Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7764706

ENHANCE CYBER ATTACK DETECTION ACCURACY BY HYBRID ATTENTION NEURAL NETWORK

Manideep Beesetty
Research Scholar, Department of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, India, beesettymanideep@gmail.com

Rambabu Pemula
Associate Professor, Department of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, India, rpemula@gmail.com, rambabu.pemula@raghuenggcollege.in

RVV Murali Krishna
Associate Professor, Department of Information Technology, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, Andhra Pradesh, India, rvvmuralikrishna@gvpce.ac.in

P Praveen Kumar
Assistant Professor, Department of Information Technology, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, Andhra Pradesh, India, p.praveen@gvpce.ac.in

Bhavani Madireddy
Assistant Professor, Department of Computer Science and Engineering, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, India
bmadired@gitam.edu

Susmitha Jillela
j.susmitha1@gmail.com

Abstract— An attempt by cyber fraud to use one or more machines across one or many networks is known as a cyber-attack. Not every website that a person visits can be completely safe from cyberattacks. Thus, the user must assure cyber-security. By creating two distinct Deep Learning (DL) models that can recognize the existence of a cyberattack on a website, this study seeks to aid the user. For this purpose, the NSL-KDD dataset is used to build a database with more than 40 features related to the detection of a cyberattack. For optimal performance, the database has been preprocessed. Normalization, data encoding, and statistical highlighting are all parts of the preprocessing. The preprocessed dataset is then divided into its training and testing halves. Two different deep-learning algorithms generated two distinct models. Convolutional Neural Network (CNN) and Hybrid Attention Neural Network (HANN) are the algorithms employed in this investigation. The most effective DL model for detecting a cyberattack is identified once it has been trained and tested. Both models displayed various performance categories while being trained. The accuracy values of the model created using the CNN algorithm increased virtually linearly, reaching a point with an accuracy of more than

90% after the 14th epoch. Yet, during the 6th epoch alone, the model created using the HANN algorithm achieves an accuracy higher than 90%. During the first training period, the HANN model's highest loss value is just under 90%. The final accuracy of the model created using the CNN algorithm is 90.8%, whereas the accuracy of the HANN model is 95.8%, according to testing. In the end, it may be said that the HANN algorithm is more effective at spotting cyber-attack than CNN. This concept may one day be implemented as a backend processor for a website that verifies the legitimacy of other websites and software.

Keywords— Cyber-Attacks, Cyber-Security, Data Encoding, Filtering, Normalization, Deep Learning Models.

I. INTRODUCTION

A cyber-attack is a criminal online offence that involves using one or more computers to assault individual computers or networks. Cyberattacks are illicit attempts to access computer systems without authorization in case of theft, leak, modification, damage, or destroy data. One of the worst facts about cyber-attacks is that there are more than 15 common types of cyber-attacks and not everyone can be aware of every single type. Some common types of cyber-attacks include malware, ransomware, SQL injection, phishing attack, man-in-the-middle attack etc. Malicious software also referred to as malware, is any program or file designed to intentionally harm a computer, network, or server. Users are unable to access sensitive data or devices due to a sort of software named ransomware, which subsequently demands payment in trade for access. The code injection method known as SQL injection could be used to corrupt the database. Phishing is an attack that tries to steal someone's identity or money by coaxing them into divulging personal data. Putting oneself in the center of a user and an application's dialogue is known as a man-in-the-middle attack. Not every website visited by a user can be free of all kinds of cyber-attacks. So, the user must ensure cyber security. This study aims to assist the user by developing two different deep-learning models that can detect the presence of cyber-attack on a website. The subsequent chapters provide a comprehensive explanation of how DL models are created and used.

