International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

Improved Framework for Detecting and Predicting Various Cyber Attacks Using the NSL-KDD Dataset

Swati P. Gawand[1], Dr. Sudhir Kumar Meesala[2]

[1]Research Scholar, Department of Computer Science and Engineering, Sandip University, Nashik, Maharashtra. India.

[2]Professor, Department of Computer Science and Engineering, Sandip University, Nashik, Maharashtra. India.

Emails: *swatigawand@gmail.com[1], Sudhir.meesala@sandipuniversity.edu.in[2]*

Abstract

The cybersecurity environment continues to change rapidly, with continuous growth in the number and level of sophistication of cyberattacks. The attacks become increasingly sophisticated and pervasive, thereby emphasizing the imperative for new-age defense mechanisms. The increasing necessity for effective cybersecurity solutions is due to the evolution of numerous threats such as unauthorized access, DoS attacks, botnets, malware, and worms. These threats have resulted in large-scale computer network damage, creating heavy financial losses. Protection from security attacks is now a crucial issue for traditional cyber systems and the Internet of Things (IoT) framework. This work emphasizes the NSL-KDD dataset analysis and examines the application of different machine learning algorithms in the detection and classification of network intrusions. The NSL-KDD dataset consists of four major categories of cyberattacks: DoS, Probe, User to Root (U2R), and Remote to Local (R2L). For the purpose of implementation, the dataset was obtained from Kaggle. A number of machine learning algorithms like Logistic Regression, Gaussian Naive Bayes, Support Vector Machines (SVM), Decision Trees, Random Forest, and K-Nearest Neighbors (KNN) were used to detect and classify these cyberattacks. Comparison based on the performance measures was performed among these algorithms using cross-validation score, recall, F1-score, precision, and accuracy. Comparison from this assessment provides evidence for the algorithm with the best accuracy and reliability of results in intrusion network detection.

Keywords: *Cyber Attacks; Denial of Service attack (DoS); Wannacry attack; DoS attack, Machine Learning Algorithms.*

1. Introduction

As the frequency and sophistication of cyber-attacks in every industry grow, network security has become a significant area of research that has drawn global attention. Cyber attackers use diverse methods to exploit user defenses, intercepting sensitive information and taking malicious actions such as eavesdropping [1]. Conventional security measures like firewalls and antivirus software are, however, of no use in the context of advanced attacks like zero-day attacks, DoS attacks, and large-scale data breaches. Thus, cybercrime keeps increasing with encouragement from system vulnerabilities, weak security mechanisms, and a general lack of awareness about evolving cyber threats [2]. Incidentally, there were more than three billion zero-day attacks that took place in 2021 alone, proving the paramount need for strong and efficient security procedures[3]. The subject of this work is the NSL-KDD dataset, which is a cleaned version of the commonly used KDD Cup 99 dataset, used as a benchmark to measure intrusion detection systems (IDS). The NSL-KDD dataset is designed to overcome some of the disadvantages of its predecessor, including the inclusion of duplicate records and the absence of modern network traffic features. The dataset provides an exhaustive set of features extracted from network traffic that includes a variety of attack kinds and normal processes. Features encapsulate the likes of protocol, service,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

connection flags, and counts of packets and bytes transferred. In this research work, here we apply various machine learning techniques to the NSL-KDD data set for identification and classification of cyberattacks and forecasting the probable future attack. Machine learning is an ongoing process of detection and prevention of cyber threats by training systems to learn and identify malicious patterns in databases of security events. Through the predictive models, such algorithms provide real-time surveillance, identification, and response to threats. The rest of this paper is organized as: Section II contains the literature review. Section III outlines the proposed methodology. Section IV provides the results analysis, and Section V concludes the research with recommendations for future research work.

