Hindawi
Journal of Sensors
Volume 2024, Article ID 9853625, 1 page
https://doi.org/10.1155/2024/9853625

Retraction

Retracted: Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm

Journal of Sensors

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] P. R. Kshirsagar, H. Manoharan, H. A. Alterazi, N. Alhebaishi, O. B. J. Rabie, and S. Shitharth, "Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm," *Journal of Sensors*, vol. 2022, Article ID 9386989, 13 pages, 2022.

Hindawi
Journal of Sensors
Volume 2022, Article ID 9386989, 13 pages
https://doi.org/10.1155/2022/9386989

Research Article

Construal Attacks on Wireless Data Storage Applications and Unraveling Using Machine Learning Algorithm

Pravin R. Kshirsagar,[1] **Hariprasath Manoharan**,[2] **Hassan A. Alterazi**,[3] **Nawaf Alhebaishi**,[4] **Osama Bassam J. Rabie**,[4] **and S. Shitharth**[5]

[1]*Department of Artificial Intelligence, G. H. Raisoni College of Engineering, Nagpur, India*
[2]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Chennai, India*
[3]*Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia*
[4]*Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia*
[5]*Department of Computer Science & Engineering, Kebri Dehar University, Kebri Dehar, Ethiopia*

Correspondence should be addressed to S. Shitharth; shitharths@kdu.edu.et

Received 8 July 2022; Accepted 3 August 2022; Published 16 August 2022

Academic Editor: Sweta Bhattacharya

Cloud services are a popular concept used to describe how internet-based services are delivered and maintained. The computer technology environment is being restructured with respect to information preservation. Data protection is of critical importance when storing huge volumes of information. In today's cyber world, an intrusion is a significant security problem. Services, information, and services are all vulnerable to attack in the cloud due to its distributed structure of the cloud. Inappropriate behavior in the connection and in the host is detected using intrusion detection systems (IDS) in the cloud. DDoS attacks are difficult to protect against since they produce massive volumes of harmful information on the network. This assault forces the cloud services to become unavailable to target consumers, which depletes computer resources and leaves the provider exposed to massive financial and reputational losses. Cyber-analyst data mining techniques may assist in intrusion detection. Machine learning techniques are used to create many strategies. Attribute selection techniques are also vital in keeping the dataset's dimensionality low. In this study, one method is provided, and the dataset is taken from the NSL-KDD dataset. In the first strategy, a filtering method called learning vector quantization (LVQ) is used, and in the second strategy, a dimensionality-simplifying method called PCA. The selected attributes from each technique are used for categorization before being tested against a DoS attack. This recent study shows that an LVQ-based SVM performs better than the competition in detecting threats.

1. Introduction

Cloud computing is the ecosystem in which individuals pool information, services, and knowledge using system resources offered through the internet. It creates a convenient and dynamic infrastructure for computing for business organisations. There are a variety of dangers and difficulties that have emerged with the increased use of the computing environment. One of the greatest difficulties to cloud computing environments is keeping consumer privacy, information leakage, and identification concerns under control [1]. As a result of the unique cloud computing infrastructure, old problems have been successfully combated, but new issues with infrastructure distribution have emerged. When it comes to cloud computing security, a major concern is that networking and security systems information, cloud architecture, and individual security requirements all vary. App layer carries out responses implementing the interprocess communication. These patterns resemble genuine responses, thus conventional defenses do not apply. Transaction and demand floods assaults, delayed performance assaults, and asymmetrical assaults may all be referred to as DDoS attacks

in the cloud. A flood of these assaults not only creates traffic but also imitates that of a genuine user [2]. This makes it difficult for the target to tell the difference between such a flood of attacks and legal traffic, and therefore, they need to provide services to the genuine user. A denial-of-service assault on a commodity causes it to become unavailable or service to legitimate customers to degrade.

A physical device, a collection of machines, or a system of computers may constitute a source. An attacker may place authorized customers in a state of denial if they can successfully deny the access of the specific part [3]. The means by which this assault is conducted out varies based on how far into the OSI and TCP/IP models it is carried out. The implementation of any type of denial-of-service attack has a variety of variables at play, including the assault instrument that is used to create bandwidth, the protocol being targeted, the communications layer, and the kind of victim. Assailant motivation is to reduce the amount of resources available to the legitimate customers to the minimum needed to deny them. Although many protections may be used to shield vital resources from being attacked in this manner, the flaws that are present in the systems are a fact of computing. An assault against computation's confidentiality, trustworthiness, and authenticity is underway. Threats such as unauthorized users, asset theft, and doing beyond the permitted limits are all often used by attackers for information security purposes [4]. The abovementioned problems may be addressed by the use of IDS, which identifies and evaluates whether internet traffic is regular or unusual in order to find a solution. The emergence of many different intrusion detection systems is attributed to network setup variability. There are distinct benefits and drawbacks to every kind of IDS. IDS are disseminated IDS because it use hypervisors to identify network hosts and disseminate the results. To investigate DDoS attacks in the cloud, machine learning is used to the NSL-KDD dataset [5]. The attributes chosen by both LVQ and PCA attribute selection approaches are essential for a successful implementation of mining algorithms. Attribute selection is a classification algorithm.

1.1. Review of Literature. Dwivedi et al. (2020) [1], using a machine learning technique, make a proposal for a new grasshopper optimization algorithm (GOA) with a machine learning algorithm (GOIDS). The plan of action is implemented based on the implementation of an intrusion detection system (IDS) in order to fulfill the monitoring needs and allow for the differentiation between a regular traffic flow and an attack. GOIDS is finding out the specific characteristics in the initial IDS dataset that are best suited to identify DDoS assaults of this low pace. Once the attributes have been chosen, they become inputs to classifiers. These machine learning models, namely, the SVM, DT, NB, and MLP, is utilized to identify the assault that occurred in the system. According to Prathyusha et al. (2020) [2], in this article, a novel DDoS detection method has been proposed by using artificial immune systems. This suggested approach can identify dangers and modulate the biological resistance mechanism to react accordingly. Wang et al. (2019) [3], in order to pick the best possible attributes during the training phase, offer a multilayer perceptions (MLP) coupled sequential attribute selection. Once it is determined that substantial identification mistakes have been made, the feedback mechanism is built to update the assault detectors to prevent future breaches. Rabbani et al. (2019) [4] proposed probabilistic-neural network (PSO-PNN) for developing a new attack detector. The first step is to organize the data such that it is easy to interpret. Then, the multilayer neural network was used to distinguish harmful activities. According to Punitha and Indumathi (2020) [5], entrusting our data security to a central cloud database, which uses an algorithm that generates the empire's own security keys, puts our data security at risk. The suggested system is also capable of detecting and monitoring how information is used. ICKGA and trapdoor creator are used to generate secret keys for every user, whereas CP-ABE and key creation use the ICKGA and trapdoor generator. Once the trapdoor generator has verified the integrity of the user data in the cloud as well as on the user level, the trapdoor generator kicks in. Using a dynamically weighted ensemble neural network (DWENN), a dynamic classifier that adjusts its sensitivity dynamically to identify DDoS attacks with more strength is finally used.

