IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

The Web Attack Detection System for Internet of Things via Ensemble Classification

Mr. P. Manikanda Prabhu[1], Ambrish. T[2], Jagadeesh. M. N[3], Abishek. M[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *Internet of Things (IoT) networks contain millions of devices with the function of interacting with each other and providing useful things that were never available to us before. However, the diversity in types of IoT devices makes the IoT networks' environments more complex and more vulnerable to various web attacks compared to traditional computer networks. We propose a novel machine learning based Web Attack Detection System (WADS) to alleviate the serious issues that IoT networks faces. Specifically, we have used two machine learning classifier to detect web attacks separately. We then use an MLP classifier to make the final decision according to the results obtained from the Dataset. In order to evaluate the proposed system, we have performed experiments on a public dataset as well as a real-word dataset running in a distributed environment. Experimental results show that the proposed system can detect web attacks accurately with low false positive and negative rates.*

Keywords: Machine learning, MLP classifier, Internet of Things (IoT), web attack detection

I. INTRODUCTION

As one of the fastest-growing and widely used technologies on the Internet, Specifically, IoT contains millions of devices with the capability of interacting with each other and providing great convenience for us. Via IoT technology, smart cities, smart home, smart medical treatment, smart agriculture, and other smart fields are emerging. Our ways of life and work are becoming easier, more efficient, more interesting, and more convenient. There are millions of IoT devices all over the world, some of which are visible to us while others are not. The data collected from these devices and stored in datacenters contain vast amounts of information, which may contain individuals' private information. More visible and invisible threats are emerging and causing irrecoverable damages.

Due to the high concentration of various information, attackers often select storage and service servers as a primary attack target. Once the attackers gain access to the central severs, data breaches are inevitable. Furthermore, the local storage and computing limitations of IoT devices prevent them from detecting and defending against potential web attacks. A minor security threat has the potential to cause severe damage to IoT networks.

Therefore, there is no doubt that ensuring the security of IoT networks is of great significance to the success of IoT applications. Compared with traditional computer networks, there are more terminal devices and traffic in IoT networks, which make IoT network security issues more complex and troublesome [4]. Recent works covering web attack detection systems (WADS) have shown a great capacity for the protection of traditional networks.

1.1 MLP CLASSIFIERS:

We propose WADS, a novel ensemble deep learning-based system that can detect anomalous queries in which malicious codes are attached in an IoT network. We utilize a group of these deep learning models to produce different representations of URL requests in order to exploit the advantages from a variety of classification

An ensemble classifier is utilized in EDL-WADS to improve the detection performance by combining results from different classifiers based on multilayer perceptrons (MLP) and these method of analyzing URL requests and transforming them into vectors automatically shows its superior capability of representing URL requests accurately. It has become the state-of-the-art method in the field of web attack detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

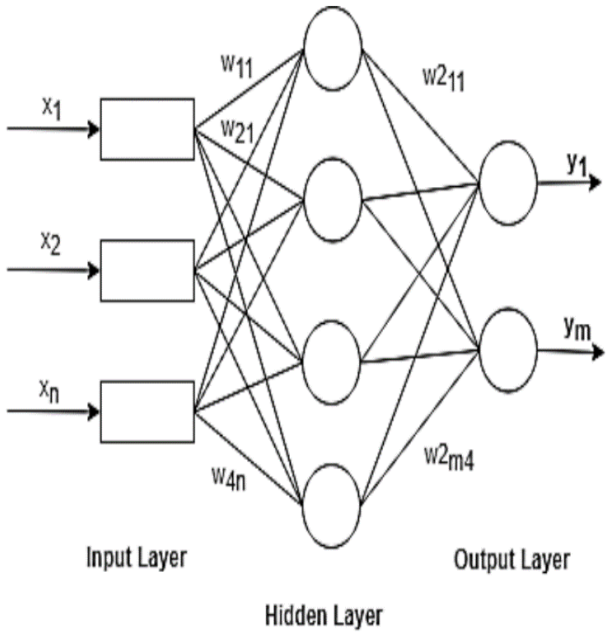


Fig 1 MLP Classifier Process Flow

II. LITERATURE REVIEW

A literature review is a body of text that aims to review the critical points of current knowledge on and/or methodological approaches to a particular topic. It is secondary sources and discusses published information in a particular subject area and sometimes information in a particular subject area within a certain time period. Usually, it has an organizational pattern and combines both summary and synthesis.

