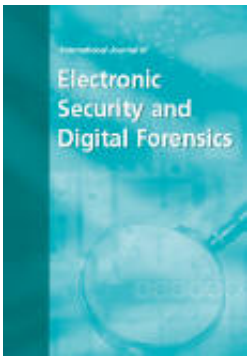


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

IoT security using deep learning algorithm: intrusion detection model using LSTM

Abitha V.K. Lija, R. Shobana, J. Caroline Misbha, S. Chandrakala

DOI: 10.1504/IJESDF.2025.10063216

Article History:

Received:	17 September 2023
Last revised:	31 October 2023
Accepted:	13 November 2023
Published online:	23 December 2024

IoT security using deep learning algorithm: intrusion detection model using LSTM

Abitha V.K. Lija*

Department of CSE,
Meenakshi College of Engineering,
Chennai, 78, India
Email: abithavklija@gmail.com
*Corresponding author

R. Shobana

Department of CSE,
S.A. Engineering College,
Thiruverkadu Post, Chennai – 600077, India
Email: rubanshobana@gmail.com

J. Caroline Misbha

Department of CSE,
Arunachala College of Engineering,
Tamil Nadu, 629203, India
Email: caroline.misbha@gmail.com

S. Chandrakala

Department of Computer Science and Engineering,
Meenakshi College of Engineering,
Chennai, 78, India
Email: pmsschandra@gmail.com

Abstract: Internet of things (IoT) and the integration of many gadgets is rapidly becoming a reality. IoT devices, particularly edge devices, are particularly vulnerable to cyberattacks as a result of the proliferation of device-to-device (D2D) connectivity Advanced network security measures are required to do real-time traffic analysis and to mitigate malicious traffic. These mechanisms must also be able to detect malicious traffic. We describe a game-changing approach to detect and classify new malware in record time. This will allow us to handle the difficulty that has been presented (zero-day malware). This article puts out the idea of a hybrid deep learning (DL) model for the detection of cyber attacks. Long short-term memory (LSTM) and gated recurrent unit are the foundations of the model that has been suggested (GRU). The results of the experiments are quite encouraging, revealing an accuracy rate of 94.50% for the identification of malware traffic.

Keywords: deep learning; gated recurrent units; internet of things; IoT; long short-term memory; LSTM; machine learning.

Reference to this paper should be made as follows: Lija, A.V.K., Shobana, R., Misbha, J.C. and Chandrakala, S. (2025) 'IoT security using deep learning algorithm: intrusion detection model using LSTM', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.283–293.

Biographical notes: Abitha V.K. Lija completed her BE in CSE from the CSI Institute of Technology, Thovalai affiliated to Anna University. She completed her ME in CSE from the Jerusalem College of Engineering affiliated to Anna University. She is currently working as an Assistant Professor in the Department of CSE in Meenakshi College of Engineering. Her area of interest includes IoT, cyber security, big data, network security and machine learning.

R. Shobana received her BE in Computer Science and Engineering from the Ponjesly College of Engineering, Nagercoil, India in 2009 and ME in Computer and Engineering from the Anna University, Coimbatore, India in 2011. She is currently working as an Assistant Professor in the S.A. Engineering College, Chennai. She is currently pursuing PhD at the Department of Computer Science and Engineering at S.A. Engineering College under Anna University, Chennai, India. Her areas of interest are cyber security, deep learning, machine learning, cloud computing and quantum learning.

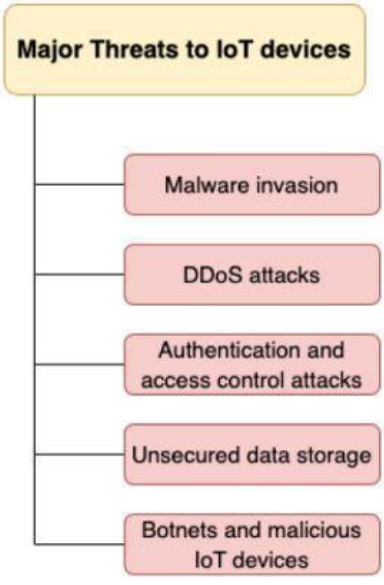
J. Caroline Misbha received her BE in Computer Science and Engineering from the Vins Christian College of Engineering, Nagercoil, India in 2009 and ME in Computer and Communication from The Rajas Engineering College, Vadakkangulam, India in 2011. She is currently working as an Assistant Professor in Arunachala College of Engineering for Women, Nagercoil. She is currently pursuing PhD at the Department of Electronics and Communication Engineering, PSN Engineering and Technology, Tirunelveli, India. Her areas of interest are big data, network security, machine learning and data mining.