According to Wani et al. (2019) [7], in order to identify the DDoS assault in the cloud environment, they developed a novel detection technique using SVM. According to the plan, it is compared to NB and RF. According to Shitharth and Sangeetha (2020) [8], a number of distributed denial of service (DDoS) assaults has been identified using machine learning-based models. Attribute selection is utilized to come up with the optimum attributes. The characteristics chosen have been trained and evaluated using support vector machines (SVM), naive Bayes (NB), ANN, and KNN classifiers. Ghanbari et al. (2020) [9] presented a new DDoS attack detection system that was intended to increase the DDoS attack detection rate in a power system. The identification rate is increased utilizing CNNs which are trained and tested in stages known as the training and testing process. According to Shitharth et al. (2020) [11], a novel DDoS detection method that leverages machine learning-based classifiers is proposed in a cloud environment. As input to the classifier, people have gathered and categorized characteristics that they believe to be helpful. Kishirsagar et.al [6, 10] elaborate the use of different algorithms for classification and prediction of benchmark datasets and real time dataset which were useful in the emerging all fields and elaborate the use of hybrid artificial intelligence along with optimization techniques for classification and prediction of various datasets with high accuracy [12]. The algorithms used in various research worked were useful in cyber security, mobile computing, and cloud computing for more accurate results with different evaluation parameters.

Deepa et al. [13] have devised an ensemble approach to combat DDoS assaults. They used four distinct machine learning algorithms in the SDN environment to identify suspicious network traffic. SVM-SOM method obtained superior results, with 98.12% accuracy, than the other ML algorithms. A DDoS attack-detection system for SDN was presented by the authors. Two separate security steps were used. Signature-based attacks were detected by Snort, which

is a tool designed to spot them. Using the SVM classifier and the DNN machine learning method, they launched an attack classification scheme thereafter.

Mašetić et al. and Rao et al. [14, 15] and developed an automated DoS attack categorization method for cloud computing. This research is conducted in stages, such as conducting an assault simulation, collecting information, and choosing attributes, before applying categorization to the results. For this research, data is acquired via mimicking the cloud environment and DoS assault, together with Wireshark's Tshark capability. One of the categorization models for DoS attacks and standard network activity is the support vector machine (SVM).

1.2. Research Gap and Motivation. In addition to different methods that are provided in earlier sections, some recent articles also focused on detecting DoS attacks using different data set where [18] used CAIDA for experimental verification cases. However, if CAIDA is used, large data set cannot be stored in the system thus high case external attacks is not prevented. In [19–23], data detection in industrial applications is analysed as data in entire segment inside the industry must be protected in reaching external users. Thus, the protection is provided using machine learning algorithm with two directional data flow procedures. Even though bidirectional flow is provided, the amount of data traffic in the system can be handled with single traffic flow itself, thus preventing less amount of users. There is clearly a need of a strategic plan to use machine learning methods in a methodical manner in order to make comprehensive evaluations possible, as otherwise built-in issues like collinearity, multicollinearity, and duplication would present in machine-mined data. Additionally, the use of machine learning methods in data science-driven ways requires integrating all of the key needs of data science-driven approaches. A modeling may not fulfill its goal, but if that is the case, the model will always incorporate aspects of classifier. Integrating machine learning and attribute engineering techniques in a single framework also has a significant impact on the current research. In other words, all inclusive experimentation and trustworthy results need joint consideration.

1.3. Proposed Methodology. Many existing methods [1–15] emphases only on basic attacks where data is processed with low security features. Even many methods does not incorporate learning techniques for avoiding attacks from external users. It is always necessary that a user must acquire knowledge from existing data and unnecessary data must be eliminated using attribute engineering procedures. The abovementioned technique is carried out in case of intrusion prevention systems where different machine learning techniques can be allocated. To overcome the gap that is present in existing methods, proposed method is incorporated by reducing dimensionality of entire data handling systems.

The proposed methodology is used for preventing denial of service attack using a quantization model which eliminates all attacks using step processing procedures. By incorporating the proposed method, unidentified attributes are directly removed from the system, thus making all data to revolve in a hassle free environment. Moreover, the losses that are present in this type of system are reduced even if the data is stored in the cloud. Furthermore, volume of information in presence of large data set is prevented using machine learning algorithm where ten initial attributes are completely knowledgeable; thus, it is used as reference data for preventing external attacks in the system.

1.4. Objectives. The major objective of proposed work focuses on deciphering three objectives which is considered as minimization problem as follows:

(i) To minimize the denial of service attack on data that is included within the systems and to provide potential defence for large data set

(ii) To incorporate machine learning algorithms by rationalization process without describing any dimensions for entire data set

(iii) To categorize and allocate resources based on target customers, thus increasing the security of data that is provided to all users

2. Distributed DoS

The malicious distributed-denial-of-service (DDoS) assaults that plague the internet these days are a major worldwide threat. These assaults are deftly executed and use the same methods of conventional denial of service (DoS) attacks, but they are implemented on a larger scale due to the usage of botnets. In order to spread quickly, a botnet may spread by taking use of malware that infects tens or even hundreds of computers which are then used to further spread the malware by being managed by an attacker that is targeting a victim [16]. Attacks on the internet provide an exciting potential for attackers to take control of users computers and generate zombies. By infecting people through worms, Trojan horses, or backdoors, the zombies use the tricks of their trade: compelling links, e-mail content, or trustworthy sender addresses. Computers linked to the Internet, such as Web servers, have vulnerabilities and flaws that may be exploited by attackers using a range of different hacker methods. This leads to malicious malware being placed on these systems, and subsequently to these computers being placed in a vulnerable position, giving malevolent programmes full control over them. These machines are often known as "handlers" and "zombies." The attackers, under control of the controllers, have the command of the zombie army.

When an attack is first begun, the assailant controls as many computer systems as possible, enabling him to initiate the assault. An estimate for the number of zombies may be anything from a few hundred to a few thousand. In the figure below, Figure 1, you can see how a botnet of zombie-related attacks develops [17]. The size of the botnet impacts the amount of damage, the intensity, and the range of an attack. A botnet that may inflict debilitating and catastrophic attacks is a serious threat. For

