



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Next-Generation IoT Security: The Tactics for Boosting Threat Detection Performance

S.PRIYANKA, KAVIPRIYA S, HEMALATHA M, LOGESHWARI K

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

ABSTRACT: The commercialization of IoT services and applications is heavily dependent on security and privacy. Various sectors, such as healthcare and business, have been impacted by security breaches that range from basic hacking to well-coordinated intrusions at the corporate level. Due to their restrictions and the environment in which they operate, IoT devices and apps face significant security issues. IoT security and privacy concerns have been thoroughly considered from different viewpoints, including communication privacy and security, architecture data security, and identity management as well as malware analysis. explore more into the issues of security and the threat model. Improved algorithms and cross-layer architecture are also needed to address IoT privacy and security concerns. As part of an overall privacy and security method for IoT, current security solutions will be nominated for consideration, as well as new intelligent, resilient, scalable, and evolutionary methods to handle IoT security concerns.

KEYWORDS: Anomaly detection, CHAID decision tree, IoT cyber attacks, Multistep attack

I.INTRODUCTION

The Internet of Things (IoT) is becoming increasingly important in various areas, such as smart cities, healthcare, manufacturing, smart government systems, and marketing. Connected IoT objects provide automation and aid in making fateful decisions. The rapid growth and heterogeneity of an increasing number of IoT devices have intensified cybersecurity challenges. The natural mobility of the IoT and the limited capability of computational resources are jointly regarded as security limitations that increase the severity of cybersecurity threats. The intrusion detection mechanism plays an essential role in securing IoT networks. Since the 1970s, traditional intrusion detection has been used mainly to detect attacks and intrusion in the computer field and to enhance security by monitoring networks [1]. In the past decade, network evolution has resulted in scaling and fastening of the network, which allows numerous applications to rely on the network and exchange critical data through the network. Traditional IDSs failed to fulfill the requirements of a large-scale advanced network in terms of detection accuracy. To overcome the capability issues in intrusion detection in traditional IDSs, researchers have focused on utilizing the advantages of machine learning (ML) and deep learning (DL) techniques, which have recently exploded in popularity. An ML-based intrusion detection system (IDS) is a simple system for classifying network traffic by using ML mainly to detect attack patterns or abnormal traffic [2]. Both ML and DL techniques have shown tremendous improvements in intrusion detection. However, even if ML is good for classification, other methods perform better in feature transformation. For instance, ML has limited tuning capabilities, whereas DL can handle large amounts of data and can be tuned in various ways. However, both the ML approach, which heavily relies on statistical characteristics, and the DL approach, powered by large high-quality datasets, encounter difficulties when attempting to learn from a small number of examples.

The performance of ML and DL models is typically dependent on the size of the dataset; large datasets lead to good classification performance, whereas small datasets might lead to overfitting issues [3]. Network IDSs based on supervised DL techniques require a large amount of labeled data to be generalized successfully; however, gathering massive malicious data as samples to train DL classifiers is cost-prohibitive, and the field is continually developing, making these data useless or

obsolete [4]. The process of data collection is difficult, challenging, and sometimes impossible. Security and privacy regulations are among the challenges faced in data collection, as is the lack of dataset availability attributable to rare occurrences, especially in IoT networks. Apart from the limitations and prohibitive dataset collection in DL and ML, the training technique is complex and consumes a large amount of computational resources, which constrains the IoT. Moreover, ML and DL IDS-based methods suffer from detection accuracy issues and cannot detect novel attacks in some cases, such as zero-day attacks [5,6]. Today’s artificial intelligence (AI) applications (e.g., ML and DL) learn from large amounts of data, but the eventual objective of AI is to be as intelligent as humans. AI is inspired by the human brain; hence, machines should reduce the gap between AI and the human brain, avoid the complexity of the AI learning process, and easily learn new concepts by using only a few examples. Researchers have recently explored new AI techniques to fill this gap.

