DS Journal of Multidisciplinary
Volume 1 Issue 1, 16-22, Jan - Mar 2024
ISSN: XXXX-XXXX

Original Article

Intrusion Detection System via CNN-Ghostnet for IoT-Based Smart Cities

R. Surendiran

School of Information Science, Annai College of Arts and Science, Kumbakonam, India.

surendiranmca@gmail.com

Received: 19 October 2023; Revised: 19 November 2023; Accepted: 11 December 2023; Published: 22 January 2024;

Abstract - Cyber security plays a vital role in securing the data as well as the system. Poor security and high attack possibilities are present in IoT. So, an accurate Intrusion Detection System is needed to develop with high detection accuracy. In the existing methods, poor accuracy detection is termed as the major disadvantage. So, to develop the security rate and the detection accuracy, a novel Convolution Neural Network-based DEEP-Intrusion Detection System (IDS) has been developed. The main motive of this research is to improve attack detection accuracy. UNSW-BN15 and BoTIoT datasets are used to detect the attack. Moreover, the features present in the data set are extracted through the Convolution Neural Network. The layers present in the convolution networks are responsible for the feature extraction process. Then, the performance of the proposed model can be validated in different parameters such as detection accuracy, recall, precision, and F1 score. The performance score of the proposed model is then compared with the existing models. Finally, the proposed model has achieved 98% of intrusion detection accuracy. It is high when compared with the existing methodologies.

Keywords - Convolution Neural Networks (CNN), Intrusion Detection System (IDS), Internet of Things (IoT), Attacks, Data normalisation.

1. Introduction

In IoT, poor data security is the major demerit, and attacks are highly possible in IoT systems. Cyber security is responsible for providing security to the data and the system. It protects the system from cyber-attacks, and it also rejects requests that arise from unauthorised users [1]. Maintaining data security is essential for every organisation; otherwise, it is easy for hackers to attack the system. CNN is the deep learning network which learns directly towards the data [2].

In the image process, CNN are useful to find the image patterns as well as to recognise the objects and to get more information about the image category [3]. Moreover, CNN is more efficient in time series, audio classification and signal data processing. Basically, the CNN has three different layers, namely, the fully connected layer, the pooling layer as well as the convolutional layer [4].

The function of IDS is to monitor the system against suspicious activities and provide an alert indication if any attacks are detected. If any alert signs are detected, then the Security Operations Centre (SOC) predictor or incident responder can examine the problem and take the proper actions to remediate the threat [5]. Moreover, the basic IDS structure can be illustrated in Figure 1.

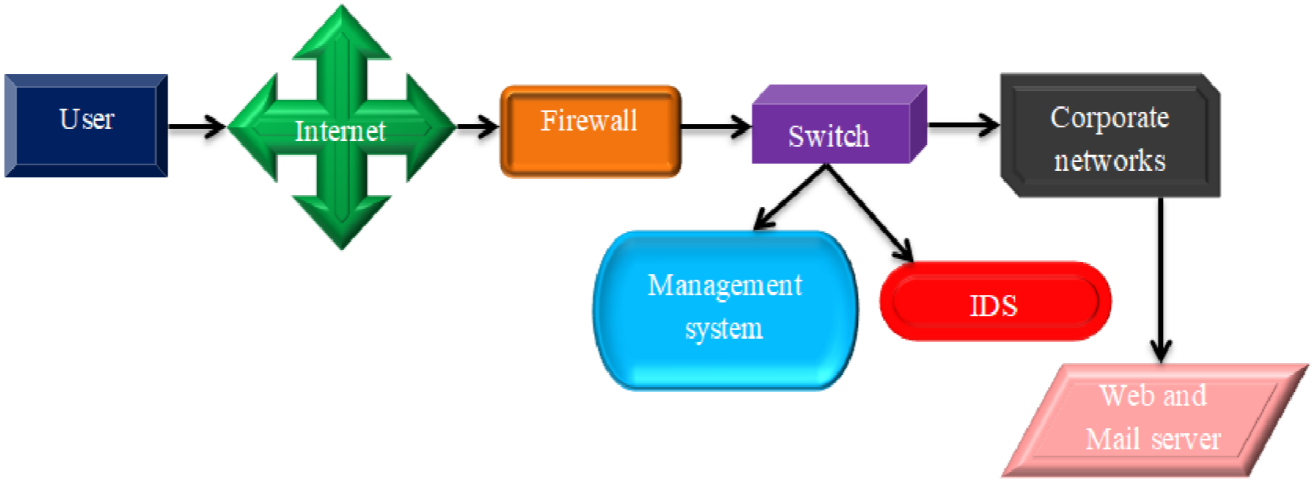

Fig. 1 Structure of IDS

The function of a firewall is to protect the network [6]. Firewalls are used for analysing the metadata, allowing traffic and blocking traffic regarding the defined set of rules [7]. If the sensor detects an attack, it can alert the switch for ignoring the wrong client. The proposed intrusion detection model detects the intrusion as well as it can able to detect the type of attack [8].

