Artificial Intelligence and Machine Learning in Healthcare Cybersecurity of Current Applications and Future Directions

Nidhi Mishra[1], Ghorpade Bipin Shivaji[2], Sheetal Sachin Barekar[3],Sukhvinder Singh Dari[4], Dharmesh Dhabliya[5], Mukesh Patil[6]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.*

KEYWORDS

Cyber Security, Health, Security, Privacy, WSN.

ABSTRACT

Data communication has increased due to the growth of technology-driven services and application deployment. Because there are always security risks to networks, the increasing throughput of networks has also increased the likelihood of cybercrimes. Additionally, the abrupt end of the COVID crisis, which caused nearly all services to go online, has increased awareness of the threat posed by cyberattacks in general. Thus, in the information and technology-driven world of today, reliable communication is crucial. The network is frequently discovered to be vulnerable to a variety of network attacks, such as spoofing, malware, and DDoS attacks. The difficulties caused by intrusions have also been covered in the current work, along with the methods to prevent and detect these kinds of intrusion attempts that have been under investigation for the past few years. Research needs have been identified by presenting and analysing the body of literature currently available on IDS. A hybrid approach has been suggested based on the information to provide a secure communication mechanism and protect the network from intruders. A cyber security strategy based on ABC and 3D CNN architecture is suggested as a solution to this. The qualities that reflect malware and DDoS attack aspects are chosen and optimised using the ABC. Neural networks are trained and classified using the retrieved data. The accuracy, recall, and f-measure analysis of the suggested cyber security method for malware and DDoS node detection were assessed. Comparative investigation demonstrated that the cyber security method was more effective at identifying network attacks.

1. Introduction

Malware that encrypts data on a victim's computer and demands money to be unlocked is known as ransomware. The victim's access rights were restored following a successful payment. Ransomware is the concern of IT professionals, cyber security analysts, and experts. Cybercrime including ransomware program attacks is increasing [1]. To safeguard their companies against cyber assaults, IT specialists and business owners must have a solid recovery plan. This entails reporting any violations of the Reportable Data Violations scheme, as well as making the necessary corporate and recovery plans for the client's data and applications [6]. Out of all the cyberthreats, it is the cybercrime that is expanding the fastest. Most ransomware does is encrypt files or prevent users from accessing a machine or network. Once inside, the hacker demands money in exchange for sensitive data that is vital to the company. Apart from the individuals who have lost their data, financial and productivity losses also pose a significant issue in these situations [2]. "Internet of Things" is referred to as IoT. It is a network of physically connected objects that are accessible over the Internet. Every physical gadget has a unique ID and can send data without the need for human assistance [3]. Due to the wireless transmission of data, there is a possibility of information loss, which could result from a cyberattack [12]. AI works in tandem to prevent and stop cyberattacks. AI altered the course of history by acting not only defensively but even offensively. One of the most significant applications of artificial intelligence is biometrics. After much study and modelling, AI is now able to identify behavioural anomalies that can be used as a defensive mechanism [9]. Unfortunately, these same techniques can also be used by thieves, hackers, or hunters to launch a cyberattack. Over the past ten years, a variety of monitoring and avoidance technologies have been developed to combat threats on computer networks. Finding these systems is essential to choosing the appropriate mitigating technique for enterprises with a variety of network infrastructures and security requirements [4]. In this section, we'll go over the processes used to analyse malware and respond to network threats. Vulnerabilities are typically used by attackers to target a collection of computer networks. Attacks that are initiated by malicious programs have a higher chance of success because malware attacks start when certain conditions are met by computer networks and systems. Because of this, it's critical to locate and remove malware from computer networks [5]. The best security mechanism keeps malware from interfering with computer network operations; that is, it keeps bad software out of particular networks or renders it incapable of interfering with computer networks. Actually, it is challenging to accomplish this goal because of how active current computer networks are and how many people and cyber systems they must communicate with. Prevention mechanisms, also referred to as the best backup defence for computer networks, consist of policy, awareness, vulnerability reduction, and threat mitigation. [11].

2. Methodology

The architecture of the proposed model is shown in Figure 1. The chapter covered a variety of AI and ML methods that are frequently employed in the creation of cyber security strategies. The difficulties with cyber security and various kinds of cyberattacks were also covered. A preliminary work flow for security mechanisms utilising ABC-3DCNN is also shown, which will aid in the development of a strong hybrid strategy that combines swarm-based meta heuristic algorithms for feature optimisation with additional classifiers for enhanced efficacy. [7].