The method based on deep learning makes full use of the advantages of big data analysis and can detect web attacks more comprehensively and accurately. Ma et al. [18] used static features and evaluated the methods with the Naive Bayes model, support vector machine (SVM), and logistic regression (LR). The results show the deep learning model's capacity of identifying web attack through these static features. Also, Kar et al.[2] proposed a system for web attack detection, in which the method based on statistical characteristics is used to represent URL requests, and a novel deep learning model is used to do classification task. The results achieved a high accuracy of 96.37%. Compared with the traditional detection method, deep learning approaches based on statistical characteristics make a significant increase in the result accuracy.

These features depend on statistical characteristics of syntax trees generated by semantic analysis and syntactic analysis instead of raw requests. Lee et al. [19] proposed a novel method to detect SQL injection with removing values of SQL queries and comparing them with predetermined syntactic rules [11] used semantic tools to get a syntax tree from URL requests and defined various of statistical characteristics based on the syntax tree. Experimental results showed that their approach achieved promising performance in web attack detection.

III. PRPOSED SYSTEM

The feature learning module is applied to analyze URL requests and transform them into vectors with anomaly information attached. The deep learning models module is composed of three independent deep learning models for classification .The comprehensive decision module is utilized to combine those parallel results in order to obtain the final results for detection .The fine-tuning and updates module is designed to pretrain updates classifiers.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

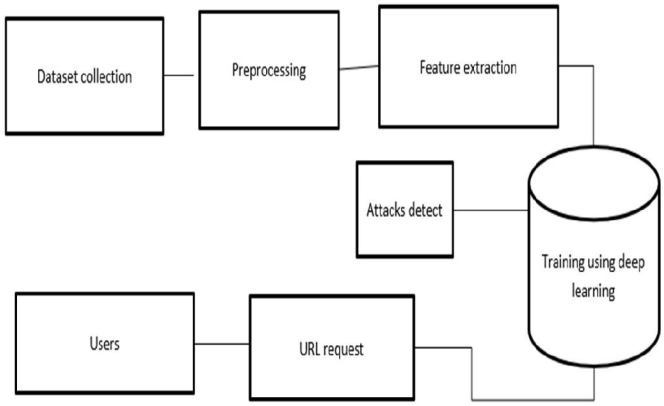


Fig 2 System Architecture of Proposed Model

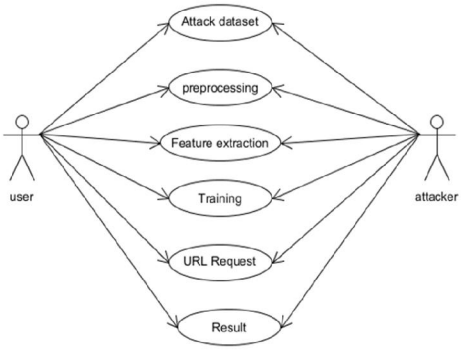


Fig 3 Use case diagram of the proposed system

IV. MODULE DESCRIPTION

Proposed System Modules

- Dataset Collection
- Pre-processing
- Feature Extraction

4.1 Dataset Collection

The CSIC 2010 dataset has been broadly used to evaluate IDS. It contains various web attacks including SQL injection, cross-site scripting (XSS), buffer overflow, etc. Significantly, we extract 3329 SQL samples, 2053 XSS samples, and 4812 benign samples and review them manually. Furthermore, we evaluate EDL-WADS on a real-word dataset, which is collected by a security company.

A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. Further the process moves and the next step of test is

To evaluate the proposed WADS, we conducted experiments on a synthetic dataset as a benchmark collected in real-time by ourselves when performing attacks to the IOT network using attack tools. As part of our Process, we implemented WADS in a distributed environment and compared WADS with several approaches.

