DOI: 10.xx/ijdsml.2023.xx

ANALYSIS OF DEEP LEARNING INTRUSION DETECTION SYSTEMS USING PRIVACY-PRESERVING TECHNIQUE

Mayank Hindka
Department of Computer Information Systems, Texas A&M University, United States of America

Abstract

There is an urgent need for globally competitive products with more variability, better and dependable quality, reduced cost, and shorter life cycles. The espousal of the IoT in industrial applications leverages communication between people, data analytics, and intelligent machines designed to fulfill emerging market demands while continuing to realize their business goals. An IDS is an indispensable cog widely used in IoT networks to recognize malevolent network activities. IDS models sense malevolent instances and create a healthful environment for business and API Security [17]. Even though DL-based IDSs perform better in identifying new cyber-attacks, they are frequently hampered by some restrictions, including higher false alarm rates, deprived reliability, ineffective against cutting-edge cyber-attacks, and lower prediction performance owing to class imbalance problems. Therefore, an efficient IDS model is inevitable in the IoT environment to handle these problems. This study proposes three IDS models by applying different DL and optimization algorithms for identifying and classifying security breaches while preserving the privacy of sensitive user data in IoT networks.

Keywords:

Internet of Things (IoT), Intrusion Detection System (IDS), Cyber Security, API Security, Privacy Preserving Technique

1. INTRODUCTION

The IoT network is susceptible to potential threats and needs perplexing methods to realize the required security level. IDS framework is a retrofit approach for designing a protective shield against cyber threats. The basic idea of IDS models hinges on the behaviors of an assailant, which will diverge atypically from that of an authorized user, and that abundant illicit actions are visible. To sneak into an IoT network, assailants might intentionally exploit the weakness of the IoT networks and create several threats, which could cause confidential private information to be revealed, data alteration, or potential data loss [1].

To mitigate adversaries or malicious nodes from distressing the average performance of the system, some network security mechanisms are required to classify these adversaries in the network inevitably and enable the network to operate securely. DL algorithms, owing to their capacity to detect intrinsic behavior of the communicating nodes and data distribution, have been employed by numerous investigators in IoT data such that abnormal data distribution or invasions in networks can be quickly sensed and timeliness decisions on security and privacy protection made [2, 3].

Several DL algorithms have delivered solutions in different circumstances such that security and privacy demands for the IoT network can be satisfied. Attack identification processes especially exploit DL approaches effectively, given their ability to deliver superior outcomes compared to traditional approaches in flagging new trends of cyber threats. Despite decades of growth, prevailing IDS models still experience challenges in increasing classification accuracy, reducing the FAR, and identifying anonymous threats [4].

Topical developments in DL algorithms have transformed IDS models and improved the performance of automatic identification of crucial dissimilarities between normal and abnormal data. These algorithms' classification performance has almost exceeded human performance. Additionally, DL approaches have a sturdy generalizability in sensing anonymous threats. Motivated by the success of implementing DL algorithms in IDS models, this study adopts DL-based IDS to carry out classification tasks and identify abnormal activity in data streams in the IoT environment.

2. PRIVACY IN THE IOT SYSTEM

Preserving privacy in an IoT network is a complex problem since it involves technical, legal, and social challenges. This section presents a summary of this domain. The devices in IoT applications are enabled to collect, analyze, and communicate a massive volume of data, which, if not processed securely, can compromise the user privacy essential to preserve a competitive advantage. The enormous size of IoT and the elements in correspondence make the framework more helpless from the security angle for protecting recognizable data [5, 6]. The privacy protection of devices (e.g., data related to regular tasks of devices, frequency of communications with different gadgets, etc.) needs unique security insurance to make IoT frameworks safer from possible cyber-attacks; study of capability maturity [16, 17] on cyber-Security has also been studied to complement this research. An invader may attempt to disrupt the connection between communicating nodes and create a replay of exchanges to achieve communications under a counterfeit identity [7].

Also, the assailant can use illegal logging data of a system and can engender cyber threats such as self-promoting attacks where a malevolent node gives positive recommendations for itself, good-mounting attacks in which malicious users provide a positive reference for themselves, and bad-mounting attacks where a hostile user gives harmful recommendations against a genuine user. A phishing attack is a widely used technique to illegally access sensitive user data (e.g., username, password, bank account details, etc.). This can be done by directing seemingly genuine emails comprising malevolent links (e.g., spyware or malware). Users' private data is transmitted automatically to the invaders when they click the link. Another potential attack in the IoT environment is an attack on the database. It could be a possible attack of illegally disclosing users' sensitive data by the assailants. Hence, defending the dataset and implementing security mechanisms for local data (i.e., information stored in an IoT gadget) is fundamental to information secrecy in an IoT framework [8]. It is also essential to scheme security protocols for resource-constrained IoT networks that need a minimum of recognizable data of users and

devices. Context-aware privacy mechanisms are another vital aspect of privacy in IoT networks.