II. LITERATURE SURVEY

A study used the analysis of attack graphs to determine the risk of cyberattacks [1]. They suggested a risk assessment approach based on deterministic and predictable methods for cyber-physical systems. The former uses attack graphs to evaluate the likelihood of an attack, while the latter looks at any possible cyber-physical impacts. This is done by simulating the cascade failures of the power system caused by cyberattacks using a dynamic model of the cyber-physical power system. They also suggested a vocabulary specific to domains to describe the capabilities of digital distribution systems to further model the attack graphs. The suggested method is used to construct integrated risk metrics that consider the likelihood and consequences of cyber risk scenarios. The research uses a particle filter in the detection of cyber-attack [2]. Based on a particle filter, the attack detection issue for cyber-physical systems is investigated. The three forms of assaults that are implemented in the three-tank system in this work are dos, random, and false data injection. The three-tank system models and cyberattacks will be covered first. The three-tank system that is exposed to cyberattacks is then estimated using a particle filter. A residual is created using the sliding-time window technique following the estimation results to detect attacks.

The article proposed that any virtual layer is more prone to attacks than physical layers [3]. In this work, we investigate the challenge of efficient cyber-attack detection for decentralized microgrids with constrained process and measurement noises. The cyberattack that is being discussed is a covert one, it is assumed. An LSTM neural network-based strategy is recommended to construct the intrusion detection and prevention tool without using the data from the sounds. Case studies show that the suggested assault detection method can effectively handle the next two situations. The size of the cyberattack is modest, and it is unclear what the system noises' statistical properties are. Simpler systems are not the exclusive targets of cyberattacks. The journal propose that naval systems also have a high risk of attack [4]. The main objective of this study is to design a system monitoring model which is exclusively designed to keep the naval systems from cyber-attacks. Researchers mentioned that the initial operational response is highly encouraging, even though it is still in the development stage.

The authors designed an analysis-based power system to prevent cyber-attacks [5]. The platform can simulate a power grid, and a communication network, and can even show how actual gadgets and cyberattacks affect the power system. Also, a man-in-the-middle attack modelling and implementation technique for communication networks is developed. Based on this platform, a case study of an attack in a conventional CPPS is shown. The simulation findings demonstrate the value of considering the distinct effects of the communication system, operational devices, and cyber-attack in electric grid simulations. They also validate the platform's functionality. Researchers used the Bayesian Belief Network in the detection of cyber-attacks [6]. Using Bayesian Belief Networks, this paper aims to identify cyberattacks against the supply chain in the physical system. To determine how an attack would spread, they used the DAG approach to model cyberattacks. To further illustrate the relevance of the assault and the cascade repercussions, they presented a case study involving the smart grid. The findings demonstrate how Bayesian Belief Network may be modified to identify uncertainty in the case of cyberattacks against the supply chain realm.

III. MATERIALS AND METHODS

A database consisting of over forty features which are related to the identification of a cyber-attack is collected from the NSL-KDD dataset. This dataset then undergoes all the processes mentioned in figure 1 to identify the best DL algorithm that can be used in the detection of cyber-attacks.