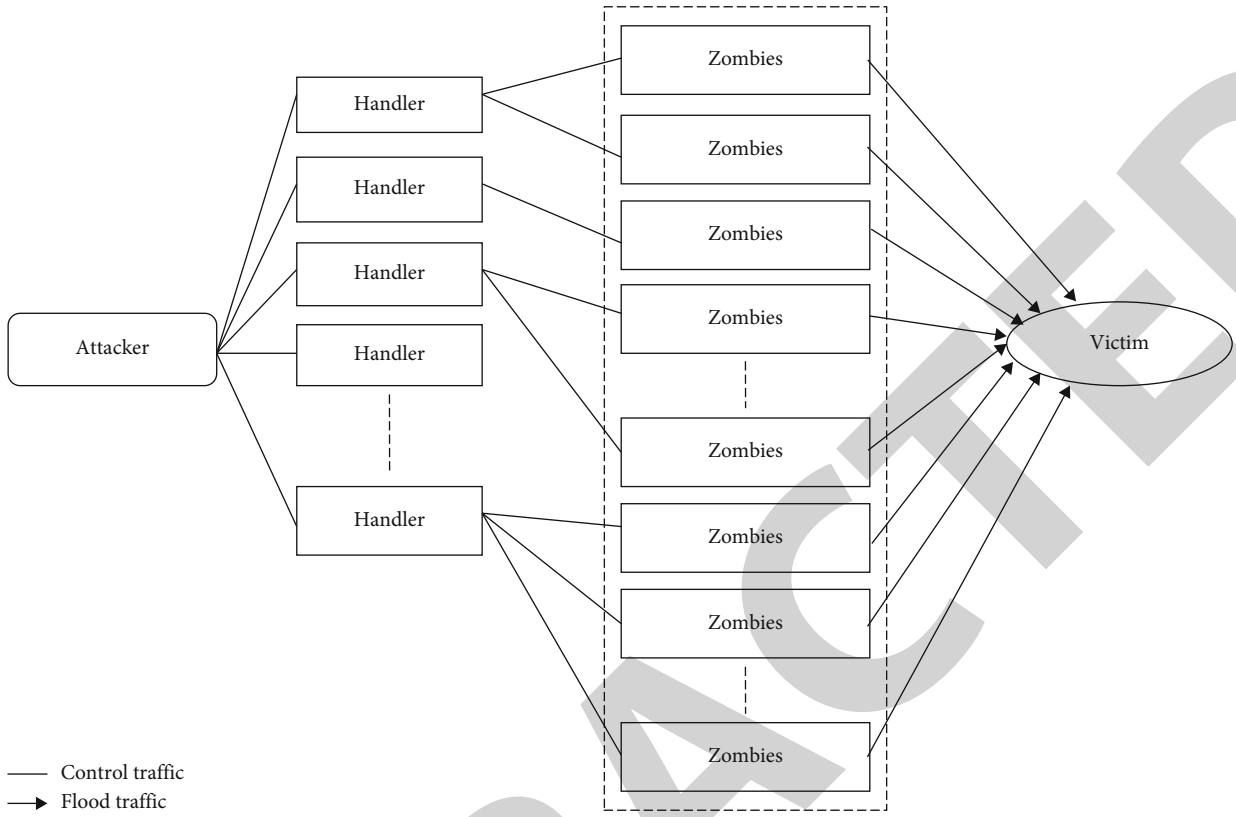


Figure 1: DDoS attack architecture.

example, just a little amount of information is given by one zombie. In contrast, on user devices, meanwhile, the huge amount of zombies that have risen depletes computer resources. When single connection speed traffic looks as normal, traffic floods using low packet rates that are part of a DDoS attack are especially difficult to detect. Attacks that inflict extreme damage may happen due to existing detection methods tending to increase the speed of DDoS attacks. At the present, DDoS assaults are done through link and packet flooding. This kind of attack has increased drastically on the Internet because hackers know where and how data is obtained [17]. This kind of assault may be carried out because weaknesses in the protocols, operating systems, and web applications constantly surface. In such attacks, the most common motives include money gain, blackmail, hacking, or personal problems. This usually happens when web-based media, such as internet poker, social media sites, or internet shopping, are attacked.

2.1. Detection Approach for DDoS Attack. ML techniques that include attribute engineering and data science procedures such as attribute extraction and information science best practices may be used to get the most optimal detection in a DDoS dataset. A conceptual plan, one that involves treatments of attributes in addition to machine learning advances, is presented in this study. In Figure 2, the fact that performance of the model may occur is emphasized. According to the nature and structure of data, characteristics are always systematically treated. Extending this concept, any kind of cyber-intrusion such as a distributed denial of service (DDoS) assault may also be included in the suggested method to deal with all the inherent problems of data, including skewness, collinearity, and multicollinearity. Completing the attribute engineering process will also include attention to the missing values. This may be done by averaging, using the maximum and minimum values, or by replacing the missing data with the lowest, maximum, or average values. Attribute unusability is caused by high value for missing data vs. supplied values. Based on the proportion of missing values in the dataset, one may determine that the appropriate treatment should be done in an attribute elimination or attribute adjustment phase of the attribute engineering module. A collection of datasets are provided with a reduced range of attributes, enabling machine learning techniques to be used to analyse those attributes after the attribute selection stage is completed inside the new framework attribute engineering module.

These machine learning techniques may be seen in the research findings in Figure 2. The machine learning module of the proposed framework does not contain the full collection of algorithms (including AdaBoost and CART), but it is not limited to just those five algorithms. Regardless of whether it is supervised, unsupervised, or semisupervised, the machine learning algorithms may be used to any kind of study. The target classes are made available to supervised algorithms because of the nature of the supplied datasets.

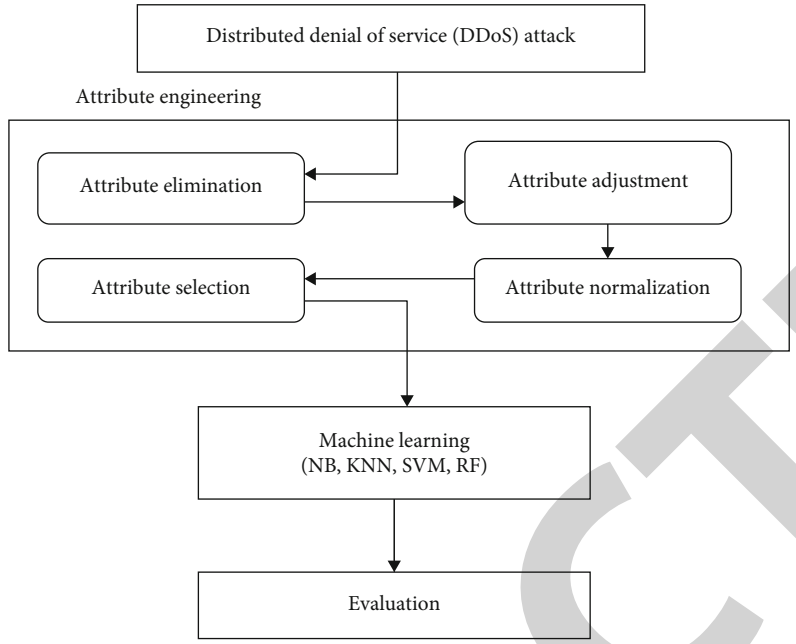


Figure 2: Strategic level framework for DDoS attack detection.