This will help industries deploy protective mechanisms by considering the present environmental conditions (e.g., user, device, location, and so on) and the concept of privacy by design [9]. Also, an invader can divulge a user's privacy by controlling the devices explicitly through device tracking/capturing and tag tracking mechanisms (e.g., RFID tag tracing). In such cases, one significant issue is stealing privileges (e.g., passwords and logging information). This can be carried out by the identity spoofing of the device, where an assailant can gain illegal access to sensitive IoT devices (e.g., medical apparatus) by violating the security measures and using an evil act (e.g., altering the dosage of an insulin pump) into a ratified session [10].

3. METHODOLOGY

DL-based privacy-preserving is a technique in an IoT network to identify cyber-attacks. The model includes (i) preprocessing methods such as data cleaning, normalization, and encoding to extract helpful information from the dataset; (ii) feature selection (FS) algorithm for optimal attribute selection method; (iii) A comprehensive set of experiments are conducted on KDD Cup dataset. The working process of the IDS approach is illustrated in Fig.1.

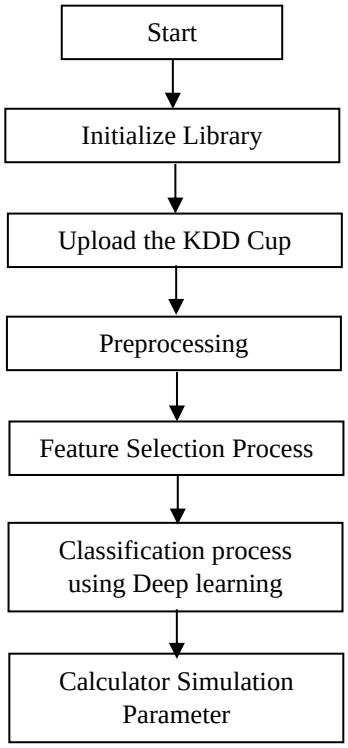

Fig.1. Process flow of the -IDS model

Designing the classifier using autoencoders is a deep learning neural network that contains several layers of sparse AE network and performs splendidly in classifying suitable high-level attributes for the improved depiction of raw input data. The chosen subset of attributes derived from the FS algorithm is given for classification purposes. An automatic encoder-based DL network is developed in this work using multiple AEs. The sparse AE adds sparse restrictions to the AE, i.e., usually a sigmoid function. During training, the output value is nearly 1 when a neuron is activated. When the output is 0, the neurons are suppressed. When several sparse AE create a deep network, it can be known as a deep network process that depends on a sparse stack autoencoder. The network model using the autoencoder is illustrated in Fig.2.

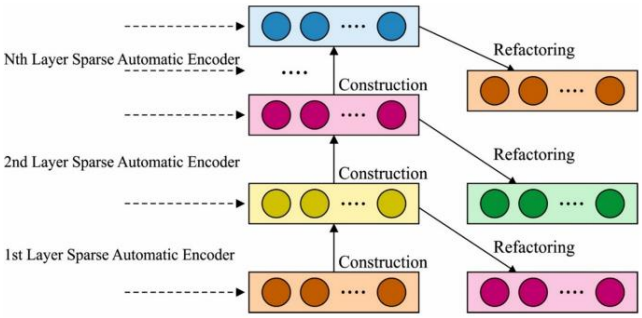

Fig.2. Structure of Auto-encoder

The performance is improved by optimally adjusting the hyperparameters of the classifier. Hence, the performance of the IDS model is improved.

4. RESULT ANALYSIS

So, the accuracy can be measured according to Eq.(1):

$$Accurancy = \frac{TN + TP}{TN + TP + FN + FP} \quad (1)$$

Different measures incorporate Accuracy, Awareness or Review, and Particularity. The recipe to determine these actions is given in Eq.(2) and Eq.(3).