The introduction of the proposed model is presented in Section 1; recent literatures related to this topic is discussed in Section 2. The proposed model is presented in Section 3. Moreover, the result and discussion of the proposed model are presented in Section 4, and the research is concluded with the conclusion in part 5.

2. Related Works

Some of the recent literatures related to this topic is discussed below;

Jung Hyun Ryu and Jong Hyuk Park [9] have proposed the Machine Learning (ML) based IDS. Currently, the cloud computing-related IoT environment is suffering from difficulties such as enhanced traffic data rate, heterogeneity and delay. The above-mentioned difficulties are overcome by fog or edge computation mechanisms. To enhance the performance rate, an AI-based IDS system is developed. However, high error possibilities are present in ML-based mechanisms.

Laisen Nie et al. [10] have presented the Deep CNN-based IDS to detect the intrusion accurately. The CNN-based backpropagation algorithm is developed in this research. The main motive of this research is to reduce the error rate and enhance the detection accuracy of the existing models. Here, the features are extracted through the layers of CNN. However, when training the data set over, overfitting occurs sometimes, which is considered the major demerit in CNN.

Tanzila Saba et al. [11] have suggested anomaly-based IDS for IoT networks by the Deep Learning (DL) mechanism. The major motive of this research is to enhance the security rate of IoT. Here, CNN based method for anomaly-related IDS is proposed. Initially, the disadvantages of IoT in various fields are analysed. NID and BoT-IoT data sets are chosen for detection purposes, and the proposed model has attained a higher accuracy rate. However, gradient discharge is considered the major drawback in the CNN model.

Yifan Guo et al. [12] have proposed the unverified anomaly detection IoT over smart cities. In this research, a Gated Recurrent Unit (GRU) related Gaussian Mixture VAE mechanism, called GGM-VAE, is developed. Here, GRU is responsible for developing the correlation among time series data. The major disadvantage presented in

the existing methodologies is insufficient data capturing. A novel Bayesian Inference Criterion (BIC) is developed to find distribution over Gaussian Mixture latent space to overcome this issue. However, the GRU acquires lower learning efficiency.

Wajdi Alhakami et al. [13] have developed the network anomaly IDS through a Nonparametric Bayesian mechanism. The anomaly-based IDS's main demerit is that it produces many unsuitable false alarms when any irregular events are detected. Thus, the higher rate of producing false alarms decreases the performance of the detection system and also decreases the security rate. This research develops a nonparametric Bayesian mechanism for both known and unknown attacks. Moreover, the proposed model was processed with a popular dataset, and the model attained higher efficiency than the existing models. Compared with other neural networks, the Bayesian neural networks are more complex.

3. Proposed Deep-IDA Model

At present, smart cities have been developed as a promising model over the transition towards providing efficient and real-time-based smart services. In spite of the huge potential it conveys to the individual's life, security and privacy matters still need to be addressed. Due to the technology developments, a huge amount of data is created, where the Deep Learning-based mechanism is applied to acquire significant patterns. Such methodologies can be utilised to provide extra security and privacy assertions during the live movement of Virtual Machines (VMs) over the cloud and to protect IoT networking systems.