The results are summarized in specifically, we first set group A based on our experiments and received promising results with accuracy, TPR, and FPR all higher than 98.5%. We then make little changes from group A to group C, the performance increased slowly and achieved the highest in group C. However, the performances of accuracy and precision

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

came to a sharp drop. We come to a conclusion that the kernel with size of 7 × 7 is too wide to extract useful features for the MRN model. The accuracy and precision increased immediately when the kernel of 7 × 7 is replaced. In the feature representation, we map every word in the URL requests to a vector of k-dimension, which is the row of the input matrix. T

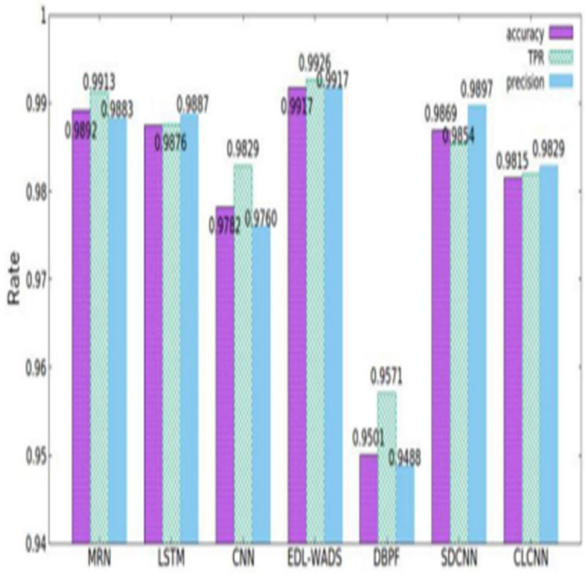


Fig 4.1 Accuracy graph on real world dataset

4.2 Pre-processing

Data preprocessing is a process of preparing the raw data and making it suitable for a machine learning model. The URL requests will be tokenized by all punctuations and become easier and more readable to handle after data processing and then, The embedding layer is added into deep learning models and is trained with classifiers , we use data preprocessing task.

In the fine-tuning and updates module, all raw URL requests, normalized data, and detection results are recorded in a database to facilitate further analysis by the security experts. Moreover, EDL-WADS is designed to take advantage of experts' analysis to fine-tune deep learning models in the training phase and update these models incrementally in order to discover new web attacks.

When one of the three models is being fine-tuned and updated, the remaining two other models continue to work. This ensures the fine-tuning and update on one model makes very little negative impact on the overall detection making. Most importantly, in terms of the reliability, our proposed system is fault tolerant, namely, when one deep learning model is under attack e.g., attacks described in two other deep learning models are still active and making decisions jointly with very little performance degradation.

In WADS, we used an MLP model as an ensemble classifier to combine all intermediate vectors and make the final decision. The structure of the ensemble classifier is depicted in Fig. 7. The inputs of the model are vectors calculated using immediate vector Vi and reliability vector Vr. The concatenation and flatten layer will merge these vectors into one and propagate it to the MLP model. The MLP model and sigmoid layer will make the final decision on web attack detection.

We perform a comprehensive check and use an ensemble classifier. The comprehensive check is to calculate a vector Vr that denotes the reliability of results of every deep learning model, as described in Algorithm. First, we get Vm that represents the average of immediate vectors.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

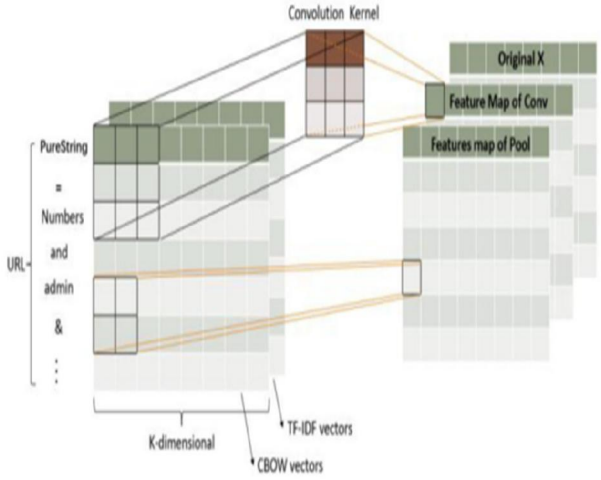


Fig 4.2 Comprehensive check of MLP classifiers

4.3 Feature Extraction

Features are the core of all deep learning applications on account of deciding the ceiling of the performance. As the first module of WADS, it plays a critical role in keeping the quality and integrity of the input data. Considering the diversity of URL requests, data processing is utilized to remove unimportant information and decode the data flow.

In the feature representation of WADS, we use two methods for URL analysis, which are a method based on embedding layers and an approach presented. Significantly, we have concluded that automatic methods performed best in related works and utilized two automatic methods to analyze URL requests and transform them into vectors in WADS.

We utilized three deep learning models for classification, they are the MRN model, LSTM model, and CNN model, respectively. Further, the process proceeds and then, the MRN is a new structure of a computing unit, which has been improved on the bias of Residual Network (ResNet).