S. Chandrakala obtained her Bachelor's in Computer Science and Engineering from the R.V.S. college of Engineering, Dindigul affiliated to Anna University, Chennai and ME in the Dr. Sivanthi Aditanar College of Engineering, Tiruchendur affiliated to Anna University, Chennai, India. She has three years of teaching experience and currently working as an Assistant Professor in Department of Computer Science and Engineering, Meenakshi College of Engineering, Chennai. Her areas of interest include image processing, machine learning, IoT and cyber security. She is a member of IAENG Professional Society.

1 Introduction

The internet of things (IoT), sometimes known as IoT (Tewari et al., 2018; Arisdakessian et al., 2022), is a concept that is predicated on the decentralisation of computers via the use of edge devices rather than depending on a centralised framework. These peripheral gadgets might be regional servers or frequently used gadgets like smartphones and laptops. IoT has completely changed the way devices communicate with one another because it makes device-to-device (D2D) communication simple. Some of the most important ones are that it permits several communication protocols to coexist and that a centralised server is not required (Cvitic et al., 2021).

Figure 1 Major dangers to IoT network devices (see online version for colours)



Edge computing, which makes use of IoT devices, Lu et al. (2021) has made it possible for computation to take place close to the data source, which has dramatically expanded the amount of data that can be collected and processed at the edge itself (Dahiya et al., 2022; Vinoth et al., 2022). On the other hand, since it is now so easy to send and receive data at the edge, this has resulted in a significant increase in internet traffic at the edge, that leaves these websites open to the risk of being attacked by cybercriminals (Sahoo et al., 2018). There have been many various ideas offered as potential answers to the problem of cyber threats to IoT devices. Some of these ideas include encryption methods like homomorphic encryption and secure-multiparty computing. Other ideas involve introducing noise via differential privacy. The use of artificial intelligence, on the other hand, is one of the most innovative approaches that may be used to solve the issue of cyber attacks.

1 *The identification of anomalies:* A file or data source may be evaluated with the use of anomaly detection to determine whether or not it contains malicious code. In most cases, massive datasets that have already been labelled are already accessible and may be used to train a model that can determine whether or not a particular file contains dangerous content. Anomaly detection often employs machine learning techniques such as support vector machines, Naive Bayes, decision trees, random forests, and others. It is advantageous to avoid DDoS attacks since SVM is so good at building nonlinear separation planes. More complex datasets are no problem for decision trees and random forest. Deep learning (DL) and neural networks are two methods that may be used to process data that is increasingly complicated.

2 *The anticipation of cyber attacks:* One preventative measure that may be used against cyber dangers is known as cyberattack forecasting. It can identify threats to a network system in real-time, in contrast to anomaly and malware analysis, which might be helpful for studying the type and severity of dangerous files. Monitoring

the incoming and outgoing traffic on an internet network is the method that is used most often for predicting potential cyber attacks. The patterns that emerge from the time-series investigation of the data on internet traffic need to demonstrate long-range dependencies. The RNN, long short-term memory (LSTM), and bi-LSTM models are often used in DL because of their ability to provide value predictions based on earlier sequential inputs.

3 *Controlling access while authenticating users:* Authentication and access control for certain authority may be decided by employing facial recognition (Vinoth et al., 2022; Sahoo et al., 2018; Gupta et al., 2009) or fingerprint identification systems that are constructed on deep CNN models. These systems can be used to identify who should have access to what. In addition, voice recognition software may be constructed by combining a deep neural network (DNN) with a recurrent neural network (RNN) or any of its derivatives. These capabilities may be readily activated on edge devices such as mobile phones, computers, and so on.