2. Related Work

The assessment is done with different machine learning algorithms by comparative testing of system performance. Algorithmic performance is determined in terms of prime measures such as cross-validation score, recall, F1-score, precision, and accuracy [1]. The common application of machine learning processes is used in an attempt to train the system to identify and detect cyberattacks. Automatic alarm notification would then be through email towards forwarding data to security teams or end-users upon detection of attacks [4]. Classification models can be used to categorize different types of attacks, including determining if an attack is DoS/DDoS. One of the well-known classification models is Support Vector Machine (SVM), a supervised machine learning method that analyses data for patterns. Low human intervention systems are typically optimal for such uses. Some of the most popular machine learning classification techniques include Logistic Regression, K-Nearest Neighbours (KNN), Support Vector Machine (SVM), Naive Bayes, Decision Tree, and Random Forest. Due to the availability of large annotated datasets, deep learning models such as Restricted Boltzmann Machines (RBM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) have been highly successful for complex classification tasks. Deep learning models prefer to incorporate feature extraction along with dense neural networks for increasing prediction correctness provided that sufficient labelled data is available [1]. Mona Alduaili et al. [3] proposed a cloud-based approach to detecting DDoS attacks for the aim of reducing misclassification errors in detection. The work applies feature selection techniques like Mutual Information (MI) and Random Forest Feature Importance (RFFI) for the selection of most important features. Using selected variables, algorithms such as Random Forest (RF), Gradient Boosting (GB), Weighted Voting Ensemble (WVE), K-Nearest Neighbor (KNN), and Logistic Regression (LR) were used with a 0.99 accuracy score when validated using 19 features. Preprocessing of data is carried out to remove missing values and outliers in the Cyber Attack Detection Model (CADM) using a machine learning approach [5]. The feature extraction algorithms are then used to draw out the most informative features and then ensemble-based classification. The ensemble methods are used to increase the accuracy of classification by using multiple models together to make more reliable decisions. CADM utilizes DBSCAN for addressing multi-dimensional data and LASSO to reduce dimensions, ultimately selecting the best performing network features for the classification of attacks. Predicting future cyberattacks is another prominent area of research. Developing defensive strength in cyberspace is crucial to protecting sensitive information and critical infrastructure. Analysis of past cyber incidents and prediction of future threats helps in the development of security profiles and pre-emptive defense strategies, minimizing attackers' first-mover advantage [7]. Machine learning plays a crucial role in the improvement of intrusion detection systems, using both supervised and unsupervised learning methods. Supervised machine learning algorithms work on labelled data, learning to differentiate between pre-defined labels. In contrast, unsupervised learning algorithms work on unlabelled data to identify patterns and groupings independently. Since labelled data can be limited and difficult to obtain, in certain situations supervised methods become impractical. Trained machine learning models on large data-set can help in anomaly detection, preventing data leaks, and improving

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

intrusion and malware detection systems [8]. In another study in crime prediction [36], city time-series data from San Francisco, Chicago, and Philadelphia was used to make predictions of criminality in the future. Decision Tree (DT) models were more effective compared to Naive Bayes (NB) and K-Nearest Neighbours (KNN). Crime details like location, type, date, time, latitude, and longitude were explored for prediction purposes in Canada and had an accuracy of 39% to 44% by using DTs and KNN. A subsequent analysis using Logistic Regression (LR), Decision Trees (DT), Random Forest (RF), Support Vector Machine (SVM), and Bayesian techniques revealed that KNN had the highest accuracy of 78.9% in predicting crime.

3. Methodology

This section describes the system methodology in detail. Figure 1 illustrates the proposed model, wherein the dataset is used as the input for subsequent processes. Several machine learning algorithms are utilized to train the model based on the varying nature of cyberattack data in the dataset. The framework includes the following important steps: Dataset Selection: Determine and pick the dataset upon which the model will be trained and tested. Data Preprocessing: Clean or remove irrelevant and missing data, and use encoding techniques on data to get ready the dataset for analysis. (Figure 1)

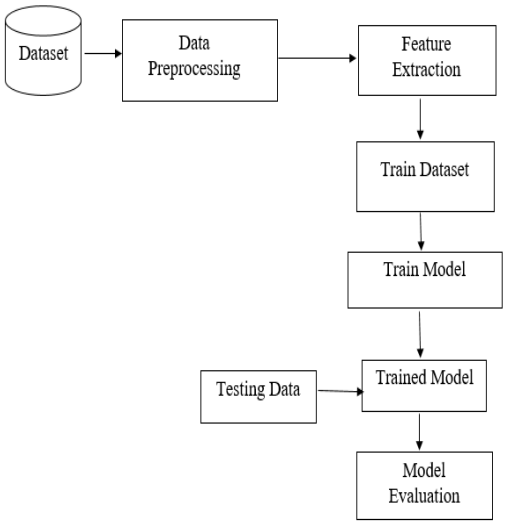

Figure 1 Proposed System Architecture

3.1.Feature Extraction

Discover and pick features most appropriate to the dataset that will enhance the accuracy of detection and model efficacy.

3.2.Data Splitting

Partition the dataset into training and test subsets to create and train the suggested model.

3.3.Model Training

Train the model using machine learning algorithms like Logistic Regression, Gaussian Naive Bayes, Support Vector Machine (SVM), Decision Tree, Random Forest, and K-Nearest Neighbors (KNN).

3.4.Model Evaluation

Test the trained model on the test dataset and measure its performance using different metrics like precision, recall, F1-score, cross-validation score, accuracy, training score, and testing score.