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

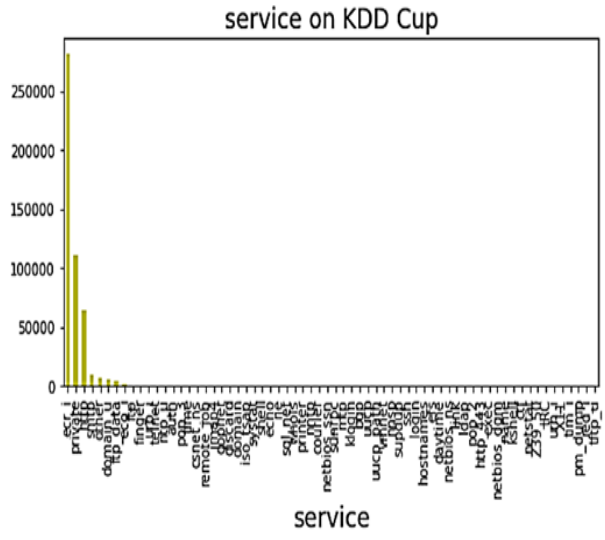

Fig.3. Different types of Service on KDD Cup

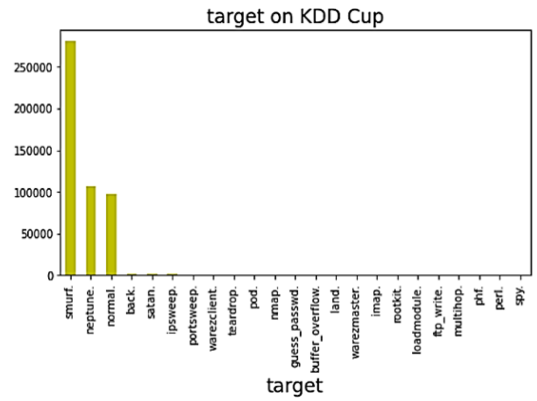

Fig.4. Different types of targets on the KDD Cup

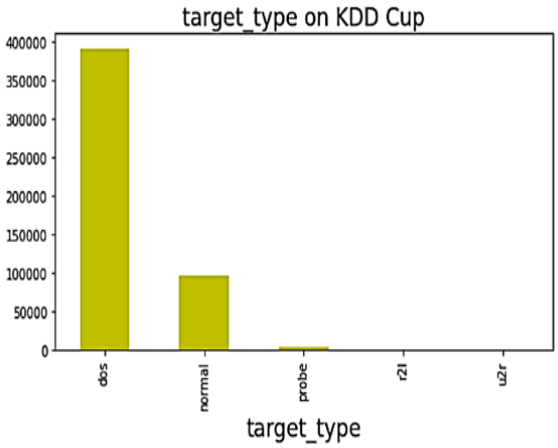

Fig.5. Target_type on KDD Cup

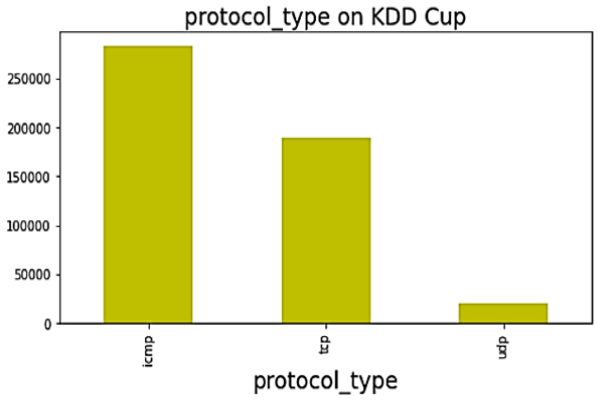

Fig.6. Protocol_type on KDD Cup

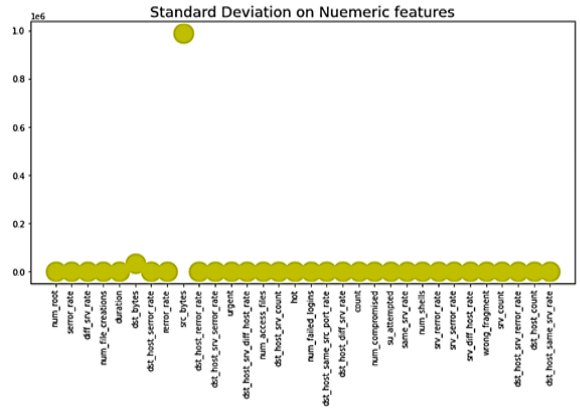

Fig.7. Standard Deviation on Numerical Features

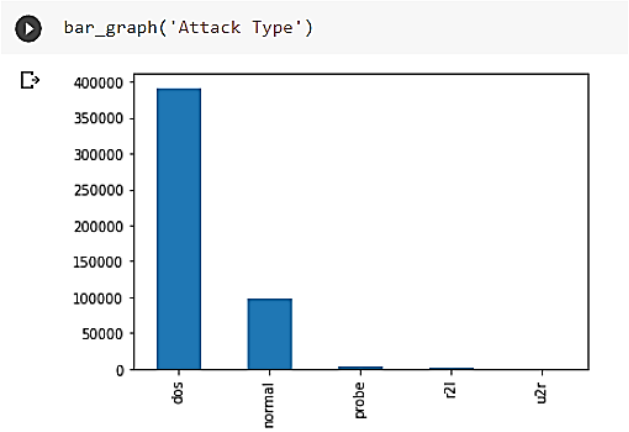

Fig.8. Different Attack Types

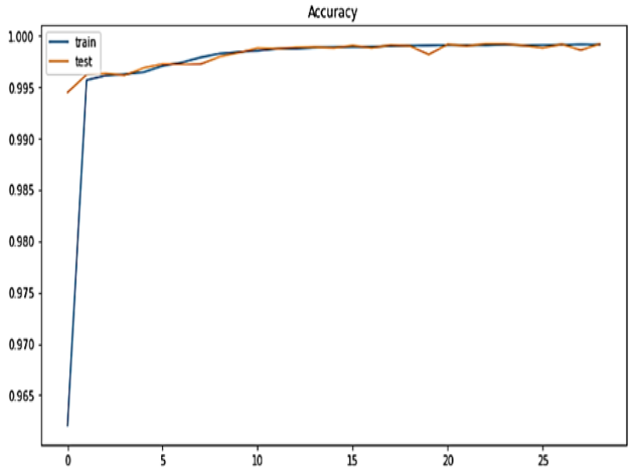

Fig.9. Accuracy for Test and Training

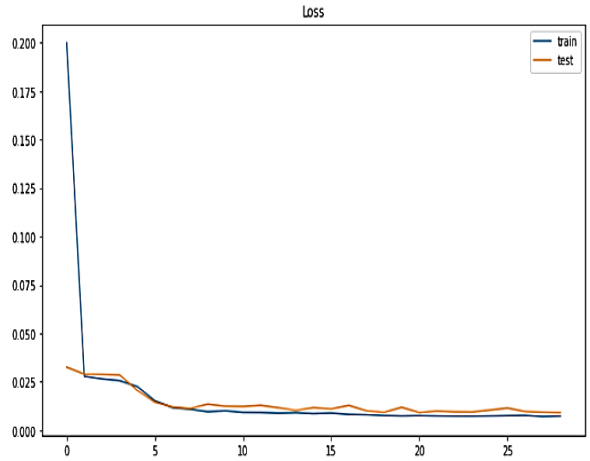

Fig.10. Loss for Test and Training

The Table.1 displays the results of the implemented method in terms of precision, recall, accuracy, loss, and F1 score. Decision tree (DT) gives a precision of 92.76%, a recall of 82.34%, an accuracy of 84.14%, a loss of 0.045, and an F1-score of 77.52%. SVM gives a precision of 93.56%, a recall of 88.46%, an accuracy of 88.46%, a loss of 0.024, and an F1-score of 88.80%. ANN-BC gives a precision of 98.78%, a recall of 93.45%, an accuracy of 98.18%, a loss of 0.003, and an F1-score of 97.88%. A graphic representation of the implemented result is presented in Fig.11 and Fig.12.

Table.1. Comparison of Result

Algorithms	Precession	Recall	F1_Score	Accuracy	Loss
Decision Tree	92.76%	82.34%	86.46%	84.14%	0.045
SVM	93.56%	88.46%	88.80%	88.46%	0.024
DL-NN	98.78%	93.45%	97.88%	98.18%	0.003