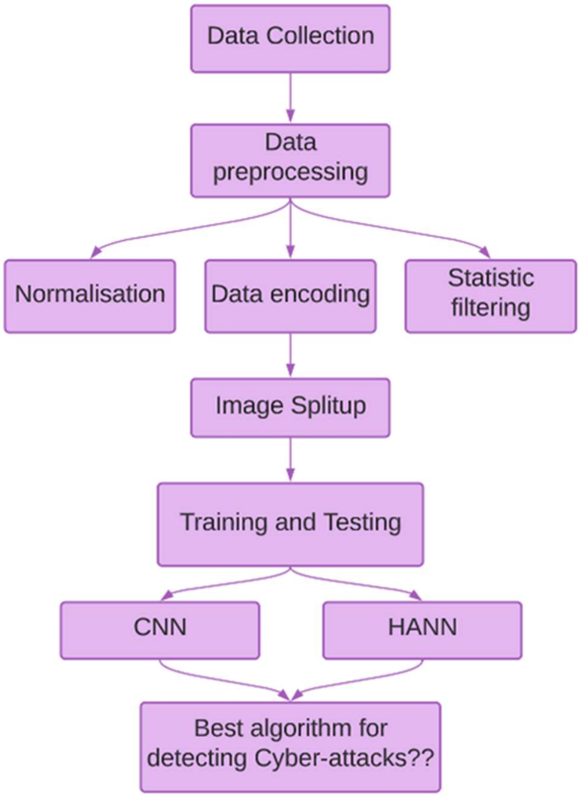
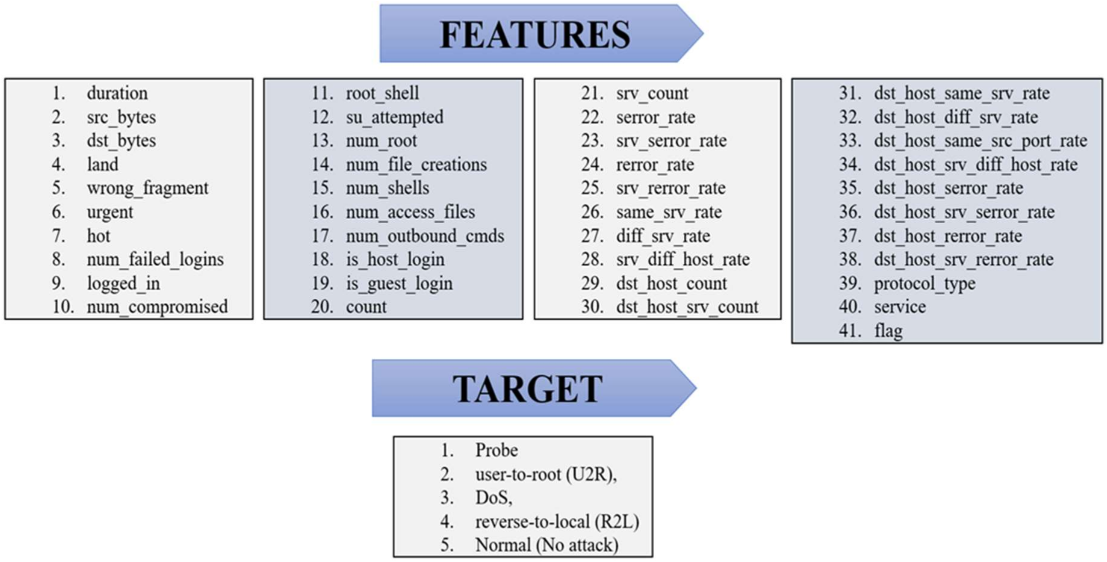


Figure 1. Workflow of the study

From figure 1, the database collected is preprocessed to ensure proper performance. The preprocessing includes normalization, data encoding and statistical featuring. The preprocessed dataset is then split into two parts – training and testing. Two distinct algorithms were used to create two DL models. CNN and HANN are the algorithms employed in this analysis. The optimal DL model which might be utilized for the detection of a cyberattack is then found once the DL models have been trained and tested.

IV. DATA COLLECTION AND PREPROCESSING

A dataset consisting of various features of a website or a software application of collected from the NSL-KDD datasets [7]. This dataset consists of various features that are associated with the safety of the website in various combinations. The sample of the features from the obtained dataset is shown in figure 2.



FEATURES

1. duration
2. src_bytes
3. dst_bytes
4. land
5. wrong_fragment
6. urgent
7. hot
8. num_failed_logins
9. logged_in
10. num_compromised
11. root_shell
12. su_attempted
13. num_root
14. num_file_creations
15. num_shells
16. num_access_files
17. num_outbound_cmds
18. is_host_login
19. is_guest_login
20. count
21. srv_count
22. serror_rate
23. srv_serror_rate
24. rerror_rate
25. srv_rerror_rate
26. same_srv_rate
27. diff_srv_rate
28. srv_diff_host_rate
29. dst_host_count
30. dst_host_srv_count
31. dst_host_same_srv_rate
32. dst_host_diff_srv_rate
33. dst_host_same_src_port_rate
34. dst_host_srv_diff_host_rate
35. dst_host_serror_rate
36. dst_host_srv_serror_rate
37. dst_host_rerror_rate
38. dst_host_srv_rerror_rate
39. protocol_type
40. service
41. flag

TARGET

1. Probe
2. user-to-root (U2R),
3. DoS,
4. reverse-to-local (R2L)
5. Normal (No attack)

Figure 2. Features in the dataset.

