracy, sensitivity, and specificity in order to evaluate how effectively certain algorithms function in the context of real-world settings. The results of the classifiers are shown in Figures 2 through 4. Because of its accuracy, sensitivity, and specificity, the Support Vector Machine (SVM) algorithm is a better way for categorizing malware data obtained from an Internet of Things (IoT) network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

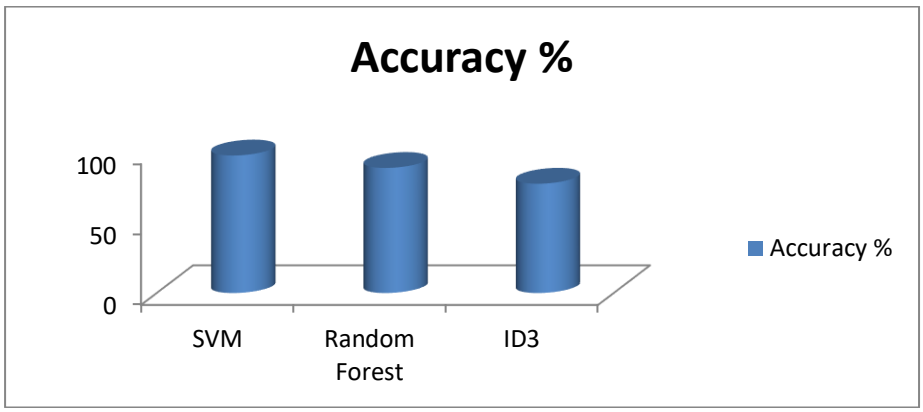

Figure 2: Accuracy of Federated Machine Learning Classifiers for IoT IDS

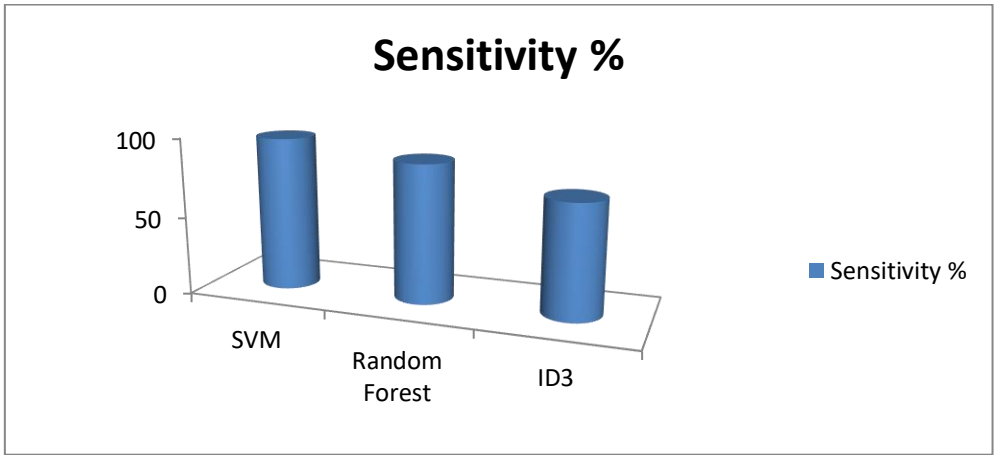

Figure 3: Sensitivity of FederatedMachine Learning Classifiers for IoT IDS

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

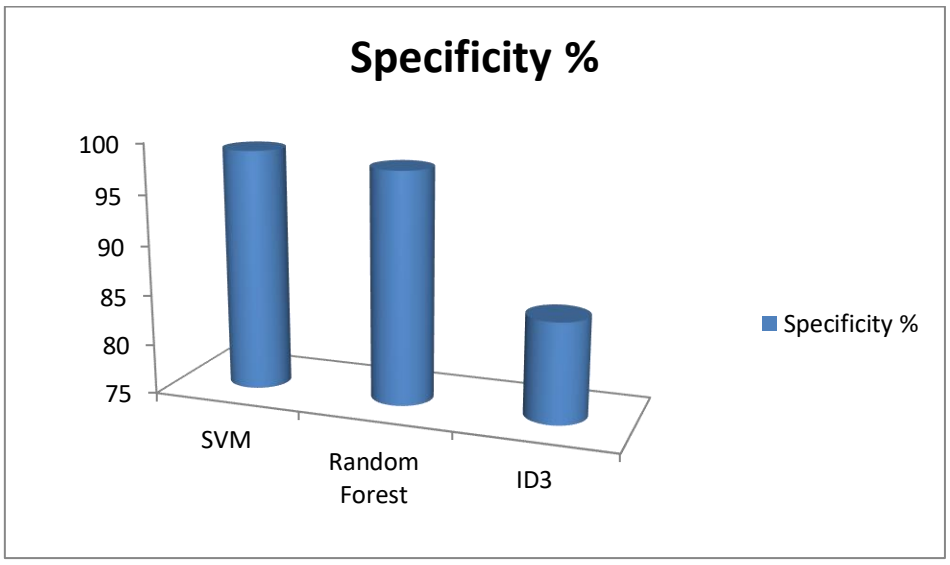

Figure 4: Specificity of FederatedMachine Learning Classifiers for IoT IDS

V. CONCLUSION

There are several facets to consider when it comes to the security of the Internet of Things, such as ensuring the well-being of both the connected devices and the Internet of Things networks to which they are connected. In spite of the fact that they were not developed with network security in mind, many other kinds of equipment, such as industrial robots, smart grids, construction automation systems, entertainment devices, and many more, are included in this. When it comes to protecting systems, networks, and data, the security of Internet of Things devices has to be able to withstand a broad variety of Internet of Things security attacks. The development of intrusion detection systems (IDSs) for the Internet of Things is a topic that is considered to be among the most pressing concerns in the area of data security. In Federated Learning, client devices (edge devices) make use of local data to train a machine learning model, and then communicate the updated model parameters to a cloud server so that they may be aggregated. Federated Learning is an example of distributed computing (rather than raw data). This paper proposes a methodology for intrusion categorization detection in Internet of Things that is enabled by federated learning and uses machine learning. Model aggregation is accomplished with the help of the FedAVG algorithm. Models are trained in their own localities, or nodes. The processes of training and testing models make use of machine learning methods such as Support Vector Machine, Random Forest, and ID3. The NSL KDD data collection is used for research and development purposes. SVM is having better accuracy, sensitivity and specificity.

REFERENCES

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 308–318

[2] T. H. Hubert Chan, Elaine Shi, and Dawn Song. 2012. Privacy-Preserving Stream Aggregation with Fault Tolerance. In Financial Cryptography and Data Security, Angelos D. Keromytis (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 200– 214

[3] Melissa Chase, Ran Gilad-Bachrach, Kim Laine, Kristin E Lauter, and Peter Rindal. 2017. Private Collaborative Neural Network Learning. IACR Cryptology ePrint Archive 2017 (2017), 762.