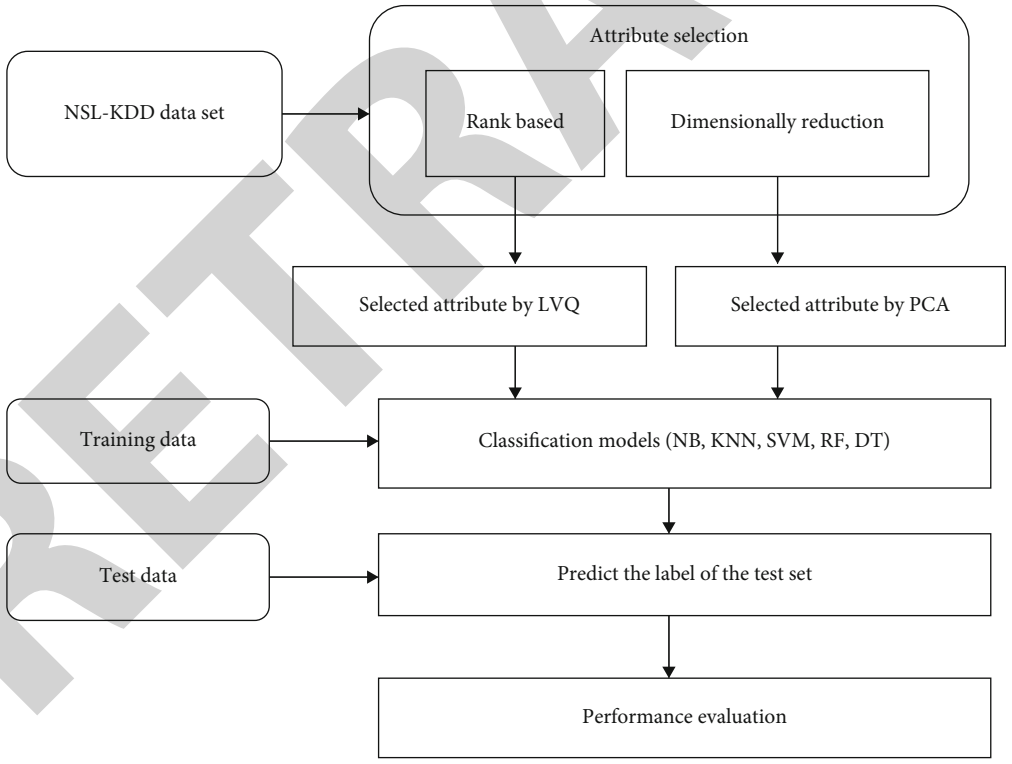


Figure 3: IDS in cloud environment.

3. Data Set Description and Attributes

In a dispersed test environment, wired network is extremely costly. Modeling is a widely-used technique in network research. It is useful for studying network issues that vary depending on protocols, traffic, and topologies, as well as evaluating network protocol tests [14]. The sets of data that are accessible are those that are built from the ground up, like a direct data set, and those that have been obtained from public sources, like a public data set. When open source

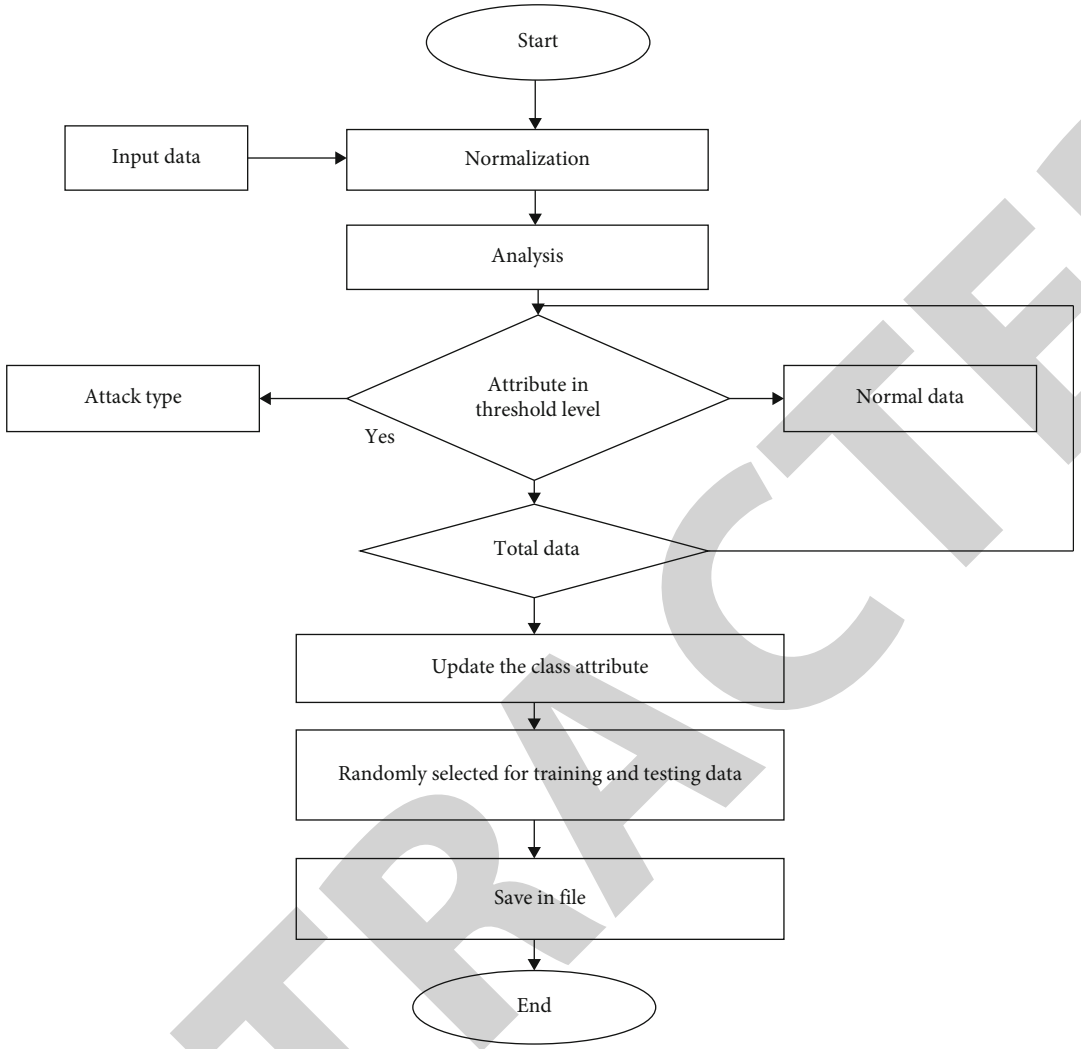


Figure 4: Flowchart of SVM algorithm for attack detection.

Table 1: Results of LVQ method.

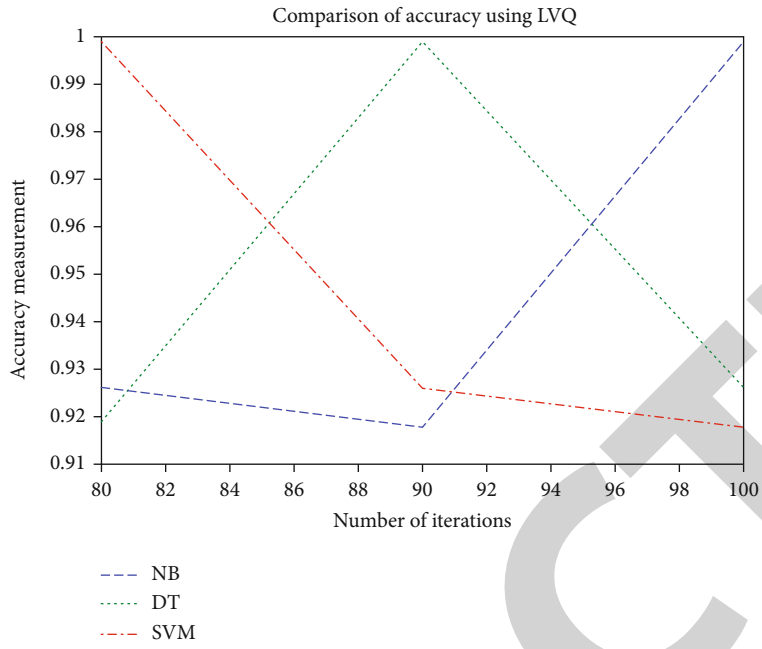
Parameters	NB	DT	SVM
Accuracy	0.9286	0.9176	0.9985
Recall	0.9176	0.9142	0.9768
Precision	0.9814	0.9886	0.9928
F-measure	0.9486	0.9571	0.9940

software is used to generate a direct dataset, the resulting dataset is termed direct data set. If the dataset is made available to the public, it is called public data set. This study makes use of a public dataset, NSL-KDD, which is deliberated in Figure 3.