A total combination of 148,486 features is used for both testing and training in this study. For training, 125,943 data of the total data are used and the remaining 22,543 images are used to test both models to determine the final accuracy.

A. Normalisation

Data preparation for the DL model typically involves the normalization procedure. It only becomes necessary when features have different ranges. The goal of normalization is to scale down the numerical values in the dataset's columns without erasing any information or altering the value ranges [8]. Normalization is particularly important for neural networks since unnormalized inputs to activation functions might cause them to become stuck in a very flat region of the domain and possibly not learn at all. Moreover, it generally accelerates learning and promotes speedier convergence.

B. Data encoding

Data transformation into machine-readable form is called encoding. Both text values and numerical values can be subject to this process. Encoding is typically performed for features with lower cardinality [9]. The term "cardinality" is used to describe the greatest number of possible values for a given column. For instance, certain dataset features may have between five and six possible values. In this scenario, each potential value is given a number, typically starting at 0, and the entire dataset is modified accordingly.

C. Statistical Filtering

The process of selecting a smaller portion of your data collection and employing that subset for observation or analysis is known as statistical filtering. Filtering is often a transient procedure because the complete data set is stored but only a piece of it is used for the calculation. Examining a dataset to remove, reorganize, or distribute data under specific criteria [10]. A customer may become confused or uneasy if there is duplicated or inaccurate data. Data screening can also produce more useful results. To identify the scenarios you want to include in your analysis, filtering necessitates the specification of a rule or logic.

V. CONSTRUCTION OF THE DEEP LEARNING MODEL

The study's mind might be referred to as the DL model. To train and test the DL model, the photos are gathered and prepared. It is therefore safe to assume that DL models are essential for the detection of cyberattacks [11]. The optimal DL algorithm that can be used for this purpose is identified by comparing two different methods. There are two algorithms used: CNN and HANN.

A. CNN

The CNN algorithm is a DL technique designed especially for categorizing images. But it can also be utilized for a variety of other purposes, including data categorization and The CNN algorithm is more efficient because it is supervised. One of the main benefits of this algorithm is the reduced requirement to specify each layer due to the integrated convolutional layer [12]. This preconstructed layer only needs a small modification rather than being created from the beginning. Four layers are usual for a finished CNN model. The layers are a max-pooling layer, a completely connected layer, a convolutional layer, and a ReLu layer. These levels are modified in response to demand [13].

B. HANN

A niche deep-learning model was developed by a group of researchers from Saudi Arabia [14]. This model was initially designed to detect Covid-19. The benefit of HANN is that it will enable the primary user to both record and explain the relative and crucial differences between various types of data. The idea includes CNNs and Bidirectional Long Short-Term Memory (Bi-LSTM) networks with attention modules, and two deep neural networks. In the HANN, the preprocessing step seeks to reduce noise and improve prediction. It is followed by an embedding layer that was created using a GLOVE model that had already been created. The convolutional neural network is the HANN algorithm's next phase. A Bi-LSTM layer comes after this one. The output layer is the last one. Between the output layer and the Bi-LSTM layer, however, is an attention layer. This layer, in fact, attention mechanisms highlight crucial details by giving keywords a larger weight [15].

VI. RESULT AND DISCUSSION

The NSL-KDD dataset is used to compile a database of more than 40 features linked to the detection of a cyberattack. To guarantee proper performance, the database is preprocessed. The training and testing components of the preprocessed dataset are then separated. Two different deep-learning models were produced using two different techniques. The algorithms used in this investigation are CNN and HANN. After the DL models have been developed and put to the test, the optimum one that can be utilized to detect a cyberattack is found. Two attributes are used during training and validation. They are accuracy and loss. The accuracy graph of the CNN model is shown in figure 3.