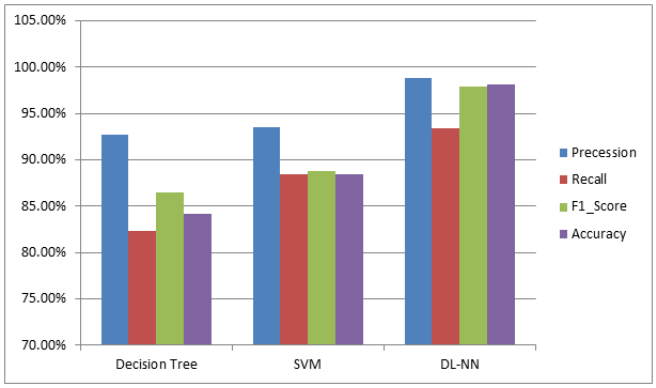

Fig.11. Graphical Represent for Precision, Recall, F1-Score, and Accuracy

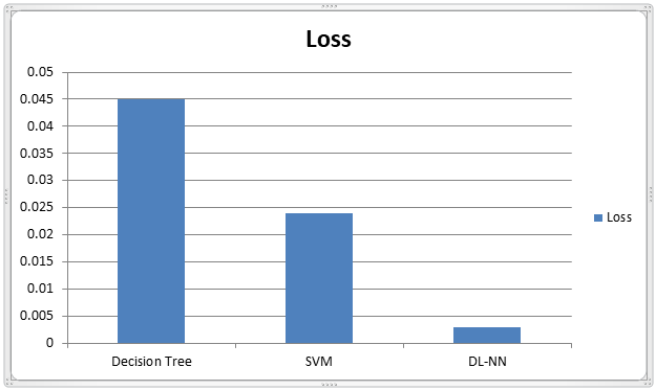

Fig.11. Graphical Represent for Loss

5. CONCLUSION

Implemented a deep learning-based IDS model to achieve secure, privacy-preserving data transmission in an IoT environment. This model includes preprocessing, feature selection, classification, and parameter optimization. A comprehensive set of experiments is carried out on benchmark datasets such as the KDD Cup. The results are analyzed in different ways.

REFERENCES

[1] A. Aburomman, "A Survey of Intrusion Detection Systems based on Ensemble and Hybrid Classifiers", *Computer Security*, Vol. 65, pp. 135-152, 2017.

[2] N.O. Aljehane, "A Secure Intrusion Detection System in Cyber-Physical Systems using a Parameter-Tuned Deep-Stacked Autoencoder", *Computers, Materials and Continua*, Vol. 68, No. 3, pp. 3915-3929, 2021.

[3] K Hujamatov, E. Reypnazarov and N. Akhmedov, "IoT, IIoT, and Cyber-Physical Systems Integration", Proceedings of International Conference on Emergence of Cyber Physical System and IoT in Smart Automation and Robotics, pp. 31-50, 2021.

[4] A. Shahraki and O. Haugen, "Boosting Algorithms for Network Intrusion Detection: A Comparative Evaluation of Real AdaBoost, Gentle AdaBoost and Modest AdaBoost", *Engineering Applications of Artificial Intelligence*, Vol. 94, pp. 1-12, 2020.

[5] M. Al-Qatf and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection", *IEEE Access*, Vol. 6, pp. 52843-52856, 2018.

[6] R. Roman and Z. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things", *Computer Networks*, Vol. 57, pp. 2266-2279, 2022.

[7] A.L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 2, pp. 1153-1176, 2016.

[8] T. Vaiyapuri and S. Binbusayyis, "Application of Deep Autoencoder as a One-Class Classifier for Unsupervised Network Intrusion Detection: A Comparative Evaluation", *PeerJ Computer Science*, Vol. 6. pp. 23-32, 2020.

[9] A.N. Jahromi and K.K.R. Choo, "Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems", *IEEE Internet Things Journal*, Vol. 8, No. 17, pp. 13712-13722, 2021.

[10] M. Sarhan and P. Marius, "Towards A Standard Feature Set for Network Intrusion Detection System Datasets", *Mobile Network and Application*, Vol. 11, pp.1-14, 2021.

[11] Y. Jacob, O. Salman and M. Malli, "Cyber-Physical Systems Security: Limitations, Issues, and Future Trends", *Microprocess Microsystem*, Vol. 77, pp. 1-11, 2020.

[12] A. Javaid and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System", *EAI Endorsed Transaction on Security and Safety*, Vol. 3, No. 9, pp. 202-214, 2016.

[13] L.A. Pacheco and E. Alchieri, "Evaluation of Distributed Denial of Service threat in the Internet of Things", *Proceedings of International Symposium on Network Computing and Applications*, pp. 89-92, 2016.

[14] S. Sicari and Coen-Porisini, "Security, Privacy, and Trust in Internet of Things: The Road Ahead", *Computer Networks*, Vol. 76, pp. 146-164, 2015.

[15] M. Tavallaee and A.A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set", *Proceedings of IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1-6, 2009.

[16] M. Hindka, "Design and Analysis of Cyber Security Capability Maturity Model", *International Research Journal of Modernization in Engineering Technology and Science*, Vol. 6, No. 3, pp. 1706-1710, 2024.

[17] M. Hindka, "Securing the Digital Backbone: An In-depth Insights into API Security Patterns and Practices", *Computer Science and Engineering*, Vol. 14, No. 2, pp. 35-41, 2024.