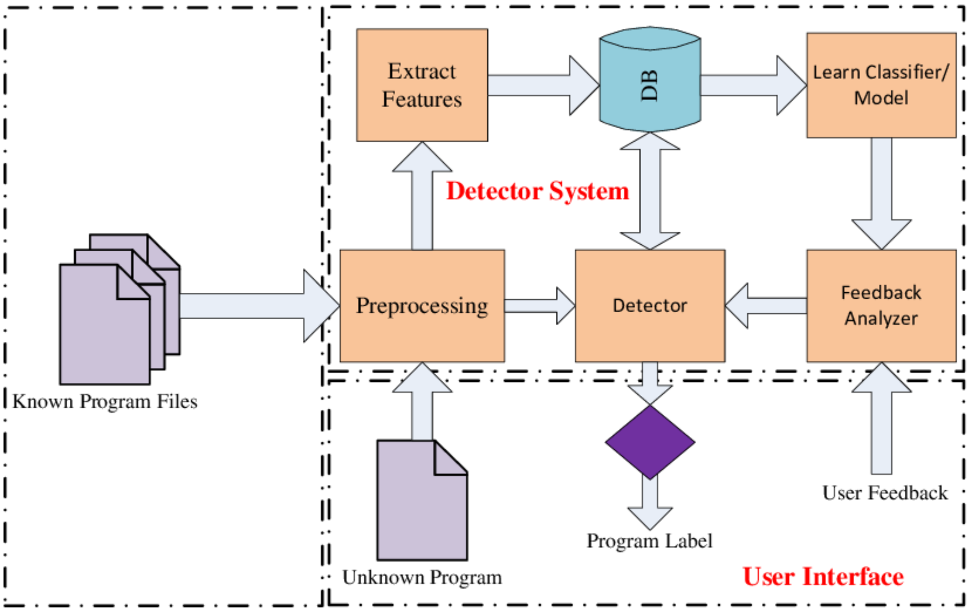

Figure 1. Schematic Diagram of proposed framework

The algorithm initially preprocesses the data files. Then the attributes are selected algorithms with ABC [8] are employed to ascertain the relative importance of the qualities. Radial-based function networks can be used to locally represent an N-dimensional space. It is executed by the control zone, which is confined by baseline functions. The requirements for this baseline function are calculated by

$$\varphi_j(x) = \exp\left(\frac{\|x-\mu_j\|^2}{2\sigma^2{}_j}\right) \qquad (1)$$

Where $\mu_{\ j}$ reference vector and $\sigma_j\ is\ the$ circumstances of the influence field

Each 3D-CNN unit that can be expressed mathematically as a function of a radial basis

$$\varphi_j(x) = \varphi(\|x - x_j\|) \qquad j = 1,2,\ldots N \qquad (2)$$

Where N represents the dimension of the preparation model and $(\|x - x_j\|)$is the Euclidean norm of the vector $(x - x_j)$. The Jth input data point x_j determines the RBF center, and the pattern vector x is added to the input layer. Gaussian function is used in the hidden layer of the network as the radial basis function in which each computing unit is located.

$$\varphi_j(x) = \varphi(x - x_j) = \exp\left(-\frac{1}{2\sigma_j^2}\|x - x_{\ j}\|^2\right) \qquad j = 1,2,\ldots N \qquad (3)$$

Where, j is a measure of the width of the Gaussian jth function with $x_j$center. All the Gaussian hidden units are usually, but not always, allocated a specific width.

The hybrid approach to addressing cybersecurity concerns leverages machine learning and deep learning techniques as well as optimisation methods inspired by nature. The selection criteria ABC has been applied to pick relevant features from the huge dataset. Next, the features that aren't relevant are filtered away using ABC. Lastly, 3DCNN is employed to classify attacks and normal [13][10].

3. Results And Discussion

No technique other than machine learning could have been considered to reduce the computation complexity of the identification network to shield the system from potential threats in the future. There are two methods for learning in machine learning: the statistical approach and the experience approach. While the experience approach seeks to learn from decision-making, the statistical approach seeks to address the problem through quantitative expression. Presenting the real-time categorisation exercise was intended to aid in the identification of cyberattacks. The recommended ABC with 3D-CNN was executed on a single Windows 7 Virtual Machine (VM). Our approach uses the KDD Dataset to identify malware and DDoS attacks.