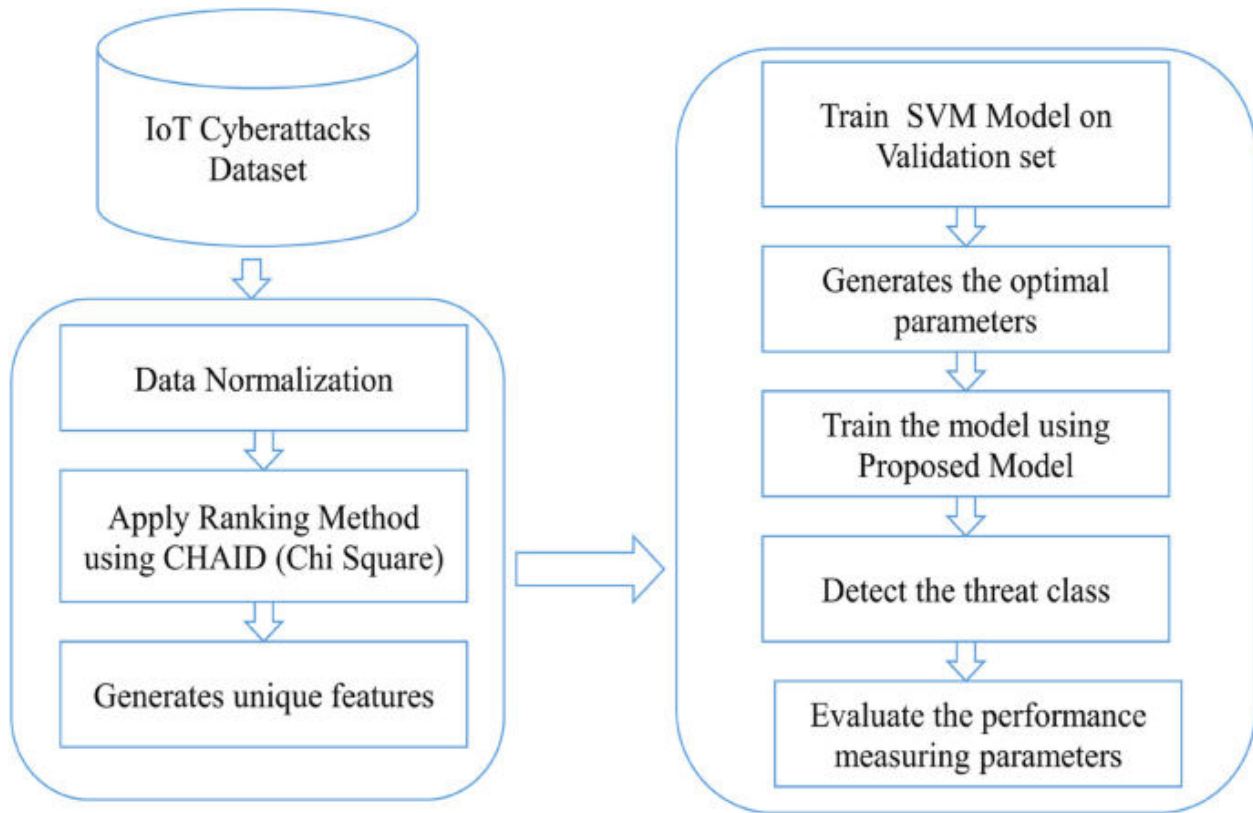


Fig 1: Next-generation cyber attack prediction for IoT

Few-shot learning (FSL) is the concept of accurately classifying objects by using a few samples in a training dataset. The first FSL model was proposed by Fink [7], who embedded samples in a kernel and successfully classified image objects to their proper class by using only one example instead of a large training dataset. FSL has since received much attention and is now a hot topic because of the scientific objective of AI in approaching human capabilities and the industry requirement for ensuring low learning costs. The following are some basic terminologies for FSL: N-way refers to the number of categories, while K-shot represents the number of samples in each category [8]. One-shot FSL simply means a one-sample-based configuration, while zero-shot FSL means the absence of samples, which means that the module learns from a distinctive defined feature. However, FSL is also the general term for all types of learning, known as low-shot learning. This method supposes the inclusion of one to three samples but is not limited to those numbers; in fact, it may contain fewer or more samples. The overall combination of N-way and K-shot is known as a support set, in which the Q-query is a test sample that is not embedded in the training set. An increase in the shot number (K-shot) improves the prediction process. Meanwhile, a low number of N-ways implies improved performance [9]. The embedding and use of FSL in IDS may aid in overcoming the