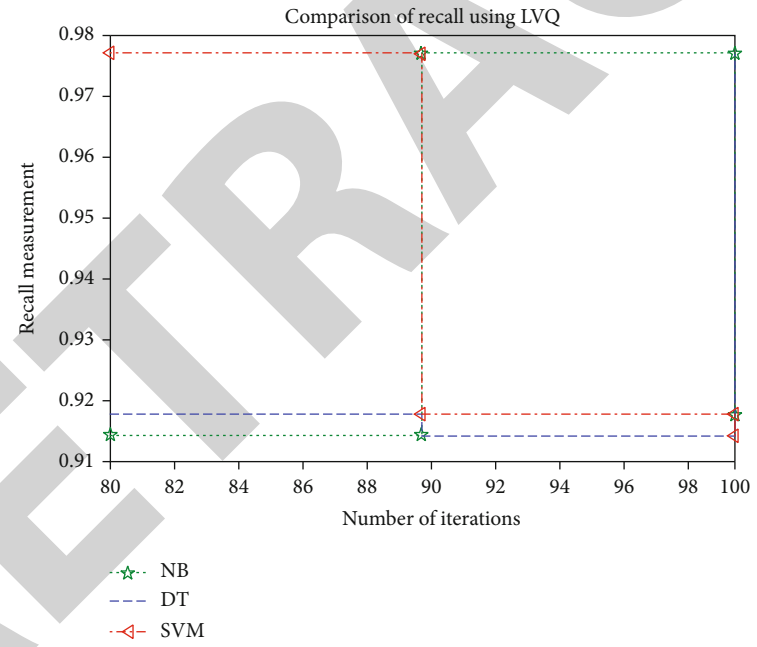
Attribute selection method is a strategy that uses several parameters, selecting the ones that are the most significant and have the greatest effect on the anticipated variable. The data used in attribute selection is not the whole data set, with regard to attribute selections, the addition and deletion of information have no effect on the entire collection. Attribute selection is done out in the proposed study using two different approaches. They are a technique of filtering and a means of reducing complexity.

3.1. Classification Technique. SVM is being used successfully for multiple-class classification, but researchers are still trying to figure out how to expand it. The two predominant kinds of multiclass SVM methods at this time are hypothesis-based and algorithm-based. The first method uses several binary classifiers to construct the overall classifier, whereas the second method directly incorporates all training examples to derive the classifier. By choosing examples at the edges of the class descriptors, the SVM may choose the optimal separating hyper plane for training inside the attribute space. The SVM model that we create has the number of classes equal to k. All of the positive instances are used in training an SVM with classifier set I, and all other examples are used in training an SVM with classifier set II.

Thus, given l training data $(x_1, y_1), (x_2, y_2), \cdots (x_l, y_l)$, $i = 1,2,3, \cdots l$ where $x_i \in R^l$ and $y_i \in \{1, 2, \cdots k\}$ are the

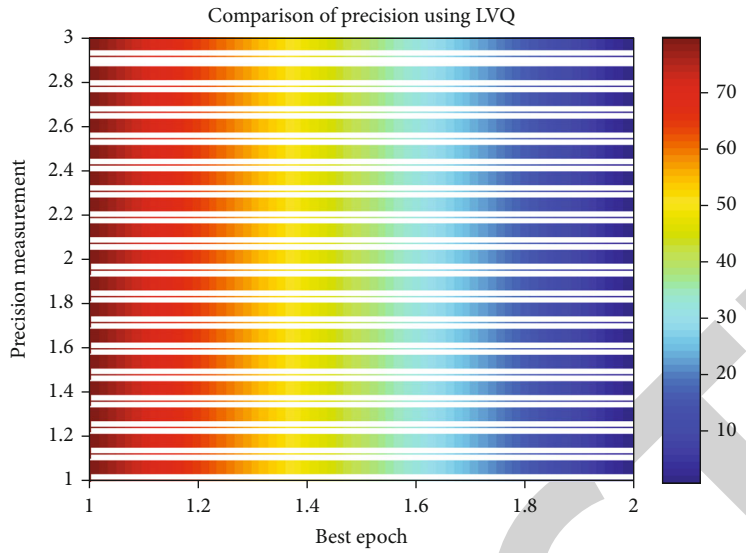


(a)

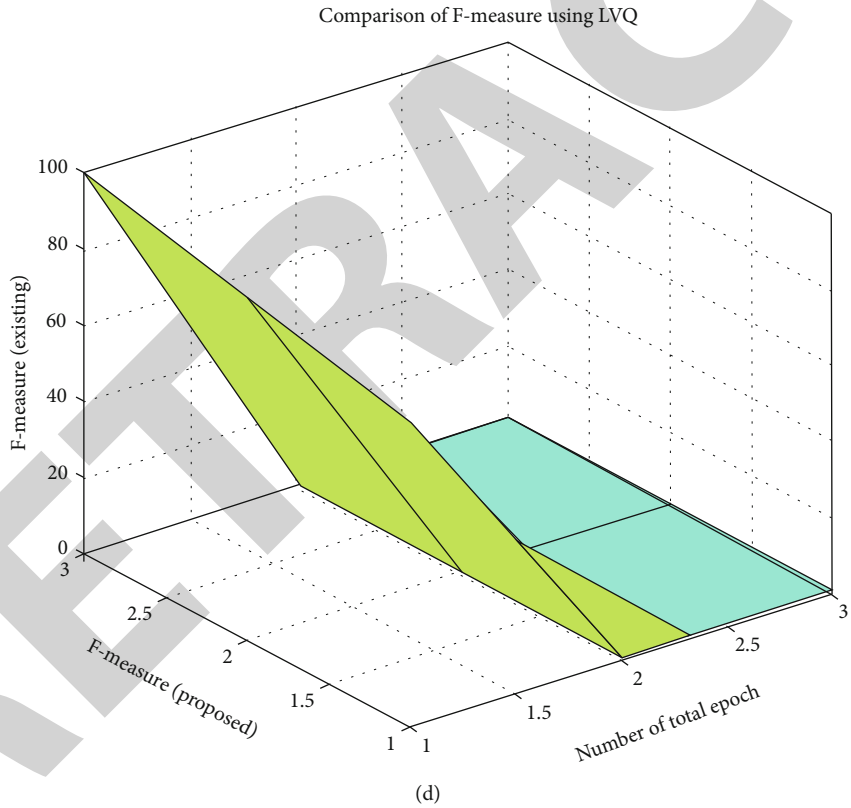


(b)

Figure 5: Continued.