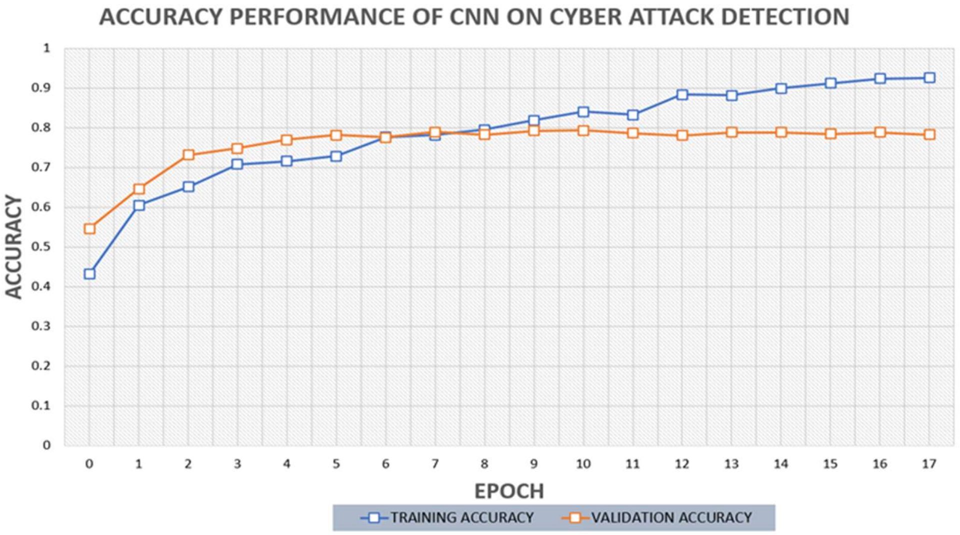


Figure 3. Accuracy graph of the CNN algorithm

Though the accuracy of the model is quite low during the initial epochs, it increases as the number of epochs increases and it reaches 90% during the fourteenth epoch. But during validation, the accuracy stays lower than 80% throughout the process. The loss graph of the same model is shown in figure 4.

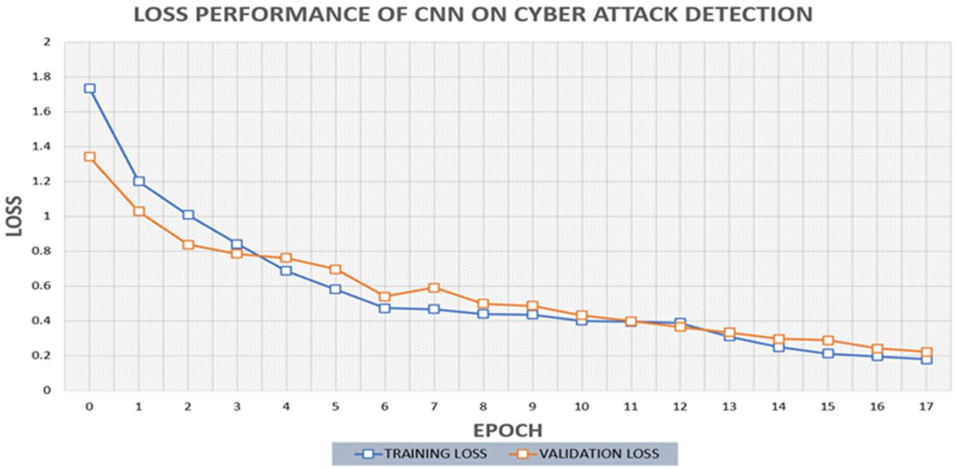


Figure 4. Loss graph of the CNN algorithm

The loss value of the model is extremely high during the initial epochs. But it decreases and reaches its lowest during the final epochs of both training and validation. The accuracy graph of the HANN algorithm is shown in figure 5.