3.5.Collection of Dataset

For experimentation data is taken from Kaggle. It is open source repository. Dataset that can be accessed https://www.kaggle.com/hassan06/nslkdd In this research database NSL-KDD is used to create intrusions detection models. Dataset it has two sections as NSL-KDD train, and NSL-KD D test sets. All type attacks on NSL-KDD datasets are categorized to in four class namely DoS, Probe, R2L, and U2R [4]. Train + dataset.

3.6.Data Preprocessing

Data preprocessing involves transforming raw data into a suitable format for machine learning models. It is a fundamental and essential step in building an effective model. The dataset used contains missing and redundant values, commonly referred to as outliers. Therefore, preprocessing is performed to identify and eliminate these outliers, ensuring data quality and improving model performance.

3.7.Feature Extraction

Feature extraction focuses on selecting the most relevant attributes from a dataset to enhance detection accuracy and processing speed. The dataset consists of 42 columns, from which 10 key features are selected for training. To achieve optimal feature selection, the Recursive Feature Elimination (RFE) method is employed. Compared to other selection techniques, the feature importance ranking of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

Random Forest demonstrates high accuracy. RFE works iteratively by training an estimator on the complete set of features, then systematically removing the least significant ones. This process continues until the optimal number of features is retained, ensuring an efficient and effective model.

3.8.ML Algorithms

In this model we are applying machine learning algorithms like Logistics Regression, Gaussian Naïve Bayes, Support Vector Machine (SVM), Decision Tree, Random Forest Nearest Neighbour (KNN)

3.9.Trained Model

In this stage, the trained model's performance is assessed using a test dataset. Various evaluation metrics are applied, such as precision, recall, F1 score, cross-validation score (CV), accuracy, training score, and testing score. These metrics help analyze the model's effectiveness and its capability to generalize to unseen data, ensuring reliable performance.

4. Result & Discussion

4.1.Data Analysis

The NSL-KDD dataset is a widely recognized benchmark for evaluating and comparing intrusion detection systems. It is divided into two subsets: the NSL-KDD training dataset and the NSL-KDD test dataset. The training set comprises 4,898,431 records, while the test set includes 311,027 records. This dataset consists of 41 features, along with a 42nd feature that categorizes network connections into five classes—one representing normal traffic and four representing different types of attacks. These attack classes are further classified into four major categories: Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The categorization of these categories of attacks is given in Table 1

4.2.Correlation Heatmap

A correlation heatmap is a visual representation of the correlation matrix, which displays the pairwise correlation coefficients between variables in a dataset as a color-coded matrix. This heatmap provides a quick and intuitive way to identify patterns of correlation among variables. Correlation heatmap is typically created and interpreted (Figure 2)

Table 1 Classification of Attacks

Attack Class	Attack Type
DoS	Back , Land , Neptune , Pod , Smurf , Teardrop, Worm
Probe	Satan , Ipsweep , Nmap , Portsweep , Mscan , Saint
R2L	GuessPassword, Ftpwrite, Imap, Phf, Multihop, Warezmastery
U2R	Buffer Overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm

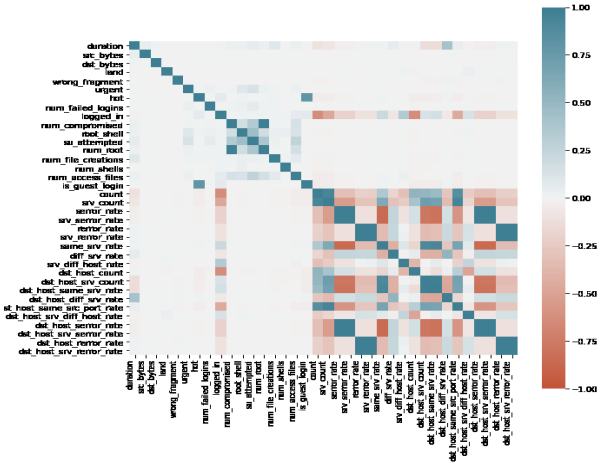

Figure 2 Correlation Heatmap of NSL KDD Dataset

Table 2 Performance Evaluation on Training

Algorithm	Precision	Recall	F1 Score	Accuracy
Logistic Regression	82.351	81.432	80.389	80.312
Gaussian Naive Bayes	86.762	89.231	89.176	89.19
Support Vector Machine	87.543	87.327	86.160	87.155
Decision Tree	99.520	99.600	99.054	99.401
Random Forest Classifier	99.580	99.815	99.985	99.986
KNN	88.451	88.243	86.308	88.306