issues of data collection, rapidly training the model by using only a few samples, and harnessing the ability to detect novel attacks. The advantages of few-shot learning classification include its strong adaptability, low overheads in terms of resources, and the ability to transfer across various scenarios easily [10]. However, existing FSL intrusion detection systems models are complex and may be inappropriate for low-power networks such as IoT, and their performance is still not satisfying. In IDSs based on Siamese networks, it is challenging to control randomness in pairwise selection and they perform poorly with imbalanced data.

II. LITERATURE REVIEW

Intrusion detection is a rich area of study. Since the past decade, scientific researchers have focused on improving the performance of IDSs. Moreover, embedding various ML and DL algorithms in IDSs results in excellent performance and accuracy of the modeled algorithm compared with traditional algorithms. However, in the case of a shortage of anomalous samples, conventional ML cannot enhance the detection results, as ML and DL are highly dependent on a large amount of training data that enable the efficient training of models [12,13]. Classification is a difficult process. Several scholars have faced challenges in improving the accuracy of classification techniques in ML by using datasets of limited size because they have few features and because the classification model cannot generalize patterns shown in training data. Yang et al. [14] proposed a method for creating Gaussian distributions by using smoothness features. For outputs classified based on inputs, two inputs that are close to each other result in outputs that are also close to each other. However, the aforementioned methods suffer from issues of data replication and noise. Another approach involves two methods proposed by Andonie [15], who utilized fuzzy ARTMAP to train neural networks (NNs) on limited datasets. Nevertheless, the method is still limited and is unscalable.

Despite other attempts, FSL has achieved good classification results by using few samples. In contrast to typical ML approaches, FSL employs existing knowledge and experience to aid in the exploration of new tasks [16]. Intrusion detection approaches based on FSL can efficiently address the problem of a limited number of abnormal samples, reduce complexity, and enhance the detection rate and overall accuracy. Moreover, the application of FSL in intrusion detection has been reviewed in detail from different perspectives.

In terms of network intrusion detection, Chowdhury et al. [17] employed FSL by utilizing a CNN for feature extraction in attribute learning, and this approach was applied as an SVM input. An experiment was conducted using the KDD99 and NSL-KDD datasets, and experimental verification was performed. The findings suggest that the proposed model can effectively classify any type of attack into five primary categories with an accuracy level of 97.5%. The model can identify rare attack types by including only a few samples in learning and can handle the sample imbalance problem; the proposed model operates similarly to a hybrid CNN-SVM model. However, each model was trained separately. Hence, this kind of training is ineffective at learning the feature representation of sample data. In addition, scalability issues may occur when dealing with large amounts of data as a result of the complex structure caused by utilizing an SVM with a Gaussian kernel function as a classifier [18].

Similarly, YU and the Biennial Informatics Network (BIAN) [19] employed the advantages of deep neural networks (DNNs) and CNNs to model an IDS via FSL. The aim of the model was to overcome the lack of abnormal samples for effectively training advanced IDSs. Some attack categories involve an extremely limited number of samples, which hinders an IDS from detecting and referring to its proper class, especially for unbalanced datasets. The multistage model used only a few samples in the support and testing dataset and embedded DNN and CNN for use in feature extraction. The Euclidean distances between samples were also computed. With only 1% of the dataset used, the model achieved a high accuracy, which was 92.34% for the NSL-KDD dataset and 85.75% for the KDDTrainC + dataset. Moreover, compared with those of other approaches, the detection rates of rare analytes, such as U2R and R2L, were fivefold greater for a small sample size. Both the accuracy and false alarm rate were high, enhancing the overall IDS performance. In addition, FSL depended on a balanced dataset only.