2 Related works

Maintaining a level of cyber security is an absolute need for any IoT network infrastructure. The last several years have seen an increase in the number of cyber security threats, including DDoS (Gupta et al., 2009; Dahiya et al., 2021; Gaurav et al., 2022; Chhabra et al., 2013; Negi et al., 2013; Gupta et al., 2012; Gulihar et al., 2022), XSS (Gupta et al., 2016, 2015a, 2015b; Mishra et al., 2011), and phishing (Jain et al., 2016; Almomani et al., 2013; Jain et al., 2018; Gupta and Jain, 2020; Mishra et al., 2018). Extensive research has been conducted on, the protocols that are necessary for machine-to-machine communication, as well as the problems about its security and privacy. When it comes to choosing a specific device for communication, many different types of systems depend on trusted computational models. Despite this, it is possible for a trusted device to include data that might potentially damage the user. There have been a great number of models and research conducted that go into great detail on the function that machine learning solutions play in IoT networks. Big data-based DDoS attack detection was suggested by the author in passage.

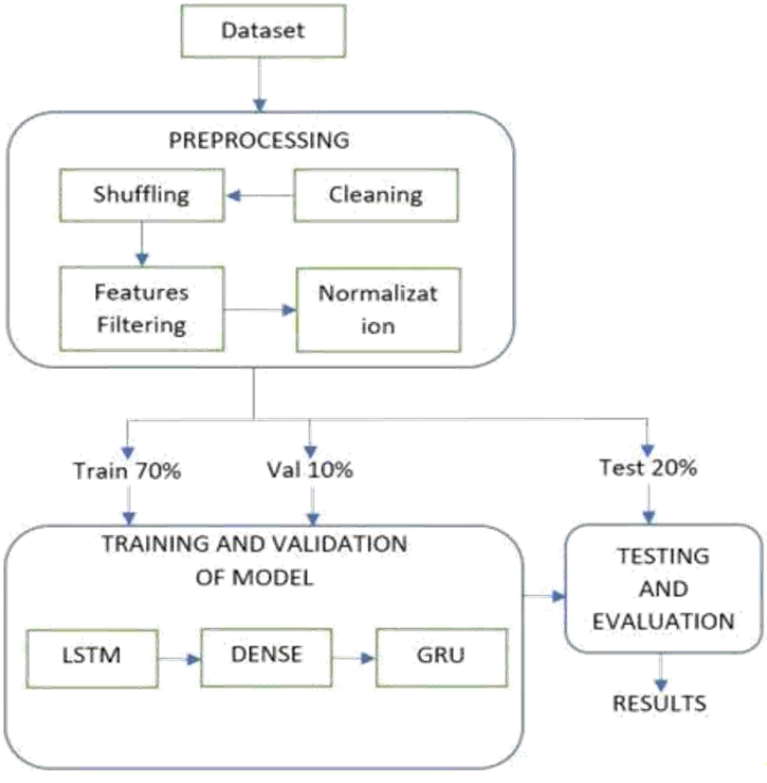
Artificial intelligence encompasses fields such as machine learning (Cvitic et al., 2021) and DL algorithm research (AI). The use of machine learning to combat cyber security risks has shown promising results. It can not only be used to identify harmful attacks, but also to predict them in order to stop them before they ever start. These are completely new kind of assaults that nobody has ever seen before. The classifications are primarily divided into three kinds of subdivisions, which are supervised, unsupervised, and reinforcement learning. Each of these subtypes is described below. Learning in reinforcement learning is based on action-response system, making it an entirely distinct paradigm of artificial intelligence than traditional machine learning. It is possible that supervised and unsupervised learning strategies will be combined in the process of reinforcement learning. Semi-supervised learning is another category that is gathering more and more attention, particularly in the area of cyber security. Learning via semi-supervision involves making use of a limited quantity of labelled data in order to categorise or create labels for a substantial amount of data that has not been labelled. In the following subsections, we will address the application of supervised, unsupervised,

semi-supervised, and reinforcement learning approaches to minimise the effects of cyber security concerns.