Table 2 Shows the Performance Evaluation on training dataset with different machine learning

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

algorithms. The performance comparison of all machine learning models on the training dataset shows that Decision Tree and Random Forest far exceed other algorithms with almost 99% accuracy, precision, recall, and F1 score. Of the other classifiers, Gaussian Naïve Bayes performs the best with 89.19% accuracy, then comes Support Vector Machine (87.15%) and K-Nearest Neighbors (88.31%), with Logistic Regression having the lowest accuracy at 80.31%. These findings emphasize the greater efficiency of tree-based models in classification tasks and thus render them the most appropriate option for this dataset given their capacity to learn complex patterns effectively. From the observations Random Forest and Decision Tree achieves 99% accuracy, Precision, Recall and F1 Score.

Table 3 Presents the Performance Assessment

Algorithm	Precision	Recall	F1 Score	Accuracy
Logistic Regression	74.73	73.65	70.66	76.58
Gaussian Naive Bayes	66.76	69.23	69.17	69.19
Support Vector Machine	82.52	79.53	69.48	79.53
Decision Tree	83.62	89.23	87.25	89.63
Random Forest Classifier	89.70	86.81	83.79	87.82
KNN	80.57	76.59	71.50	76.59

Table 3 presents the performance assessment of various machine learning models on the test dataset. Among them, Decision Tree and Random Forest exhibit strong performance**,** with accuracy rates of 89% and 87%**,** respectively. In terms of precision**,** Random Forest attains 89.70%, while Decision Tree reaches 83.62%**.** Additionally**,** Decision Tree records a recall of 89.23%, whereas Random Forest achieves 86.81%**.** On the other hand**,** Gaussian Naïve Bayes shows the lowest accuracy at 69.19%**,** indicating its comparatively weaker performance on the test dataset.

Table 4 Performance Evaluation on Testing Dataset

Algorithm	Train Score	Test Score	CV Score
Logistic Regression	74.73	73.65	70.66
Gaussian Naive Bayes	66.76	69.23	69.17
Support Vector Machine	82.52	79.53	69.48
Decision Tree	83.62	89.23	87.25
Random Forest Classifier	89.70	86.81	83.79
KNN	80.57	76.59	71.50

Table 4 depicts the Train, Test and CV Score. Decision Tress (DT) Train Score is 100%. Random Forest (RF), algorithm Train, Test Score and CV Score is 99%. From Observations we can say that Random Forest (RF) and Decision Tress (DT) algorithm is more accurate for classification and prediction of attacks. An experiment utilizing the NSL-KDD dataset**,** which consists of multiclass data, demonstrated that Decision Tree and Random Forest outperformed other algorithms in terms of accuracy**.** However, the effectiveness of these models may fluctuate depending on the dataset's specific values and characteristics.

Conclusion

With the rapid advancement of technology, maintaining system security has become increasingly challenging, particularly in detecting cyber-attacks. This study provides a comparative analysis of machine learning algorithms for cyber threat prediction and detection. Using the NSL-KDD dataset, multiple algorithms were evaluated, with Random Forest achieving the highest accuracy (89%)**,** followed by Decision Tree (87%)**,** while Gaussian Naïve Bayes recorded the lowest accuracy (69%)**.** The results underscore the effectiveness of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

machine learning in enhancing network security monitoring**.** Future research will focus on utilizing multiclass datasets to further assess system performance and explore more complex cyber-attack scenarios.

References

[1]. Gawand, S, & Kumar, M. S. (2024). Analytics of Binary Class Detection & Forecasting of Cyber Incident by Machine Learning Methods. International Journal of Intelligent Systems and Applications in Engineering, 12(20s), 100–108. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5122

[2]. Kousik Barik, Sanjay Misra, Karabi Konar, Luis Fernandez-Sanz Murat Koyuncu," Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study", Applied Artificial Intelligence, Published with license by Taylor Francis Group, pp 1-25,2022

[3]. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez- Sanz Vera Pospelova," The Emerging Threat of Ai-driven Cyber Attacks: A Review", Applied Artificial Intelligence, Published with license by Taylor Francis Group,1-36, DOI: 10.1080/08839514.2022.2037254,2022

[4]. Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Aldu- ailij, and Fazila Malik," Machine-Learning-Based DDoS Attack Detection Using Mutual In- formation and Random Forest Feature Importance Method", Cloud Computing and Symme- try: Latest Advances and Prospects,1-15, DOI https://doi.org/10.3390/sym14061095,2022