III. METHOD

Given that related work has focused mainly on IoT networks, we conducted comprehensive scholarly reviews of various types of IoT datasets. On the basis of these reviews, we selected recent, network-simulated, and various scenarios involving different types of attacks. The dataset should also be reliable and effective for IDS classification and feature extraction. Therefore, the experiments were conducted using the MQTT-IoT-IDS2020 dataset. Furthermore, we used a common IDS

dataset to emphasize that our work can be evaluated with other works by using the FSL approach in IDS. To the best of our knowledge, the MQTT-IoT-IDS2020 dataset has not been used in FSL IDSs.

The MQTT-IoT-IDS2020 dataset is an IoT network dataset generated by Hendy et al. [32]. The dataset contributes to the IoT cybersecurity committee and is considered the first dataset simulated in the IoT MQTT network. The dataset is generated using various IoT sensor devices and aimed at recoding five different types of normal and attack behaviors. The dataset mainly consists of five classes: one normal sample record and four different types of attack. The first attack type is called Scan_A, which represents an aggressive scan attack. The second attack is recorded as Scan_sU, which refers to a UDP scan, and DDP stands for the user diagram protocol. The third one is Sparta, which is short for Sparta SSH brute force attack. The fourth record, MQTT_BF, represents MQTT brute force.

The term deception in the “CICIDS2017” dataset typically consists of three parts: CIC, IDS, and 2017. CIC stands for the Canadian Institute for Cyber Security, while IDS refers to an IDS; the last number, 2017, is the date of release. The CICIDS2017 dataset [33] is one of the most common datasets used in IDSs. This scheme has been widely emphasized in several IDS studies. The dataset is rich in content because it contains various types of intrusion attacks. Among the 15 classes, 1 class is normal and the rest are different types of cyber intrusion attacks, such as botnet, SQL injection, and DDoS attacks.