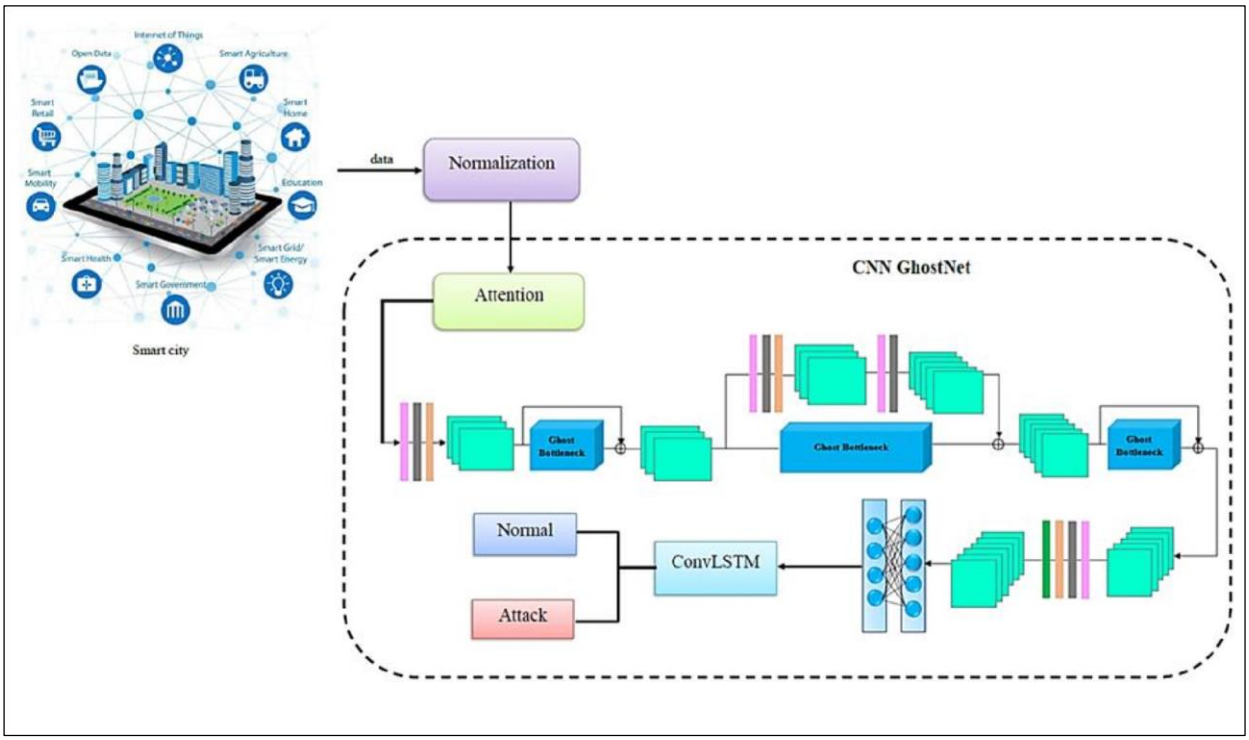

Fig. 2 Overall block diagram for the proposed DEEP-IDA system

It would permit the security-based transmission of VMs amongst data centres or to the cloud providers in real time. This research develops a novel Deep Intrusion Detection System (DEEP-IDS) system, which offers security-based distributed intrusion detection in IoT.

In the privacy-preserving method, the inconsequential end-to-side neural networks design Ghost Net and convLSTM are selected for developing a long-term recurrent CNN. The combined approach realises the

classification of behaviours. Subsequently, the developed model and its approaches are evaluated through network datasets such as UNSW-BN15 and BoT-IoT. Then, the performance of the proposed model can be compared with some attack detection techniques to measure its efficiency while arranging it to the cloud. Finally, the overall proposed model is given in Figure 2.

3.1. Data Initialising

In this research, UNSW_BN15 and BoTIoT data sets are used for detection purposes. The initialised data set contains both normal data as well as attack data. The type of data is analysed and detected through a Convolution Neural Network. Thus, the data initialisation function of the model can be declared through Equation (1),

$$I(d) = \{(A,A'',K,K'' \ldots\ldots \ldots\ldots N,N'')\} \quad (1)$$

Where, I(d) refers to the function used for initialising the data set, and A,A", ...N,N" determines the data present in the dataset.

3.2. Normalisation and Attention

Data normalisation is a de-noising method, and the function of normalisation in CNN is to standardise the data. After data initialisation, each data present in the data set is trained and tested. Training the data set can be declared through Equation (2),

$$T'' = [I(d)] \quad (2)$$

Where the function T" is used to train the data set and Equation (2) is denoted as that the initialised dataset is trained. Then normalisation is done; otherwise, the detection accuracy of the system is reduced, and the system increases the detection time. Moreover, the function of normalisation is it arranges the data present in a dataset based on the database. Normalisation function of the model can be declared through Equation (3),

$$n(d) = \sum_{k=0}^{n=1} T''(d) \quad (3)$$

Where the term n(d) refers to the normalisation function used to normalise the data, T"(d) represents the trained data, as the terms k and n refer to the range of data. Data attention is connecting an input data arrangement to the output data sequence. Data attention is very useful for evaluating the detection accuracy of the proposed model.