(c)



(d)

Figure 5: Results of LVQ method. (a) Accuracy. (b) Recall. (c) Precision. (d) *F*-measure.

class of x_j the j^{th} SVM solves the following optimization problem

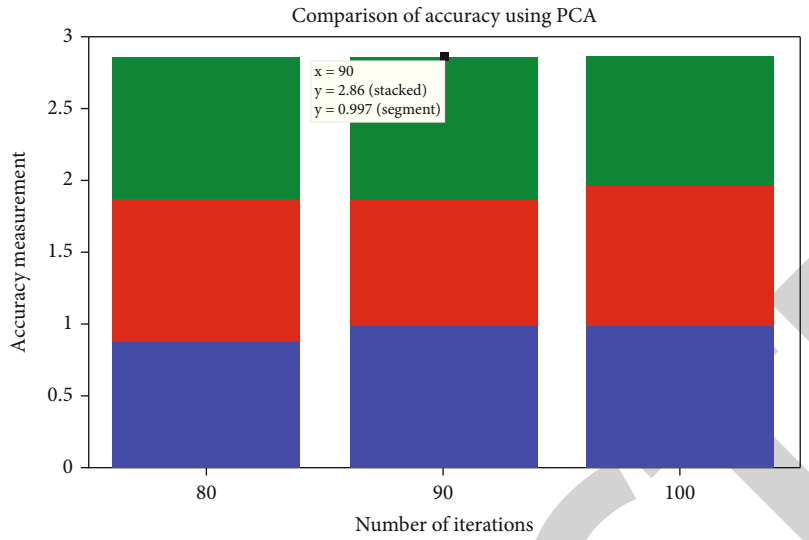
$$\min_{w^j b^j \xi_i^j} \left\{ \frac{1}{2} \left(w^j\right)^T w^j + c\left(\sum_{i=1}^{l} \xi_i^j\right) \right\}, \tag{1}$$

$$\left(w^j\right)^T \varnothing(x_i) + b^j \geq 1 - \xi_i^j \quad \text{if } y_i = j, \tag{2}$$

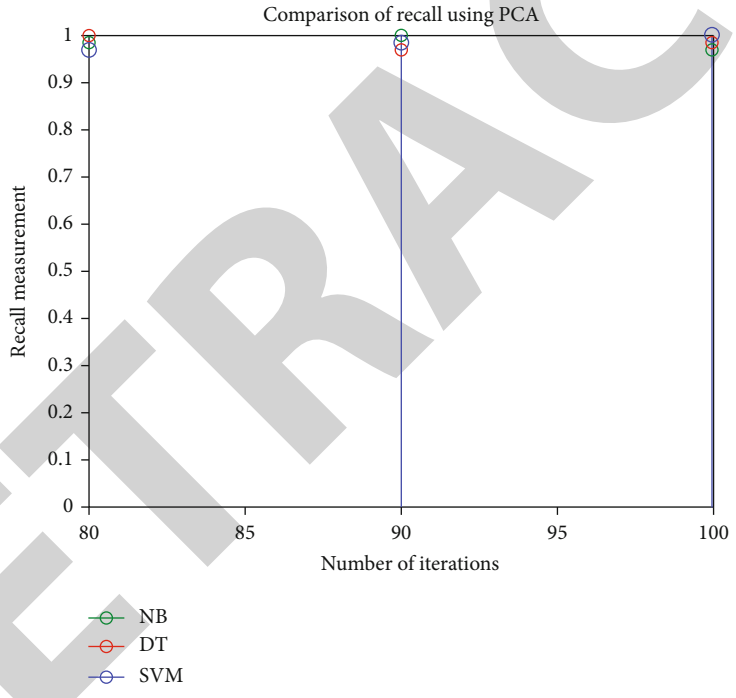
$$\left(w^j\right)^T \varnothing(x_i) + b^j \leq -1 + \xi_i^j \quad \text{if} \quad y_i \neq j, \tag{3}$$

$$\xi_i^j \geq 0, i = 1, \cdots .l. \tag{4}$$

Since the nonlinear function, w, b, and ξ have weight, bias, and slack variables, respectively, then $\varnothing(x_i)$ may be mapped into a higher dimensional space by the function. There is a constant, established a priori, which is C. Quadratic programming issue (shown as equation (1) in the



(a)



(b)

Figure 6: Continued.

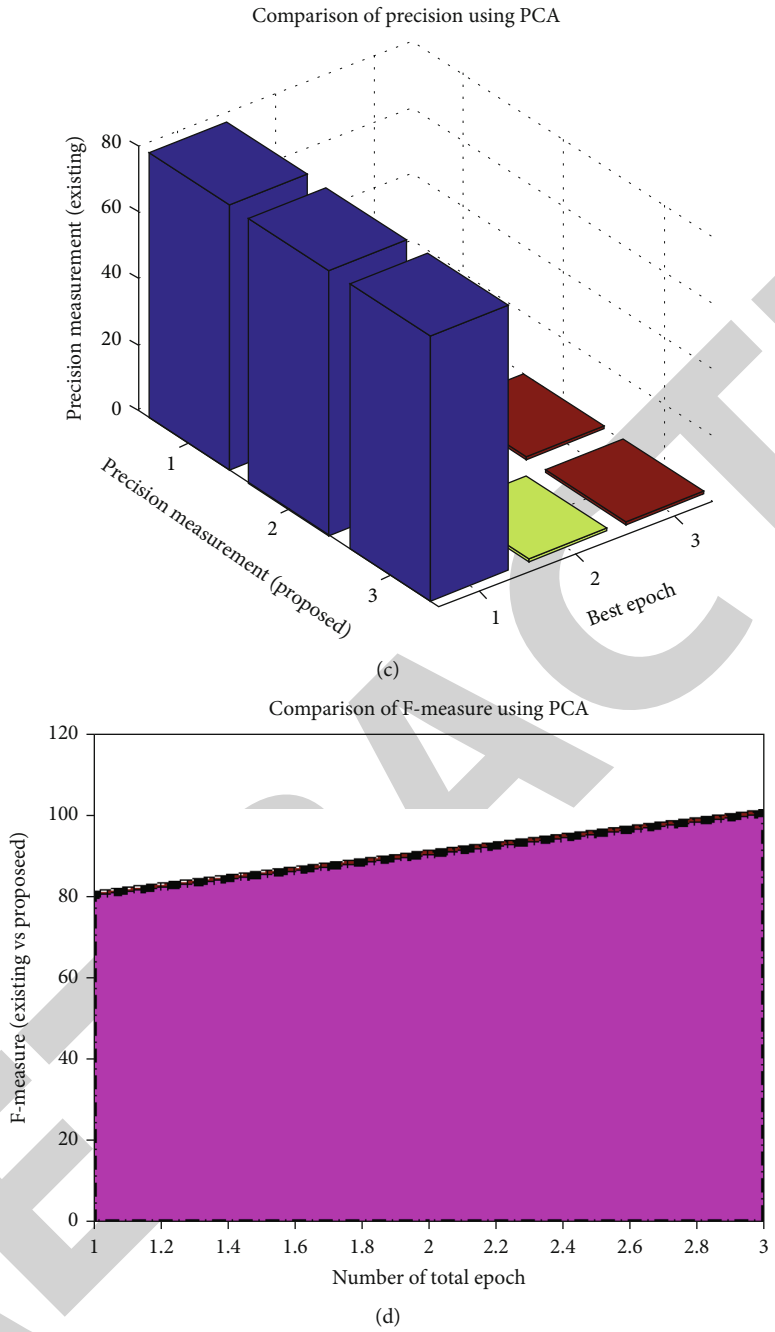


Figure 6: Results of PCA method. (a) Accuracy. (b) Recall. (c) Precision. (d) *F*-measure.

Table 2: PCA method results.

Parameters	NB	DT	SVM
Accuracy	0.8832	0.9758	0.9971
Recall	0.9673	0.9815	0.9975
Precision	0.8672	0.9753	0.9892
F-M	0.9143	0.9786	0.9975

Table 3: Comparable results of LVQ and PCA.