3 Methodology

Many studies have employed LSTM or GRU for multiple layer models, or integrated it with other DL algorithms, in order to increase the effectiveness of the recognition rate of malicious attacks in the networks. However, this results in a high reaction time for the system. Both LSTM and GRU are trained to operate on time series data.

Figure 2 Intrusion detection model diagram (see online version for colours)

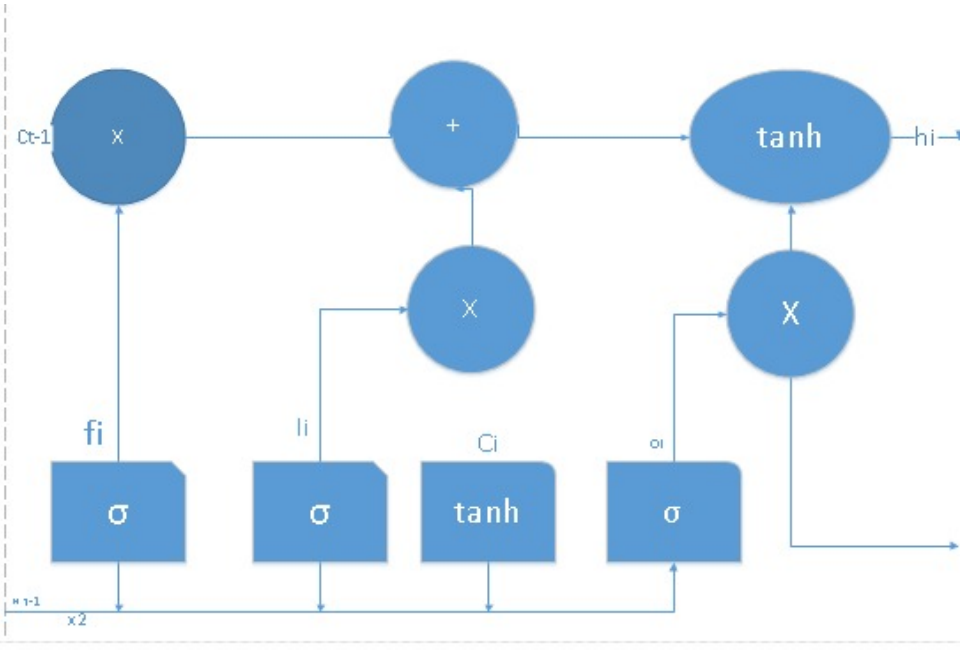


Both the LSTM and the GRU are designed to solve the issue of the RNN's disappearing gradient. When it comes to detecting intrusions, the functioning of multiple layer LSTM is superior; nevertheless, the reaction time is slow. In addition to this, the reaction time of GRU is shorter, but its functioning is not as excellent as that of LSTM. We propose a hybrid DL model that blends the two. Figure 2 provides a block diagram representation of the suggested design for the system. The LSTM layer, the DENSE layer, and the GRU layer make up this structure. The new model cuts down on the amount of time needed for training and reaction across numerous layers of LSTM, resulting in improved performance when it comes to identifying malicious attacks in networks.

3.1 LSTM

The model starts with an LSTM layer. In the combined DDoS dataset, the first hidden layer input is expressed as (none, 48, 1). In this case, the number of instances that make up the dynamic size is 'none', the number of features is '48', and the value of the third dimension is '1'. The combined DDoS dataset has an output shape of (none, 48, 24), while the car-hacking dataset has an output shape of (none, 10, 20). The next layer will take one of these forms as input. The data flow of an LSTM may be manipulated because to its many gates. These gates, for example, control how information enters, is stored, and leaves the system. It is accompanied by two more phases, the cell state and the concealed state. Figure 3 depicts the LSTM in its simplest version.