In WADS, we designed a CNN model that uses a feature representation method based on the embedding layer. The same procedure for URL requests normalization and feature representing model. However, in method two, the embedding layer is added into deep learning models and is trained with classifiers, while in method one, the model for normalization and classifier is separate and the model for normalization needs to be pretrained independently. It demonstrates that the comprehensive check and ensemble classifier have the capability of combining results from multiple deep learning models accurately and comprehensively. As a result, it helped improve the detection performance of EDL-WADS.

```
print(train_X[0])

[ 1.16229295 -0.10964288  1.4465928  -0.62750562  0.48207798  1.13903241
  0.48442739 -0.22580129  2.49776369  0.12654803 -0.5641164   0.12672219
  0.80985203 -1.23510583 -0.5667066  -0.65169772 -0.41335536 -0.48850192
 -0.63845715]

[ ] print(test_X[0])

[-0.67658746 -0.10964288  0.47825092  0.9188512  -0.53227521 -0.54266714
 -0.53386286  0.11306708 -0.6199934   0.94683844  1.26672243  0.94812869
 -1.23479347 -0.31171765 -0.61579497 -0.70389918 -0.41335536 -0.48850192
 -0.63845715]
```

Fig 4.3 Training and Test Dataset

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

```
for model in models:
    model_name = model.__name__
    model = model(max_iter=2000)
    model.fit(train_X, train_y)
    print("Model Name:" + model_name)
    print("Train Score:" + str(model.score(train_X, train_y)))
    print("Test Score: " + str(model.score(test_X, test_y)))
```

```
/usr/local/lib/python3.7/dist-packages/sklearn/svm/_base.py:289:
  ConvergenceWarning,
Model Name:SVC
Train Score:0.8499181421712273
Test Score: 0.8484848484848485
Model Name:MLPClassifier
Train Score:0.9990919971934459
Test Score: 0.9967578325629173
Model Name:LGBMClassifier
Train Score:1.0
Test Score: 1.0
```

Fig 4.4 Accuracy Score of SVC and MLPC classifier

V. DEFINITION AND ACRONYMS

EDL-WADS: Ensemble Deep Learning based Web Attack Detection System
MRN : Modified Random Network
LSTM : Long short-term memory
CNN : Convolutional Neural Network
MLP : Multi-Layer Perceptron
URL : Uniform Resource Locator

VI. RESULT

The results obtained show that EDL-WADS achieves the highest accuracy, TPR, and precision as well as the lowest FPR. In this experiment, we collected 6075 anomalous requests from security tools and 4360 normal requests by programs automatically. The EDL-WADS system achieved 100% in TPR, which demonstrates that all web attacks are detected accurately. The other metrics also demonstrated high values. Only two of all requests are detected wrongly: normal requests were detected as malicious ones.

The security tools that we have used to perform attacks all use common and simple security rules to scan the target system. EDL-WADS detects such simple and common attacks with very high accuracy. Nonetheless, the EDL-WADS truly demonstrated its effectiveness on real-time web attacks detection, given these attack tools that we have selected are the most commonly used ones on the Internet.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