Classification algorithms	Detection accuracy	
	LVQ	PCA
NB	0.9289	0.8832
DT	0.9397	0.9756
SVM	0.9985	0.9951

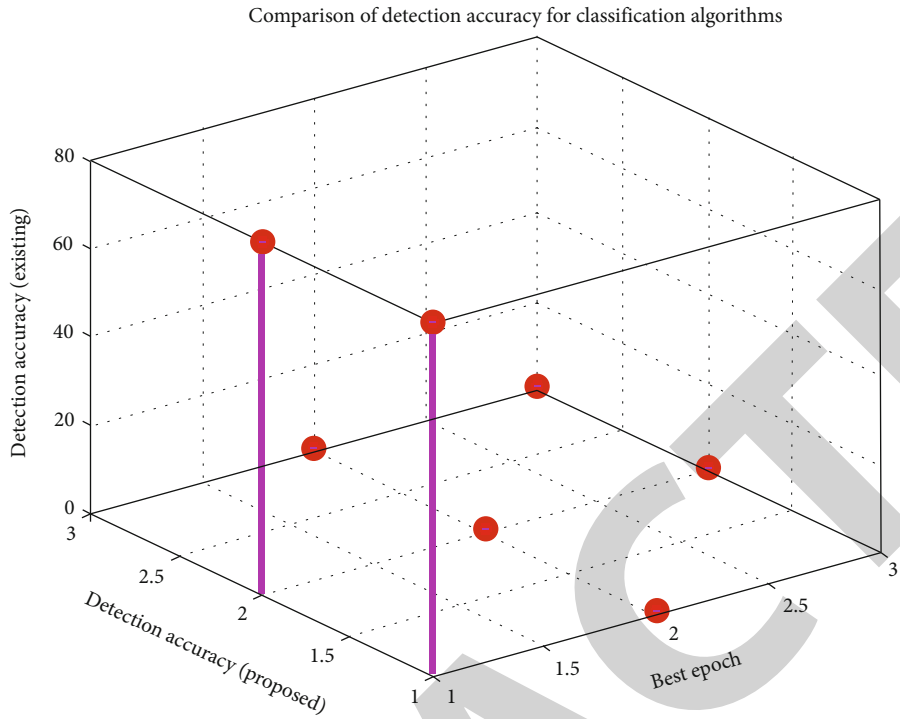


Figure 7: Comparative results of LVQ and PCA.

graphic below) involves searching for the best hyperplane in equation (1). Minimizing $1/2(w^j)^T w^j$, therefore, researchers want to increase $2/\|w^j\|$ the difference between assault categories. Data do not exist in a linear format, therefore, there is a cost. $c = (\sum_{i=1}^{l} \xi_i^j)$. SVM tries to find a compromise between the regularization term and training mistakes $1/2$ $(w^j)^T w^j$ corrections and training mistakes. Once you have determined k decision functions from equation (1), you are finished solving for k.

$$\sum_{i=1}^{l} \alpha_i^j K(x, x_i) + b^1, \tag{5}$$

$$\sum_{i=1}^{l} \alpha_i^j K(x, x_i) + b^k. \tag{6}$$

We state that the value of the choice function for class x_i is in the class with the greatest value:

$$\text{class of } x = \text{argmax}_{i=1\cdots k} \sum_{i=1}^{l} \alpha_i^j K(x_l, x_i) + b^j. \tag{7}$$

In this section, we will be using the Gaussian kernel $K(x, x_i)$ and the Lagrange multiplier. We will change the Gaussian kernel function $K(x, x_i)$ in a data-dependent manner to enhance SVM classifier classification accuracy. In SVM, the four common functions are linear, polynomial of degree d, RBF, and MLP. A flowchart depicting the algorithm's steps is given in Figure 4. The procedure of a simulation method that uses support vector machines is shown using this flowchart. The origins from both equations (1) and (7) are provided in such a way it is integrated in a single equation for defining the objective functions as follows,

$$O_i = \min \sum_{i=1}^{n} \text{DoS}_i, A_i, \tag{8}$$

where DoS_i indicates various attack process. A_i describes different attribute in a system.

4. Outcomes

Attribute selection techniques are employed, and the attribute set that results from this is used for classification. Verification measurements are computed by using these theoretical method, which relate to accuracy, precision, recall, and f-measure.

4.1. Assessment of Characteristics: LVQ Process. These results in Table 1 and Figure 5 have been obtained from experiments that follow the research set of data. Applications of different classifiers like NB, SVM, and DT are made possible with the deployment of LVQ. With respect to malicious records, the SVM classifier has a higher performance level as compared to NB and DT.

4.2. PCA Strategy: Explore Various Qualities. PCA is used for dimensionality reduction. Figure 6 shows the findings. SVM method from Table 2 does better than NB and DT when it comes to detection accuracy (0.9971 vs. 0.9965). When using

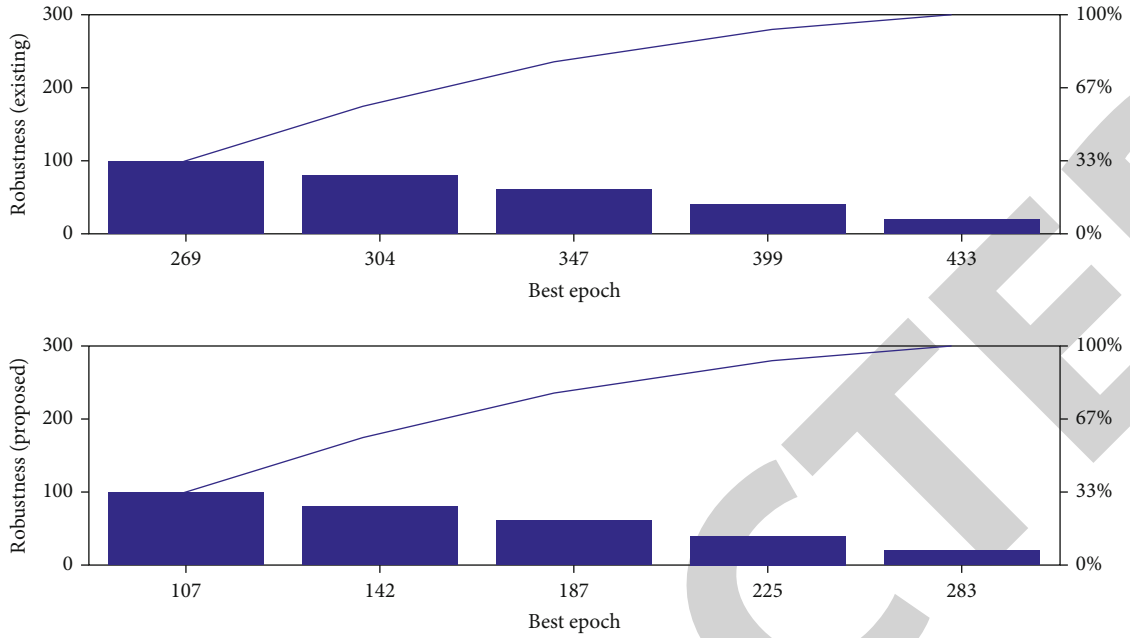


Figure 8: Comparison of robustness characteristics.

the attribute selection technique in this attribute-based selection process, 10 out of 21 attributes are used.