Figure 3 LSTM architecture



3.2 DENSE

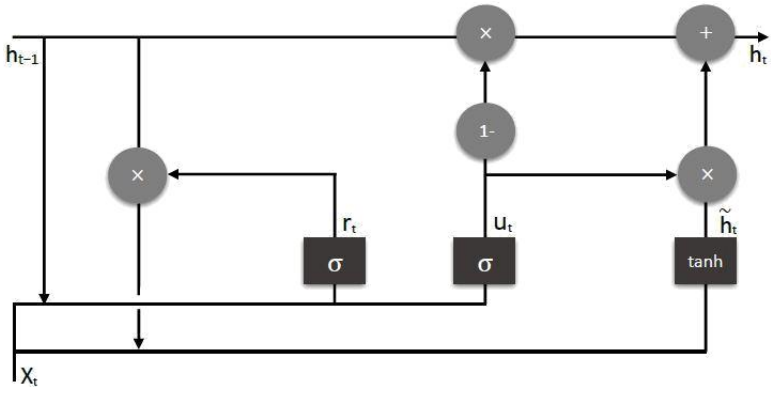
The suggested model has a second layer called DENSE, which is designed to deliver rapid answers. This layer connects LSTM and GRU. The values for the combined DDoS dataset are obtained by the DENSE layer in the shape (none, 48, 24), whereas the values for the car-hacking dataset are obtained in the shape (none, 10, 20). The layer below it is linked to this one by a connection. The next datasets each have a different output shape from this layer. ReLU could only take in positive values. The experimentally-verified positive findings might be any number from 0 to 1. In addition to being faster than other activation functions, the ReLU function also helps fix the problem of vanishing gradients. The ReLU may be understood by looking at equation (4).

$$Rx = \max(0, x) \tag{4}$$

3.3 GRU

The GRU layer is the third one in the proposed model, and it is the one that generates the final output by using the values that were obtained from the DENSE layer. The values for the combined DDoS dataset are sent to the GRU layer in the form of the shape (none, 48, 12), while the values for the car-hacking dataset are transferred in the form of the shape (none, 10, 10). The probabilities of successful output are computed at this layer. Resetting the gate, updating the gate, and concealing the status are the three gates that make up GRU and is shown in Figure 4 (one in each gate).

Figure 4 Basic architecture of GRU



4 Results and discussion

4.1 Datasets

For the purpose of intrusion detection, a variety of real-time network datasets are already available.

The datasets were used to simulate attacks on the respective networks.

4.2 Cleaning

Every dataset contains a number of records. Before beginning the training process, it is necessary to inspect the dataset for entries that are blank or undefined. These searches resulted in the return of Boolean values, which were either true or false. If the value was true, it indicated that the dataset had some missing or infinite values, but if it was false, it indicated that the dataset was complete. During the course of our investigations, we made use of two datasets, each of which had some entries that were undefined or empty. In order to tidy up these datasets, all ambiguous entries were replaced with blank records instead of being left alone. Following the transformation of undefined values into empty values, every record that was already empty was deleted from the datasets.

4.3 Shuffling

The tuples in the dataset are randomly mixed together using this method. Both kinds of data were necessary in order for the model to be trained and validated. It was necessary to reshuffle the data in order to increase the quality of the tests and the performance of the model. It was decided to employ the shuffling approach in order to generate a random order for all of the data.

4.4 Feature filtering

There are several attributes, or qualities, that define a dataset. Overfitting and underfitting are caused when a dataset includes several characteristics, some of which are irrelevant and have no effect on the output label. Remove it from the dataset if it includes many characteristics but none of them are relevant to the output label. The process of feature selection involves removing from a dataset any characteristics that are deemed to be irrelevant and keeping only those elements that are deemed to be significant. The primary purpose of feature selection was to increase its overall performance, and cut down on the amount of time required for both its training and its response.

4.4.1 Normalisation

Normalisation is a method used to fix issues in a dataset, such unequal values across features, by rescaling the numbers to fit within a predetermined range. In addition to eliminating outliers, such as features with wildly divergent values, normalisation may also be used to clean up a dataset. Based on our research, the dataset contains several characteristics with very high values as well as features with extremely low values, such as negative values. In order to find a solution to this issue, the category traits were, first and foremost, transformed into numerical values. Because each feature was comprised of numerous categories, using one-hot encoding necessitated using a higher memory capacity and took more time. Following the conversion, we used the min-max normalisation strategy to normalise data within the range of 0 and 1 by using equation (5).