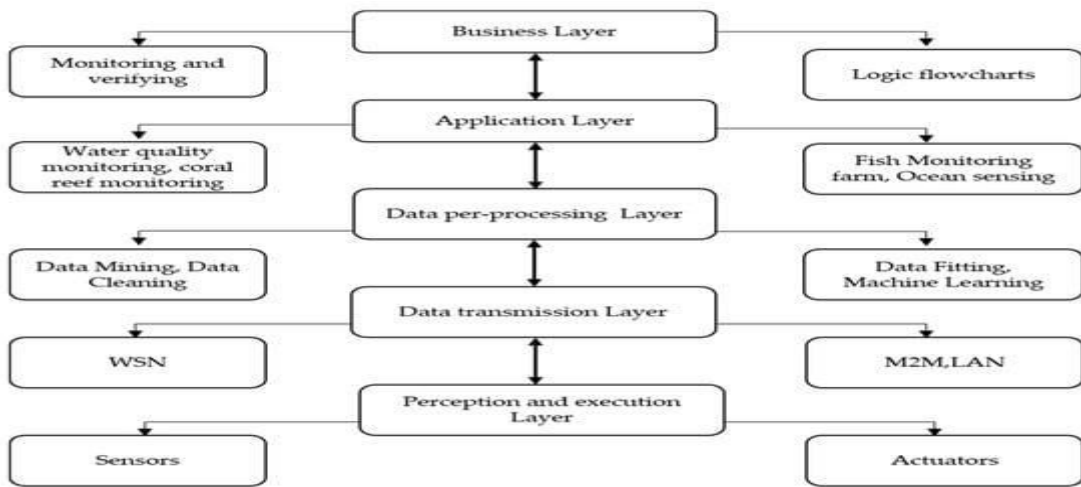


Fig 2: Data Security and Privacy

The model learns to classify query samples based on their similarity to the corresponding centroids of each class, which are computed from the support samples. The loss functions encourage the model to correctly classify both in-distribution and out-of-distribution samples. The model is trained to minimize these loss functions. The input of the model contains the original feature extracted from 1D_CNN and sets a prototype per class. Sequentially, the forward method defines how the prediction is performed after removing the fully connected layer and computes the main vectors and feature distance for each query shot and the prototype for all shots in each class to make it ready for prediction. Once the forward method is successfully applied, score calculations are performed later to classify the query shot as belonging to the correlated classes, and the query is classified as the class with the highest score, which is the lowest computed distance. In terms of the obtained optimal accurate classification, the training process is trained and evaluated for several tasks in 20 epochs. The model parameters are adjusted to backpropagate the gradients, and the loss is computed for each iteration. Additionally, the algorithm calculates and outputs the epochs and calculates the average loss. In the tuning process, we monitored the best result from the epochs; we defined this as the best validation accuracy to reach the optimal value fund during the iteration.



IV. EXPERIMENT AND RESULTS

A number of ways have been suggested to address the boundary between security and privacy concerns in DL and ML. Homomorphic encryption, differential privacy, trusted execution, and secure multiparty computing environment are the four most often used DL and ML privacy technologies. This technique uses differential privacy to prevent the adversary from figuring out which instances were utilized to build the target model. Training and testing data are protected by safe multiparty computing and homomorphic encryption. For sensitive data security and training code, trusted execution environments leverage hardware-based security and isolation. These approaches, on the other hand, greatly increase the computing burden and need a tailored approach for each type of neural network. DL or ML privacy concerns are yet to be addressed in a way that is accepted worldwide. To protect against adversarial attacks, a wide variety of security measures have been suggested, which may be divided into three categories: input preprocessing, strengthening the model's resilience, and malware detection.

Result comparison

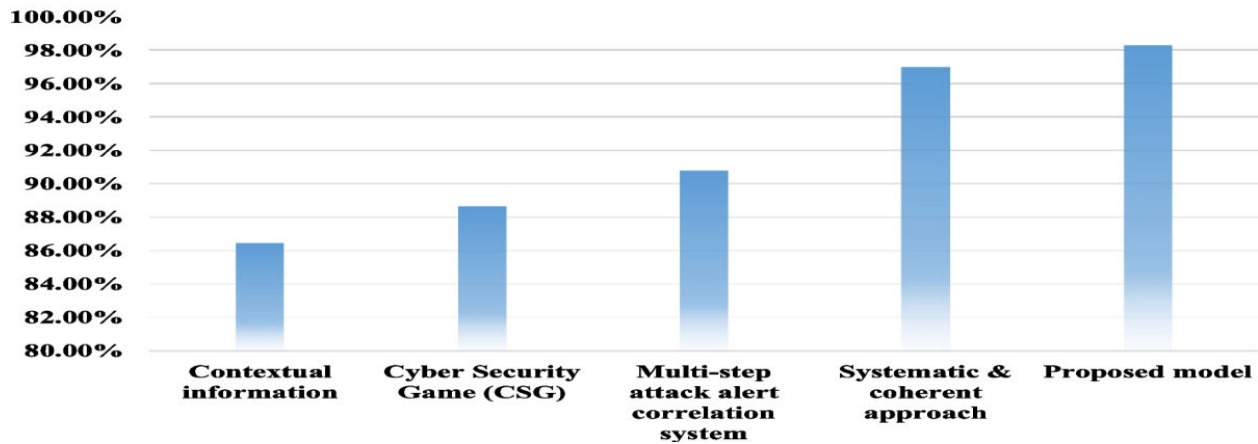


Fig 2: result of Next-generation cyber attack prediction for IoT

Preprocessing's goal is to lessen the model's reliance on immunity by doing operations such as picture transformation, randomization, and denoising that do not often need model update or retraining. Introducing regulation, feature denoising, and adversarial training as well as other techniques to strengthen the model's robustness via model retraining and change falls under the second group. Adaptive denoising and image transformation detection are the examples of third-category detection mechanisms that may be implemented before the first layer of the model. To the best of our knowledge, no defense strategy exists that can entirely protect against adversarial cases despite the many defensive mechanisms that have been offered. To counter hostile instances, adversarial training is currently the most effective technique. For poisoning attacks, there are two basic means of defense. The first is an outlier identification technique, which eliminates outliers from the relevant set. The second step is to enhance the neural network's ability to withstand contamination from poisoned samples.