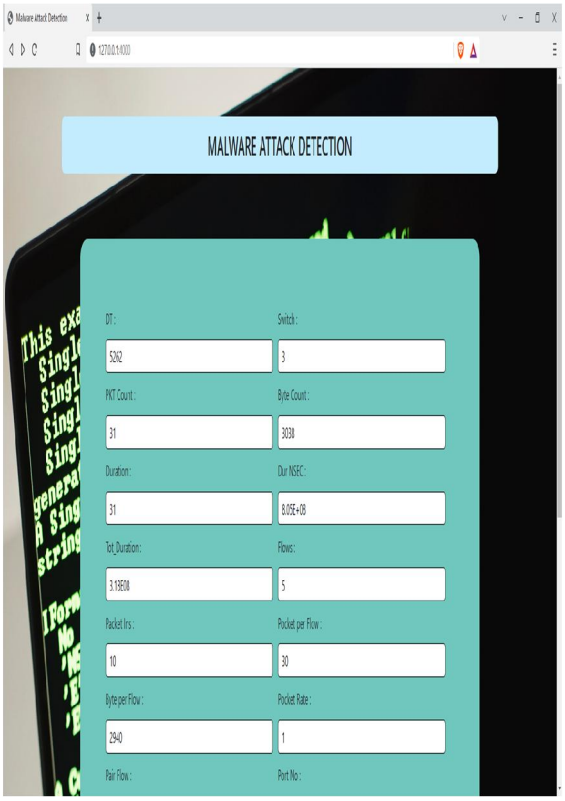
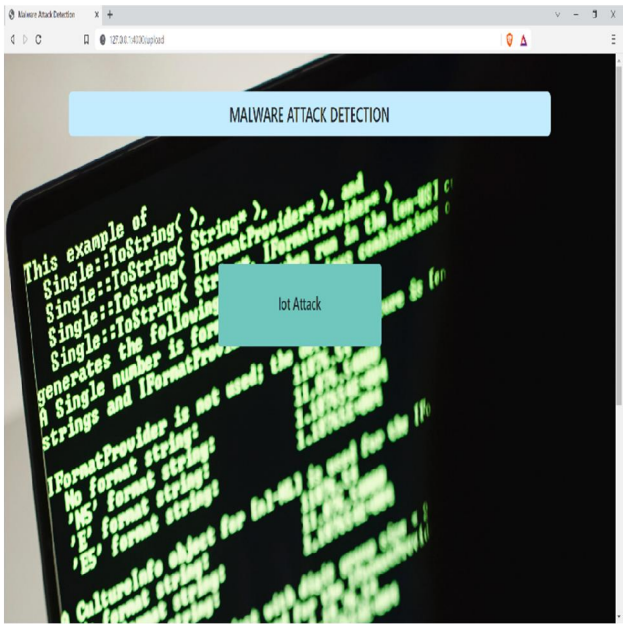


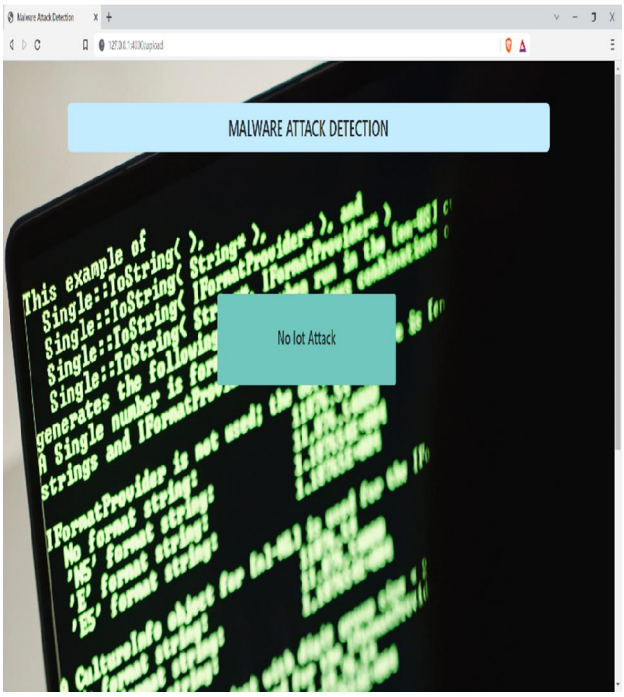
Fig 5 Output by the Proposed System

CASE 1: IOT DEVICE ATTACKED



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

CASE 2: IOT DEVICE NOT ATTACKED



VII. CONCLUSION

In this article, we proposed a novel WADS, EDL-WADS, for IoTs. Specifically, the EDL-WADS consisted of some modules. A feature learning module for URL request representations. A deep learning module composed of three deep learning models for producing different representations of URL requests in order to exploit the advantages from a variety of classification. A comprehensive decision module for combing the results from the three deep learning models and making the final decision with an ensemble classifier.

REFERENCES

[1]. M. Lin, C. Chiu, Y. Lee, and H. Pao, "Malicious URL filtering—A big data application," in Proc. IEEE Int. Conf. Big Data, 2013, pp. 589–596.

[2]. D. Kar, S. Panigrahi, and S. Sundararajan, "SQLiDDS: SQL injection detection using query transformation and document similarity," in Proc. Int. Conf. Distrib. Comput. Internet Technol., 2015, pp. 377–390.

[3]. A. Le, A. Markopoulou, and M. Faloutsos, "PhishDef: URL names say it all," in Proc. IEEE INFOCOM, 2011, pp. 191–195.

[4]. J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, "Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city," IEEE Trans. Ind. Informat., vol. 16, no. 4, pp. 2659–2666, Apr. 2020.