[4] Zarpelão, B.B.; Rodrigo, S.M.; Cláudio, T.K.; Sean, C.A. A survey of intrusion detection in Internet of Things. J. Netw. Comput.Appl. 2017, 84, 25–37.

[5] Samek,W.; Stanczak, S.;Wiegand, T. The convergence of machine learning and communications. arXiv 2017, arXiv:1708.08299.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal) |Impact Factor: 6.392|

Website: www.ijareeie.com

Vol. 7, Issue 1, January 2018

[6] Pajouh, H.H.; Javidan, R.; Khayami, R.; Dehghantanha, A.; Choo, K.-K.R. A two layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg. Top. Comput. 2016, 7, 314–323

[7] T. Eswari and V. Vanitha, "A novel rule based intrusion detection framework for Wireless Sensor Networks," 2013 International Conference on Information Communication and Embedded Systems (ICICES), 2013, pp. 1019-1022, doi: 10.1109/ICICES.2013.6508172.

[8] Y. EL Mourabit, A. Toumanari, A. Bouirden, H. Zougagh and R. Latif, "Intrusion detection system in Wireless Sensor Network based on mobile agent," 2014 Second World Conference on Complex Systems (WCCS), 2014, pp. 248-251, doi: 10.1109/ICoCS.2014.7060910.

[9] Ioannou, C. &Vassiliou, Vasos. (2018). An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. 259-263. 10.1145/3242102.3242145.

[10] S. Awatade and S. Joshi, "Improved EAACK: Develop secure intrusion detection system for MANETs using hybrid cryptography," 2016 International Conference on Computing Communication Control and automation (ICCUBEA), 2016, pp. 1-4, doi: 10.1109/ICCUBEA.2016.7860076.

[11] A. A. Gendreau and M. Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 84-90, doi: 10.1109/FiCloud.2016.20.

[12] Anthi, E., Williams, L., &Burnap, P. (2018). Pulse: an adaptive intrusion detection for the internet of things. Living In The Internet Of Things: Cybersecurity Of The Iot - 2018. doi: 10.1049/cp.2018.0035

[13] B. K. Mishra, M. Sahu and S. N. Das, "Intrusion detection systems for High Performance Computing environment," 2014 International Conference on High Performance Computing and Applications (ICHPCA), 2014, pp. 1-6, doi: 10.1109/ICHPCA.2014.7045369.

[14] R. Maqsood, N. Shahabuddin and D. Upadhyay, "A Scheme for Detecting Intrusions and Minimising Data Loss in Virtual Networks," 2014 International Conference on Computational Intelligence and Communication Networks, 2014, pp. 738-743, doi: 10.1109/CICN.2014.160.

[15] Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. Big Data Research, 3, 10-23. doi: 10.1016/j.bdr.2015.11.002

[16] G. Zhai and C. Liu, "Research and improvement on ID3 algorithm in intrusion detection system," 2010 Sixth International Conference on Natural Computation, 2010, pp. 3217-3220, doi: 10.1109/ICNC.2010.5582691.

[17] R e v a t hi, S., D. A. M a l a t hi. A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. – International Journal of Engineering Research & Technology (IJERT), Vol. 2, December 2013, Issue 12, pp. 1848-1853

[19] B. McMahan, E. Moore, D. Ramage et al., “Communication efficient learning of deep networks from decentralized data,” in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, vol. 54, pp. 1273–1282, Ft. Lauderdale, FL, USA, April 2017.