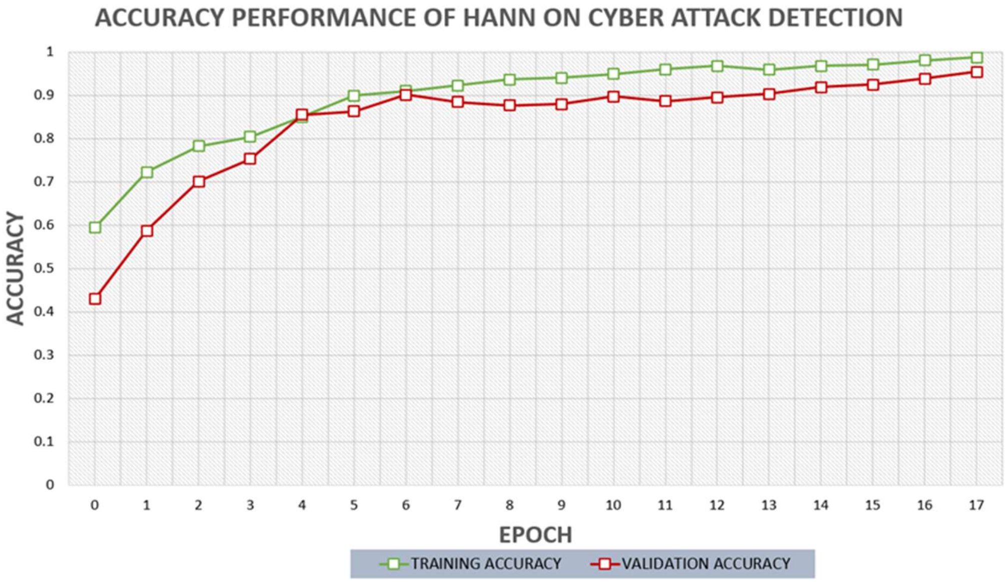


Figure 5. Accuracy graph of the HANN algorithm

The accuracy of the model developed using the HANN algorithm is quite higher than the accuracy of the CNN algorithm. The loss graph of the HANN algorithm is shown in figure 6.

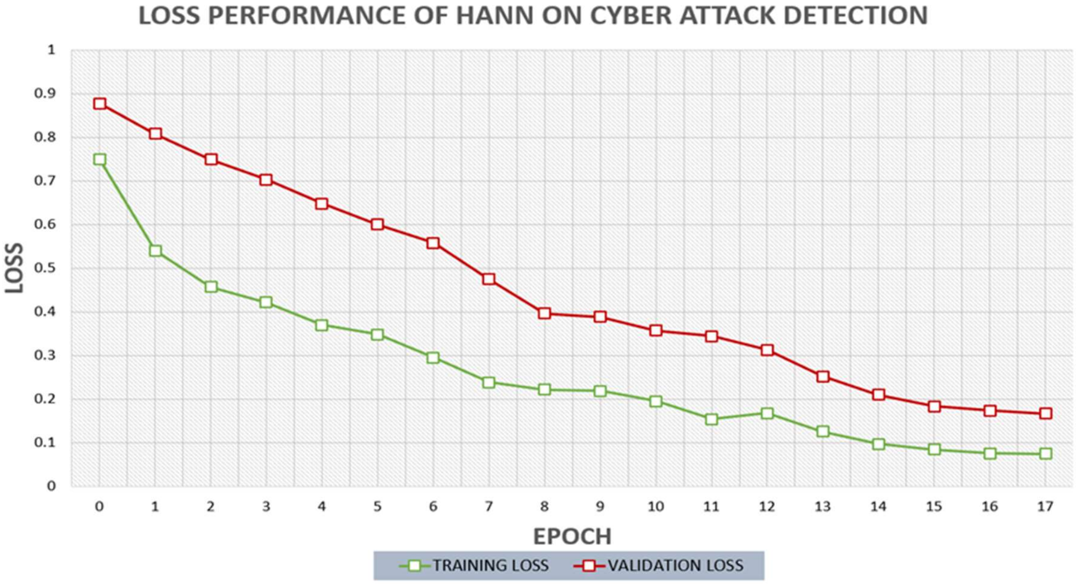


Figure 6. Loss graph of the HANN algorithm

The loss value is also relatively very much smaller when compared to the initial loss values of the CNN algorithm. After training and validation, the models are tested for results. Unlike the prior processes, the testing involves parameters like recall, precision, and F1-score. The results are obtained and tabulated. The tabulated results are then plotted into a graph for easier analysis. Figure 7 explains the final test results of both algorithms.