[5]. Arpitha. B,Sharan. R , Brunda. B. M,Indrakumar. D. M, Ramesh,"Cyber Attack Detection and notifying system using ML Techniques", Indian Journal of Computer Science and Engineering (IJCSE) ,pp 28153-28159,2021

[6]. Fahima Hossain, Marzana Akter and Mohammed Nasir Uddin," Cyber Attack Detection Model (CADM) Based on Machine Learning Approach ",2nd International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST) ,pp 567-572,2021

[7]. Abdulkadir Bilen and Ahmet Bedri Özer," Cyber-attack method and perpetrator prediction using machine learning algorithms",PeerJ Computer Science,pp 475-496 ,2021

[8]. Florian Klaus Kaisera , Tobias Budiga ," Attack Forecast and Prediction ", C&ESAR'21: Computer Electronics Security Application Rendezvous, pp 77-97, 2021

[9]. Twinkle Shah, Sagar Parmar , Kishan Panchal," Cyber Crime Attack Prediction", International Research Journal of Engineering and Technology ,pp 1037–1042. 2020

[10]. Kumar,"Cyber-attack prediction using machine learning algorithms", International Conference on Advances in Computing, Communication and Control (ICAC3),pp 1–5,2020

[11]. H. Aqahtani, I. Sarker, A. Kalim, S. Minhaz Hossain, S. Ikhlaq and S. Hossain,"Cyber Intrusion Detection Using Machine Learning Classification Techniques," In Proc. International Conference on Communications in Computer and Information Science, pp. 121-131, 2020

[12]. A. Ahmim, M. Ferrag, L. Maglaras, M. Derdour and H. Janicke, "A Detailed Analysis of Using Supervised Machine Learning for Intrusion Detection," Strategic Innovative M arketing and Tourism, pp. 629-639, 2020.

[13]. W. Zong, Y. Chow and W. Susilo, "Interactive three-dimensional visualization of network intrusion detection data for machine learning," Future Generation Computer Systems, vol. 102, pp. 292-306, 2020

[14]. O. Sarumi, A. Adetunmbi and F. Adetoye, "Discovering computer networks intrusion using data analytics and machine intelligence," Scientific African, vol. 9, p. p 1-5, 2020.

[15]. A. Nagaraja, B. Uma and R. Gunupudi, "UTTAMA: An Intrusion Detection System Based on Feature Clustering and Feature Transformation," Foundations of Science, vol. 25, no. 4, pp. 1049-1075,2020.

[16]. A. Saleh, F. Talaat and L. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers", Artificial Intelligence Review, vol. 51, no. 3, pp. 403-443, 2020.

[17]. H. Liu and A. Gegov, "Collaborative Decision Making by Ensemble Rule Based Classification Systems," Studies in Big Data, pp. 245-264, 2020.

[18]. P. Negandhi, Y. Trivedi and R. Mangrulkar, "Intrusion Detection System Using Random Forest on the NSL-KDD Dataset," Emerging Research in Computing, Information,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 834-840
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0118

Communication and Applications, pp. 519-531, 2019.

[19]. C. Gayathri Harshitha, M. Kameswara Rao and P. Neelesh Kumar, "A Novel Mechanism for Host-Based Intrusion Detection System," In Proc. First International Conference on Sustainable Technologies for Computational Intelligence, pp. 527-536, 2019.

[20]. Y. Ever, B. Sekeroglu and K. Dimililer, "Classification Analysis of Intrusion Detection on NSL-KDD Using Machine Learning Algorithms," In Proc. International Conference on Mobile Web and Intelligent Information Systems, pp. 111-122, 2019.

[21]. T. Tang, D. McLernon, L. Mhamdi, S. Zaidi and M. Ghogho, "Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach," Deep Learning Applications fo r Cyber Security, pp. 175-195, 2019.

[22]. A. Gupta, G. Prasad and S. Nayak, "A New and Secure Intrusion Detecting System for Detection of Anomalies Within the Big Data," Studies in Big Data, pp. 177-190, 2018.

[23]. A. Saleh, F. Talaat and L. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers", Artificial Intelligence Review, vol. 51, no. 3, pp. 403-443, 2017.

[24]. M.Ibrahim," An empirical comparison of random forest-based and other learning-to-rank algorithms, "Pattern Analysis and Applications, vol. 23, no. 3, pp. 1133-1155, 2019.

[25]. Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things, Volume 7,2019,100059,ISSN25426605,https://doi.org/10.1016/j.iot.2019.100059.

[26]. M. G. Raman, N. Somu, S. Jagarapu, T. Manghnani, T. Selvam, K. Krithivasan, V.S. Sriram, An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm, Artificial Intelligence Review (2019) 132