3.3. Ghost Bottleneck

The function of the ghost bottleneck is similar to the function of ResNet. In the ghost bottleneck, numerous convolution layers are integrated together to perform certain functions. The layer present in the convolution network is used for extracting the model's features. Here, features such as normal and attack data are present in the dataset. Among them, the needed features are extracted. However, the feature extraction of the proposed model can be declared through Equation (4),

$$\omega^F = \sum_{k=0}^{n=1} \{n^*(d) - a^*(d)\} \quad (4)$$

Here, the ω^F function refers to the feature extraction function, $n^*(d)$ refers to the normal data present in the dataset, and $a^*(d)$ defines the attack's present data.

4. Result and Discussion

In the result and discussion section, the performance of the proposed model can be validated. Here, the performance of the proposed model can be calculated through different metrics such as accuracy, recall, precision, and F1 measure. The proposed design attains higher performance rates, indicating that the proposed model can detect the intrusion accurately.

4.1. Accuracy

The accuracy of the proposed model defines the exact prediction done by the proposed model. Accurateness can be validated through the amount of correct and wrong detection detected by the proposed model. The accuracy of the proposed design can be declared through Equation (5),

$$a = \frac{\omega+\varphi}{\omega+\rho+\varphi+\sigma} \tag{5}$$

Where, a is the accuracy calculating function, ω refers to the amount of true positive rate, φ defines true negative, ϱ defines false positive, and σ is the false negative rate of the proposed model. The accuracy rate attained by the proposed model is about 98%.

4.2. F1 Score

F1 score is the machine learning calculation metric which calculates the model's accuracy. The F1 score is validated by combining the precision and recall rates of the developed design. Thus, the accuracy metrics are used to calculate how many times the proposed model detects the correct intrusion detection over the initialised data set. The F1 score of the proposed model can be declared through Equation (6),

$$f' = 2 \times \left(\frac{p''}{r''}\right) \tag{6}$$

Where the parameter f′ is the f1 score calculating function of the proposed design, the F1 score of the proposed model is 99%.

4.3. Precision

Precision defines the amount of correct detection done under the positive class. The precision score of the proposed model can be declared through Equation (7),

$$p'' = \frac{\omega}{\rho+\varphi} \tag{7}$$

Where the parameter p" refers to the precision function of the proposed design. The proposed model has attained 97% of the precision score.

4.4. Recall

Recall refers to the total amount of positive detection detected among all the positive occurrences. Moreover, the recall of the proposed model is 95%. Thus, the recall rate of the proposed model can be declared by Equation (8),

$$r'' = \frac{\omega}{\omega+\sigma} \tag{8}$$

Here, r" is the recall function of the proposed model.

The performance metrics of the proposed model have been measured through different metrics such as accuracy, precision, recall and F1 score. Moreover, the performance score of the proposed model is compared

with the existing models such as Hybrid Decision Tree (HDT) [14], Decision Tree (DT) [14], K-Nearest Neighbours (KNN) algorithm [14], and Support Vector Machine (SVM) [14]. Among them, the proposed model has attained a better performance score than the existing models. The performance comparison of the proposed model with the existing models is shown in Figure 3, and the overall performance of the proposed model is illustrated in Figure 4.