[5]. P. Bisht, P. Madhusudan, and V. N. Venkatakrishnan, "Dynamic candidate evaluations for automatic prevention of SQL injection attacks," ACM Trans. Inf. Syst. Secur., vol. 13, no. 2, pp. 398–404, 2010.

[6]. C. Luo, S. Su, and Y. Sun, "A convolution-based system for malicious URL requests detection," Comput. Mater. Continua, vol. 61, no. 3, pp. 399–411, 2019.

[7]. M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," IEEE Internet Things J., vol. 7, no. 7, pp. 6266–6278, Jul. 2020.

[8]. Y. H. Hwang, "IoT security & privacy: Threats and challenges," in Proc. 1st Acm Workshop on Iot Privacy Trust and Security, 2015.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

[9]. A. Jamdagni, Z. Tan, and X. He, "RePIDS: A multi-tier real-time payload-based intrusion detection system," Comput. Netw., vol. 57, no. 3, pp. 811–824, 2013.

[10]. Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denialof-service attack detection based on multivariate correlation analysis," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 447–456, Feb. 2014.

[11]. C. Torrano-Gimenez, H. T. Nguyen, G. Alvarez, S. Petrovi´c, and K. Franke, "Applying feature selection to payload-based web application firewalls," in Proc. 3rd Int. Workshop Secur. Commun. Netw., 2011, pp. 75–81.

[12]. J. Macqueen, "Some methods for classification and analysis of multivariate observations," inProc. 5th Berkeley Symp. Math. Statist. Probability, 1965, vol. 1, no. 14, pp. 281–297.

[13]. D. Kar, S. Panigrahi, and S. Sundararajan, "SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM," Comput. Secur., vol. 60, pp. 206–225, 2016.

[14]. J. Saxe and K. Berlin, "eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys," 2017, arXiv:1702.08568.

[15]. M. Ito and H. Iyatomi, "Web application firewall using character-level convolutional neural network," in Proc. IEEE 14th Int. Colloq. Signal Process. Its Appl., 2018, pp. 103–106.

[16]. J. Liang, W. Zhao, and W. Ye, "Anomaly-based web attack detection: A deep learning approach," in Proc. VI Int. Conf. Netw., Commun. Comput., 2017, pp. 80–85.

[17]. J. Qiu, Z. Tian, and C. Du, "A survey on access control in the age of Internet of things," IEEE Internet Things J., vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[18]. J. Ma, L. K. Saul, and S. Savage, "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," in Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2009, pp. 1245–1254.

[19]. I. Lee, S. Jeong, and S. Yeo, "A novel method for SQL injection attack detection based on removing SQL query attribute values," Math. Comput. Modelling, vol. 55, no. 1-2, pp. 58–68, 2012.

[20]. F. Yong, P. Jiayi, L. Liang, and H. Cheng, "WOVSQLI: Detection of SQL injection behaviors using word vector and LSTM," in Proc. 2nd Int. Conf. Cryptography, Secur. Privacy, 2018, pp. 170–174.

[21]. T. Liu, Y. Qi, L. Shi, and J. Yan, "Locate-then-detect: real-time web attack detection via attention-based deep neural networks," in Proc. Joint Conf. Artif. Intell., 2019, pp. 4725–4731.

[22]. Y. Zhou and G. Cheng, "An efficient intrusion detection system based on feature selection ensemble classifier," Computer Networks., vol. 174, 2020, Art. no. 107247.

[23]. R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Detecting malicious domain names using deep learning approaches at scale," J. Intell. Fuzzy Syst., vol. 34, no. 3, pp. 1355–1367, 2018. [24] M. E. Ahmed and K. Hyoungshick, "Poster: Adversarial examples for classifiers in high-dimensional network data," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2017, pp. 2467–2469.

[24]. N. Papernot, P. Mcdaniel, and I. Goodfellow, "Practical black-box attacks against machine learning," in Proc. ACM Asia Conf. Comput. Commun. Secur., 2017, pp. 506–519.

[25]. Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 1963–1971, Mar. 2020.

[26]. M. Zhang, B. Xu, and S. Bai, "A deep learning method to detect web attacks using a specially designed CNN," in Proc. Int. Conf. Neural Inf. Process., 2017, pp. 828–836.

[27]. HTTP DATASETCSIC 2010. [Online]. Available: https://www.isi.csic.es/ dataset/