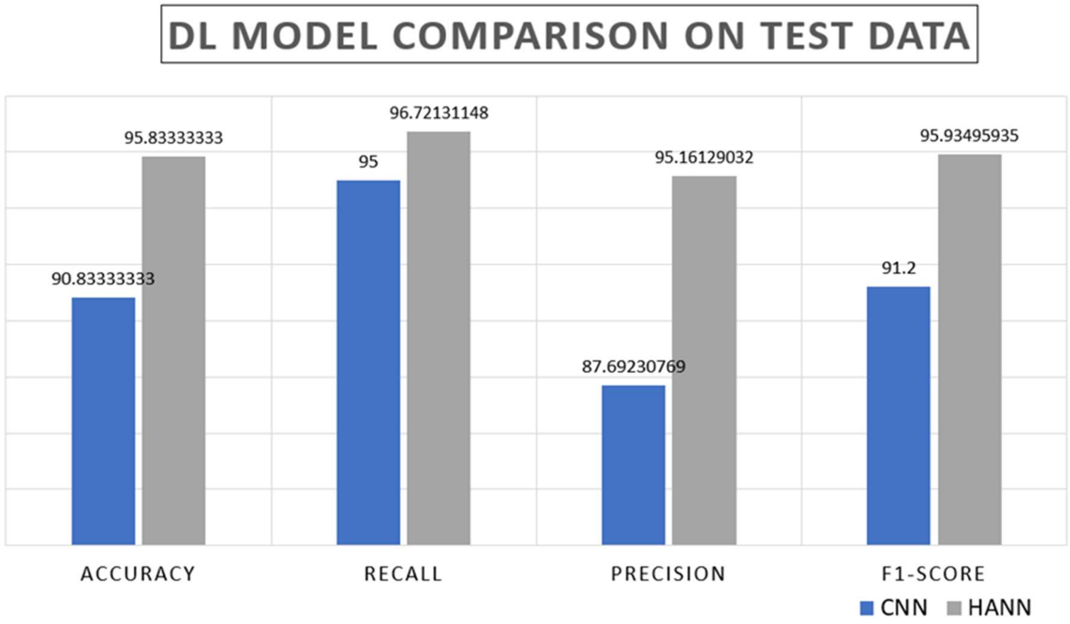


Figure 7. Test results of the DL models

From figure 7, the HANN model has a noticeable advantage over the CNN algorithm in the case of all parameters.

VII. CONCLUSION

A database containing more than 40 features connected to the identification of a cyberattack is created using the NSL-KDD dataset. The database is preprocessed to ensure proper performance. The preprocessing includes normalization, data encoding and statistical featuring. The training and testing components of the preprocessed dataset are then separated. Two different DL models were produced by two different algorithms. The algorithms used in this investigation are CNN and HANN. After the DL models have been trained and put to the test, the best one that can be used to detect a cyberattack is found. During training, both models portrayed different types of performance. The model developed using the CNN algorithm had a growth in accuracy values almost linearly and reaches a point with an accuracy higher than 90% after the 14th epoch. However, the model developed using the HANN algorithm reaches an accuracy higher than 90% after the 6th epoch itself. The highest loss value of the HANN model is a little lesser than 90% during the first epoch of training. The same pattern repeats during all epochs of validation for both models. During testing, the final accuracy of the model developed using the CNN algorithm is 90.8% and the accuracy of the HANN model is 95.8%. In the end, it can be concluded that the HANN algorithm is a better algorithm than the CNN in detecting cyber-attack. In the future, this model can be deployed into a backend processor for a website which can be used to check the authenticity of other websites and software.

REFERENCE

[1]. I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen and P. Palensky, "Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs," 2022

10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy, 2022, pp. 1-6, doi: 10.1109/MSCPES55116.2022.9770140.