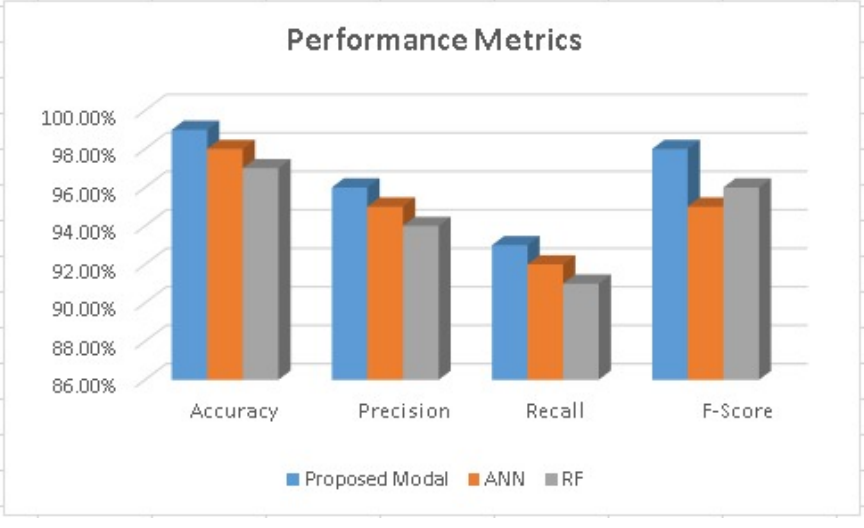
$$X_{norm} = X - X_{\min} / \left(X_{\max} - X_{\min} \right) \tag{5}$$

A 20% sample of the dataset's pre-processed data was used for the testing of the model. The proposed model, along with LSTM and GRU, also took part in long-term performance testing. A total of 2,549,370 samples, split into 79,668 batches of size 32, were used to verify the suggested model. The overall amount of time spent testing was 692 seconds, whereas the time spent on each batch was 8.7 milliseconds. The entire amount of time that was spent testing LSTM was 1,307.33 seconds, whereas the amount of time that was spent testing GRU was 1116 seconds. Based on the results of the testing, it is clear that the suggested model is more efficient than LSTM and GRU.

The Adam and Nadam optimisers both provide results that are superior to those produced by the Adamax optimiser. During this trial, we found that using Nadam on the suggested model and LSTM yielded the best results for multi-classification as well as binary classification. In this study, we evaluated the effectiveness of the suggested system by the use of k-fold crossvalidations. In addition, three-fold, five-fold, and seven-fold analyses were performed on the DDoS dataset. The suggested system continued to

provide the same level of performance, and the tabulated results can be seen in Table 1. Table 1 illustrate comparisons of the proposed research with several machine learning techniques.

Figure 5 Evaluation on Adam with the combined DDoS dataset (see online version for colours)



Deeper layers of LSTM and GRU produced greater outcomes, albeit at the expense of increased training time. Based on the findings of the experiments, the proposed model achieved success rates of more than 99% for binary and multi-class classification.

Table 1 Comparison of the HDL-IDS with other ML algorithms on the combined DDoS dataset

Algorithms	*Precision*	*Recall*	*F1-score*	*Accuracy*
Naïve Bayes	0.8003	0.7781	0.7790	0.7292
Decision tree	0.9603	0.8199	0.8745	0.9281
SVM	0.9479	0.8966	0.9267	0.9254
LSTM	0.9994	0.9997	0.9995	0.9997
GRU	0.9940	0.9963	0.9951	0.9952
Proposed study	0.9997	0.9998	0.9997	0.9998

5 Conclusions

The rapid expansion of smart vehicle networks has provided hackers with access to a number of previously inaccessible entry points. Attacks against networks that are contained inside vehicles have the potential to result in fatalities and major accidents. Based on the findings of this research, it is recommended that network intrusion detection systems use a hybrid DL model. The approach that is being proposed makes use of a hybrid mix of LSTM and GRU, which reduces the amount of time that is necessary for training as well as response. In order to evaluate how effectively the suggested method

works, a large number of tests were performed on a combined dataset, in addition to car-hacking datasets. These testing were extensive. The results of the studies indicate that the model that was provided has an accuracy of 99.5% for the combined DDoS dataset.

References

Almomani, A. et al. (2013) *Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection Zero-Day Phishing Email*, arXiv preprintarXiv: 1302.0629.