4.3. Comparative Results. Attribute selection techniques, such as SVM, were used to classifier performance, and the findings are summarized in Table 3. Table 3 and Figure 7 indicate that SVM performs better for both attribute selection methods. Classifying harmful records is best performed using an SVM-based approach.

4.4. Robustness Characteristics. In this comparative outcome section, the robustness characteristics with respect to LVQ and PCA are observed for different iteration periods, and their changes are simulated. Since more amount of data set is present in this process for preventing DoS, it is essential to find individual robustness for attributes. Further, the robustness of an algorithm determines the association between two distinct data set, thus solving the necessary properties for defining the learning rate. Figure 8 illustrates the simulation outcomes and comparison of robustness that is present in both LVQ and PCA.

From Figure 8, it is pragmatic that robustness of LVQ is much reduced as compared to PCA due to dimensionless characteristics. To validate the robustness of LVQ and PCA five best epoch is considered but original ranges are chosen from 10 to 100. Due to presence of vector quantization, the step size is chosen as 20, thus, the following best epoch such as 20, 40, 60, 80, and 100 is considered. During the abovementioned variations, it is much clear that robustness of LVQ reduces from 283 to 107 and further reduces for remaining periods. On the other hand, even though PCA reduces the amount of robustness, it is much higher for all epoch periods as dimension process for data is defined in existing method.

5. Conclusions

This page attempts to give a basic overview of the different DDoS attack methods in use, while also offering an in-depth look at potential defenses. An essential part in the overall data protection process is played by intrusion prevention. A benchmarking set of NSL-KDD standards is used to identify intruders for internet information. The study only uses information that pertain to DDoS attacks. Attributes such as LVQ and PCA were utilized to categories the attacks based on machine learning approaches such as SVM, NB, and DT. To verify whether the DDoS attack was occurring, the algorithms' performance was monitored. Ten attributes were selected using LVQ, and the remaining ten attributes were selected using PCA. Using an LVQ-based attribute selection in an SVM model was shown to be more successful in identifying attacks. When compared to other algorithms, it comes out to be more accuracy, has greater recall, is more precise, and has a higher *F*-score.

5.1. Policy Implications

(i) The proposed DoS model can be incorporated in all industries even with large amount of data set where new security features are enabled

(ii) By using the enhanced security features, more amount of data overflow can be prevented and even worst type of attacks can be prevented using loop formatting procedures

(iii) All the target systems can process different type of packets inside a particular device where less resources are allocated in productions

Data Availability

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work has been done remotely at DAAI Lab, Thu Dau Mot University, Vietnam, and i3 LABs, Techno India NJR Institute of Technology, India.

References

[1] S. Dwivedi, M. Vardhan, and S. Tripathi, "Defense against distributed DoS attack detection by using intelligent evolutionary algorithm," *International Journal of Computers and Applications*, vol. 44, no. 3, pp. 219–229, 2022.

[2] D. J. Prathyusha and G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment," *Evolutionary Intelligence*, vol. 14, no. 2, pp. 607–618, 2021.

[3] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Computers & Security*, vol. 88, article 101645, 2020.

[4] M. Rabbani, Y. L. Wang, R. Khoshkangini, H. Jelodar, R. Zhao, and P. Hu, "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing," *Journal of Network and Computer Applications*, vol. 151, article 102507, 2020.

[5] A. A. A. Punitha and G. Indumathi, "RETRACTED ARTICLE: A novel centralized cloud information accountability integrity with ensemble neural network based attack detection approach for cloud data," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 4889–4900, 2021.

[6] P. Kshirsagar, N. Balakrishnan, and A. D. Yadav, "Modelling of optimised neural network for classification and prediction of benchmark datasets," *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, vol. 8, no. 4, pp. 426–435, 2020.

[7] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019.

[8] S. Shitharth and K. Sangeetha, "Enhanced SCADA IDS security by using MSOM hybrid unsupervised algorithm," *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)*, vol. 17, no. 3, 2021.

[9] M. Ghanbari and W. Kinsner, "Detecting DDoS attacks using polyscale analysis and deep learning," *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI)*, vol. 14, no. 1, pp. 17–34, 2020.

[10] P. Kshirsagar and S. Akojwar, "Optimization of BPNN parameters using PSO for EEG signals," in *ICCASP/ICMMD-2016. Advances in Intelligent Systems Research*, vol. 137, pp. 385–394, 2016.

[11] S. Shitharth, N. Satheesh, B. Praveen Kumar, and K. Sangeetha, "IDS detection based on optimization based on WI-CS and GNN algorithm in SCADA network," in *Architectural Wireless Networks Solutions and Security Issues*, vol. 196, no. 1pp. 247–266, Springer, 2021.

[12] S. Shitharth, K. M. Prasad, K. Sangeetha, P. R. Kshirsagar, T. S. Babu, and H. H. Alhelou, "An enriched RPCO-BCNN mechanisms for attack detection and classification in SCADA systems," *IEEE Access*, vol. 9, pp. 156297–156312, 2021.

[13] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Design of ensemble learning methods for DDoS detection in SDN environment," in *Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, pp. 30-31, Vellore, India, 2019.

[14] Z. Mašetić, D. Kečo, N. Doğru, and K. Hajdarević, "SYN flood attack detection in cloud computing using support vector machine," *TEM Journal*, vol. 6, no. 4, 2017.

[15] N. S. Rao, K. C. Sekharaiah, and A. A. Rao, "A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains," *Innovations in Computer Science and Engineering*, vol. 32, pp. 221–230, 2019.

[16] G. Bhageerath Chakravorthy, R. Aditya Vardhan, K. Karthik Shetty, K. Mahesh, and S. Shitharth, "Handling tactful data in cloud using Pkg encryption technique," in *4th Smart Cities Symposium (SCS 2021)*, pp. 338–343, 2021.

[17] R. Aluvalu, V. U. Maheswari, K. K. Chennam, and S. Shitharth, "Data security in cloud computing using Abe-based access control," in *Architectural Wireless Networks Solutions and Security Issues*, vol. 196, no. 1pp. 47–62, Lecture notes in network and systems, Springer, 2021.

[18] K. K. Chennam, R. Aluvalu, and S. Shitharth, "An authentication model with high security for cloud database," in *Architectural Wireless Networks Solutions and Security Issues*, vol. 196, no. 1pp. 13–26, Lecture notes in network and systems, Springer, 2021.

[19] A. Bandi, L. Sherpa, and S. M. Allu, "Machine learning algorithms for DDoS attack detection in cybersecurity," *Studies in Computational Intelligence*, vol. 1027, pp. 269–281, 2022.

[20] F. Musumeci, A. C. Fidanci, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-learning-enabled DDoS attacks detection in P4 programmable networks," *Journal of Network and Systems Management*, vol. 30, no. 1, 2022.

[21] M. Liyanage, Q. V. Pham, K. Dev et al., "A survey on zero touch network and service management (ZSM) for 5G and beyond networks," *Journal of Network and Computer Applications*, vol. 203, article 103362, 2022.

[22] T. Shakeel, S. Habib, W. Boulila et al., "A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects," in *Complex & Intelligent Systems*, pp. 1–32, Springer International Publishing, 2022.

[23] G. Srivastava, R. H. Jhaveri, S. Bhattacharya et al., "XAI for cybersecurity: state of the art, challenges, open issues and future directions," vol. 1, no. 1, pp. 1–33, 2022, http://arxiv.org/abs/2206.03585.