[2]. H. Li, X. He, Y. Zhang and W. Guan, "Attack Detection in Cyber-Physical Systems Using Particle Filter: An Illustration on Three-Tank System," 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 2018, pp. 504-509, doi: 10.1109/CYBER.2018.8688281.

[3]. X. Fu, M. Niu and G. Wen, "Detection of Stealthy Cyber-attack in Distributed DC Microgrids Based on LSTM Neural Network," 2021 International Conference on Neuromorphic Computing (ICNC), Wuhan, China, 2021, pp. 8-13, doi: 10.1109/ICNC52316.2021.9608150.

[4]. O. Jacq, D. Brosset, Y. Kermarrec and J. Simonin, "Cyber attacks real-time detection: towards a Cyber Situational Awareness for naval systems," 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 2019, pp. 1-2, doi: 10.1109/CyberSA.2019.8899351.

[5]. Q. Wang, Z. Liu and Y. Tang, "Design of a Co-Simulation Platform with Hardware-in-the-Loop for Cyber-attacks on Cyber-Physical Power Systems," 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Suzhou, China, 2019, pp. 430-434, doi: 10.1109/CYBER46603.2019.9066575.

[6]. A. Yeboah-Ofori, S. Islam and A. Brimicombe, "Detecting Cyber Supply Chain Attacks on Cyber Physical Systems Using Bayesian Belief Network," 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 2019, pp. 37-42, doi: 10.1109/ICSIoT47925.2019.00014.

[7]. "NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB," Unb.ca, 2020. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html. [Accessed: 21 October 2020].

[8]. E. R. Hutchison, Y. Zhang, S. Nampally, J. Weatherall, F. Khan and K. Shameer, "Uncovering Machine Learning-Ready Data from Public Clinical Trial Resources: A case-study on normalization across Aggregate Content of ClinicalTrials.gov," 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Seoul, Korea (South), 2020, pp. 2965-2967, doi: 10.1109/BIBM49941.2020.9313362.

[9]. C. L. Felton, B. K. Gilbert and C. R. Haider, "Data Compression via Low Complexity Delta Transition Lossless Encoding for Remote Physiological and Environmental Monitoring," 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Honolulu, HI, USA, 2018, pp. 4379-4384, doi: 10.1109/EMBC.2018.8513277.

[10]. "Competence Investigation of Noise Detecting Procedure Found on TTSD (Triple Threshold Statistical Detection) filter for SPN," 2019 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia), Bangkok, Thailand, 2019, pp. 52-55, doi: 10.1109/ICCE-Asia46551.2019.8942190.

[11]. K. B. Lee and H. S. Shin, "An Application of a Deep Learning Algorithm for Automatic Detection of Unexpected Accidents Under Bad CCTV Monitoring Conditions in Tunnels," 2019 International Conference on Deep Learning and Machine Learning in Emerging

Applications (Deep-ML), Istanbul, Turkey, 2019, pp. 7-11, doi: 10.1109/Deep-ML.2019.00010.

[12]. S. N. Pakanzad and H. Monkaresi, "Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks," 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 2020, pp. 1-6, doi: 10.1109/ICEE50131.2020.9260686.

[13]. H. Jin, I. Kang, G. Choi, D. D. Molinaro and A. J. Young, "Wearable Sensor-Based Step Length Estimation During Overground Locomotion Using a Deep Convolutional Neural Network," 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Mexico, 2021, pp. 4897-4900, doi: 10.1109/EMBC46164.2021.9630060.

[14]. A. M. Almars, M. Almaliki, T. H. Noor, M. M. Alwateer and E. Atlam, "HANN: Hybrid Attention Neural Network for Detecting Covid-19 Related Rumors," in IEEE Access, vol. 10, pp. 12334-12344, 2022, doi: 10.1109/ACCESS.2022.3146712.

[15]. Z. Liu, C. Lu, H. Huang, S. Lyu and Z. Tao, "Hierarchical Multi-Granularity Attention-Based Hybrid Neural Network for Text Classification," in IEEE Access, vol. 8, pp. 149362-149371, 2020, doi: 10.1109/ACCESS.2020.3016727.