V.CONCLUSIONS

Traditional security and privacy strategies have many problems linked to the complexity of IoT networks. DL and ML technology can be used to adjust IoT devices to our real life. The review considered several types of IoT threats. DL and ML are addressed with several potential solutions for ensuring IoT security. A number of DL and ML models are illustrated with their application in IoT security. This review discusses the state-of-the-art solutions for IoT privacy and security utilizing deep learning and machine learning techniques and their integration. While studying machine learning privacy and security issues, we also made an effort to develop a review of IoT threats using previous studies on DL and ML. New issues and insights of ML and DL in IoT security are addressed. Moreover, future direction, security challenges, limitations, and suggestions are included for empowering future technology.



REFERENCES

1. Al-Hadhrami, Y.; Hussain, F.K. Real time dataset generation framework for intrusion detection systems in IoT. *Futur. Gener. Comput. Syst.* **2020**, *108*, 414–423. [[Google Scholar](#)] [[CrossRef](#)]
2. Min, E.; Long, J.; Liu, Q.; Cui, J.; Cai, Z.; Ma, J. SU-IDS: A semi-supervised and unsupervised framework for network intrusion detection. In *Cloud Computing and Security*; Sun, X., Pan, Z., Bertino, E., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 322–334. [[Google Scholar](#)]
3. Althnian, A.; AlSaeed, D.; Al-Baity, H.; Samha, A.; Dris, A.B.; Alzakari, N.; Abou Elwafa, A.; Kurdi, H. Impact of dataset size on classification performance: An empirical evaluation in the medical domain. *Appl. Sci.* **2021**, *11*, 796. [[Google Scholar](#)] [[CrossRef](#)]
4. Iliyasu, A.S.; Abdurrahman, U.A.; Zheng, L. Few-shot network intrusion detection using discriminative representation learning with supervised autoencoder. *Appl. Sci.* **2022**, *12*, 2351. [[Google Scholar](#)] [[CrossRef](#)]
5. Chawla, S. *Deep Learning-Based Intrusion Detection System for Internet of Things*; University of Washington: Seattle, WA, USA, 2017; p. 72. [[Google Scholar](#)]
6. Samaila, M.G.; Neto, M.; Fernandes, D.A.B.; Freire, M.M.; Inácio, P.R.M. Security challenges of the Internet of things. In *Beyond the Internet of Things: Everything Interconnected*; Batalla, J.M., Mastorakis, G., Mavromoustakis, C.X., Pallis, E., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 53–82. [[Google Scholar](#)]
7. Fink, M. Object classification from a single example utilizing class relevance metrics. In *Advances in Neural Information Processing Systems*; MIT Press: Cambridge, MA, USA, 2004; Volume 17. [[Google Scholar](#)]
8. Wang, Y.; Yao, Q.; Kwok, J.; Ni, L.M. Generalizing from a few examples: A survey on few-shot learning. *ACM Comput. Surv.* **2020**, *53*, 1–34. [[Google Scholar](#)] [[CrossRef](#)]
9. Bontonou, M.; Béthune, L.; Gripon, V. Predicting the accuracy of a few-shot classifier. *arXiv* **2020**, arXiv:2007.04238. [[Google Scholar](#)]
10. Miao, G.; Wu, G.; Zhang, Z.; Tong, Y.; Lu, B. SPN: A Method of Few-Shot Traffic Classification with Out-of-Distribution Detection Based on Siamese Prototypical Network. *IEEE Access* **2023**, *11*, 114403–114414. [[Google Scholar](#)] [[CrossRef](#)]



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details