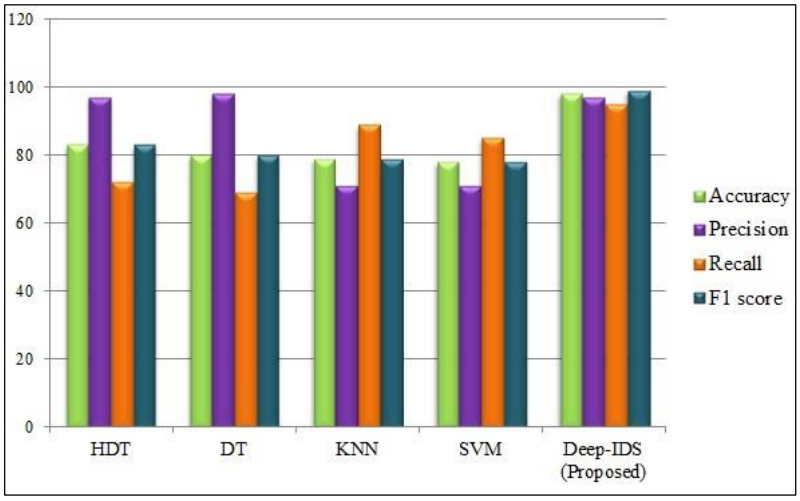

Fig. 3 Accuracy, precision, recall and F1 score comparison

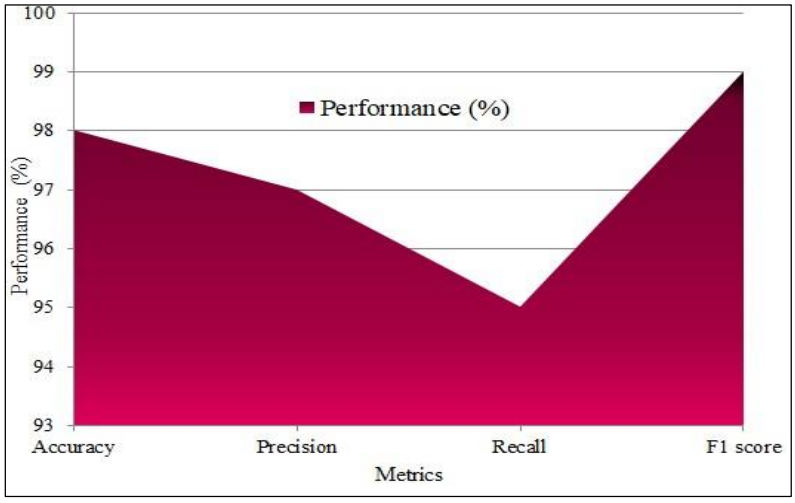

Fig. 4 Overall performance of the proposed model

5. Conclusion

Cyber security secures the data as well as the system among the attacks. Detecting the intrusion is essential for providing security. In this research, UNSW-BN15 and BoTIoT data sets are used for detecting the intrusion. The above-mentioned data set contains both the attack and the normal data. Initially, data normalisation is done to remove the noisy data present in the dataset.

Moreover, the data features are extracted through Convolution Neural Networks, and the layers are responsible for extracting the features. Thus, the performance of the proposed model can be validated through different performance metrics such as accuracy, precision, recall and F1 score. The accuracy rate of the proposed model is about 98% compared with the existing models; 15% accuracy can be improved in the developed design.

The recall score of the model is about 95%, and 6% of the recall rate is developed through the proposed model. Then, 97% of precision can be attained by the proposed model, and 99% of F1 score can be achieved through the DEEP-IDS system. While comparing the F1 score of the proposed model with the existing models, 16% of the F1 score can be improved. The improved rate of parameters indicates that the proposed system can detect the intrusion accurately.

References

[1] Karthik Kallepalli, and Umair B. Chaudhry, "Intelligent Security: Applying Artificial Intelligence to Detect Advanced Cyber Attacks," *Challenges in the IoT and Smart Environments*, pp. 287-320, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Yanmiao Li et al., "Robust Detection for Network Intrusion of Industrial IoT Based on Multi-CNN Fusion," *Measurement*, vol. 154, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jin Yuan et al., "Gated CNN: Integrating Multi-Scale Feature Layers for Object Detection," *Pattern Recognition*, vol. 105, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Yong Soon Tan et al., "Convolutional Neural Network with Spatial Pyramid Pooling for Hand Gesture Recognition," *Neural Computing and Applications*, vol. 33, pp. 5339-5351, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Selina Y. Cho, Jassim Happa, and Sadie Creese, "Capturing Tacit Knowledge in Security Operation Centers," *IEEE Access*, vol. 8, pp. 42021-42041, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sun Jingyao et al., "Securing a Network: How Effective Using Firewalls and VPNs Are?," *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference,* vol. 2, pp. 1050-1068, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Soliman Abd Elmonsef Sarhan, Hassan A. Youness, and Ayman M. Bahaa-Eldin, "A Framework for Digital Forensics of Encrypted Real-Time Network Traffic, Instant Messaging, and VoIP Application Case Study," *Ain Shams Engineering Journal*, vol. 14, no. 9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Vikash Kumar et al., "An Integrated Rule-Based Intrusion Detection System: Analysis on UNSW-NB15 Data Set and the Real Time Online Dataset," *Cluster Computing*, vol. 23, pp. 1397-1418, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jung Hyun Ryu, and Jong Hyuk Park, "Machine Learning-Based Intrusion Detection System for Smart City," *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 2018*, Springer Singapore, pp. 405-409, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Laisen Nie et al., "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2219-2230, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Tanzila Saba et al., "Anomaly-Based Intrusion Detection System for IoT Networks through Deep Learning Model," *Computers and Electrical Engineering*, vol. 99, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yifan Guo et al., "Unsupervised Anomaly Detection in IoT Systems for Smart Cities," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2231-224, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Wajdi Alhakami et al., "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection," *IEEE Access*, vol. 7, pp. 52181-52190, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Seyedeh Mahsan Taghavinejad et al., "Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree," *6th International Conference on Web Research,* 2020. [CrossRef] [Google Scholar] [Publisher Link]