Arisdakessian, S., Wahab, O., Mourad, A., Otrok, H. and Guizani, M. (2022) 'A survey on IoT intrusion detection: federated learning, game theory, social psychology and explainable AI as future directions', *IEEE Internet of Things Journal*, Vol. 4, No. 15, p.1, Article ID: 34631.

Chhabra, M. et al. (2013) 'A novel solution to handle DDoS attack in MANET'.

Cvitic, I. et al. (2021) 'Ensemble machine learning approach for classification of IoT devices in smart home', *International Journal of Machine Learning and Cybernetics*, Vol. 12, No. 11, pp.3179–3202.

Dahiya, A. et al. (2021) 'A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense', *Future Generation Computer Systems*, Vol. 117, pp.193–204, ISSN 0167-4048.

Dahiya, A., Gupta, B., Alhalabi, W. and Ulrichd, K. (2022) 'A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media', *International Journal of Intelligent Systems*, pp.82–85.

Gaurav, A. et al. (2022) 'DDoS attack detection in vehicular ad-hoc network (VANET) for 5G networks', in *Security and Privacy Preserving for IoT and5G Networks*, pp.263–278, Springer.

Gulihar, P. et al. (2020) 'Cooperative mechanisms for defending distributed denial of service (DDoS) attacks', in *Handbook of Computer Networks and Cyber Security*, pp.421–443, Springer, Switzerland.

Gupta, B.B. and Jain, A.K. (2020) 'Phishing attack detection using a search engine and heuristics-based technique', *Journal of Information Technology Research*, Vol. 13, No. 2, pp.94–109.

Gupta, B.B., Joshi, R.C. and Misra, M. (2009) 'Defending against distributed denial of service attacks: issues and challenges', *Information Security Journal: A Global Perspective*, Vol. 18, No. 5, pp.224–247.

Gupta, B.B., Misra, M. and Joshi, R.C. (2012) *An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach*, arXiv preprintarXiv: 1203.2400.

Gupta, S. et al. (2015a) 'PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications', in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, pp.1–8.

Gupta, B., Gupta, S., Gangwar, S., Kumar, M. and Meena, P. (2015b) 'Crosssite scripting (XSS) abuse and defense: exploitation on several testing bed environments and its defense', *Journal of Information Privacy and Security*, Vol. 11, No. 2, pp.118–136.

Gupta, S. et al. (2016) 'XSS-Safe: a server-side approach to detect and mitigate cross-site scripting (XSS) attacks in JavaScript code', *Arabian Journal for Science and Engineering*, Vol. 41, No. 3, pp.897–920.

Jain, A.K. et al. (2016) 'Comparative analysis of features based machine learning approaches for phishing detection', in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, pp.2125–2130.

Jain, A.K. et al. (2018) 'Phish-safe: URL features-based phishing detection system using machine learning', in *Cyber Security*, pp.467–474, Springer, Switzerland.

Lu, J. et al. (2021) 'Blockchain-based secure data storage protocol for sensors in the industrial internet of things', *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 8, pp.5422–5431.

Mishra, A. et al. (2011) 'A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques', in *2011 European Intelligence and Security Informatics Conference*, IEEE, pp.286–289.

Mishra, A. et al. (2018) 'Intelligent phishing detection system using similarity matching algorithms', *International Journal of Information and Communication Technology*, Vol. 12, Nos. 1–2, pp.51–73.

Negi, P. et al. (2013) *Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment*, arXiv preprint arXiv: 1304.7073.

Sahoo, S.R. et al. (2018) 'Security issues and challenges in online social networks (OSNs) based on user perspective', *Computer and Cyber Security*, 1st ed., pp.591–606, Auerbach Publications, eBook ISBN9780429424878.

Tewari, A. et al. (2018) 'A mutual authentication protocol for IoT devices using elliptic curve cryptography', in *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, pp.716–720.

Vinoth, R. et al. (2022) 'An anonymous pre-authentication and post authentication scheme assisted by cloud for medical IoT environments', *IEEE Transactions on Network Science and Engineering*, Vol. 9, No. 5, pp.3633–3642.