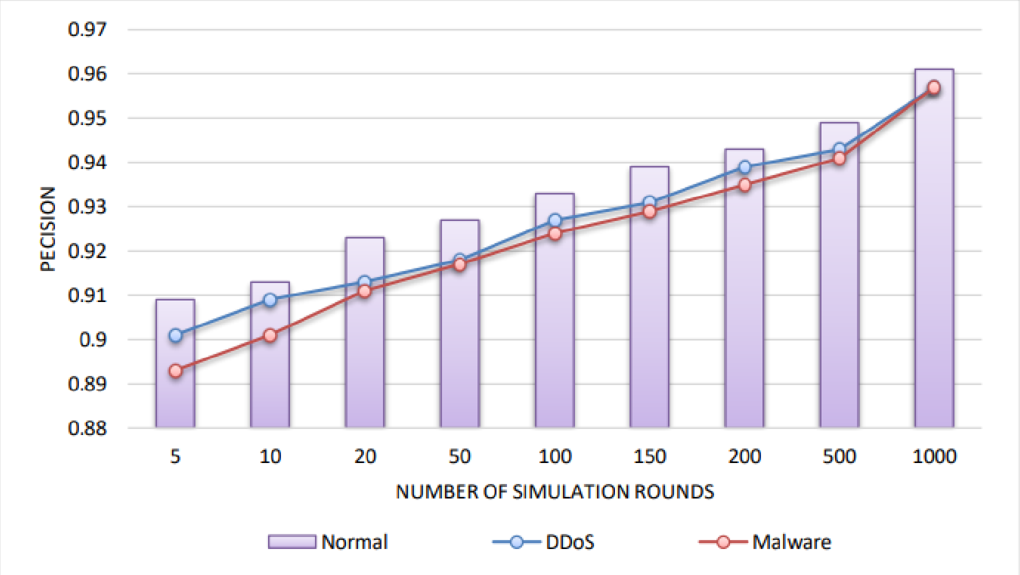

Figure 2. Precision Analysis of Cyber Security Approach

The accuracy analysis of individual attacks compared to the average situation is shown in Figure 2. In practically all simulation rounds, it is found that the accuracy of DDoS attack detection is far closer to the typical situation than that of malware attack detection. The maximum average precision for DDoS attack detection is found to be 0.926, while the regular scenario's observed precision is 0.933. Malware attack detection has an average precision of 0.923.

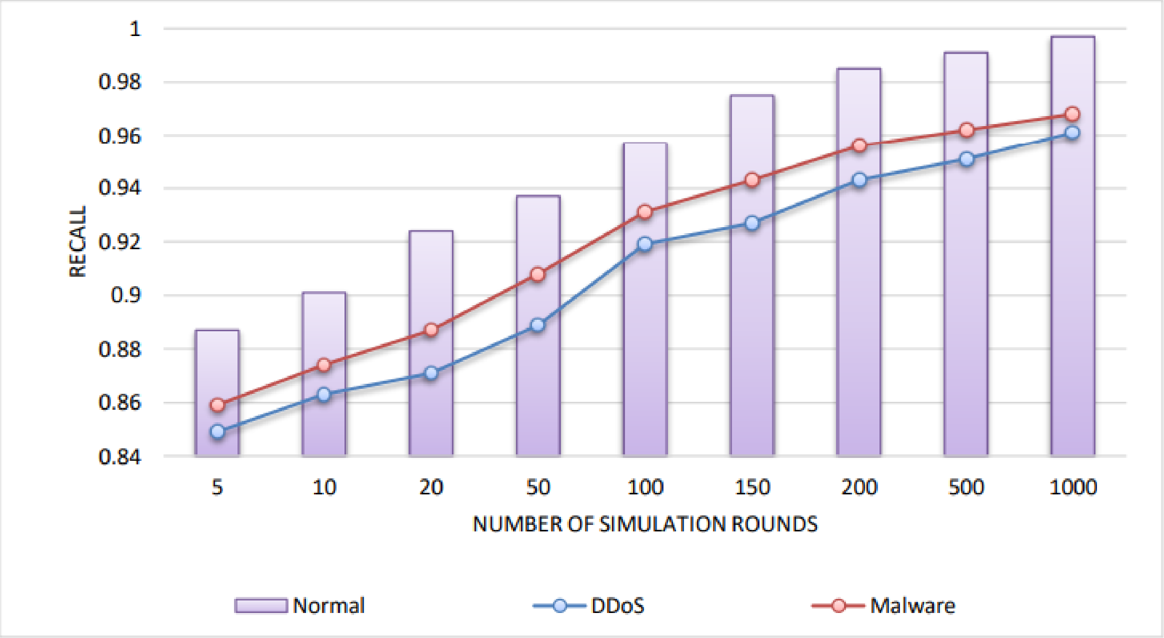

Figure 3. Recall Analysis of Cyber Security Approach

Recall rises from 0.849 to 0.961 in the event of a DDoS attack, from 0.859 to 0.968 in the case of a malware attack, and from 0.869 to 0.984 in the case of a spoofing attack. The recall fluctuation for simulation rounds ranging from 5 to 1000 is depicted in Figure 3. For every simulation round that was examined, the recall of DDoS was found to be extremely similar to the typical situation, as Figure 3 illustrates. The average recall for malware and DDoS has been found to be 0.920 and 0.908, respectively. Between the two attacks, DDoS's recall is extremely similar to the typical scenario's average recall of 0.950.

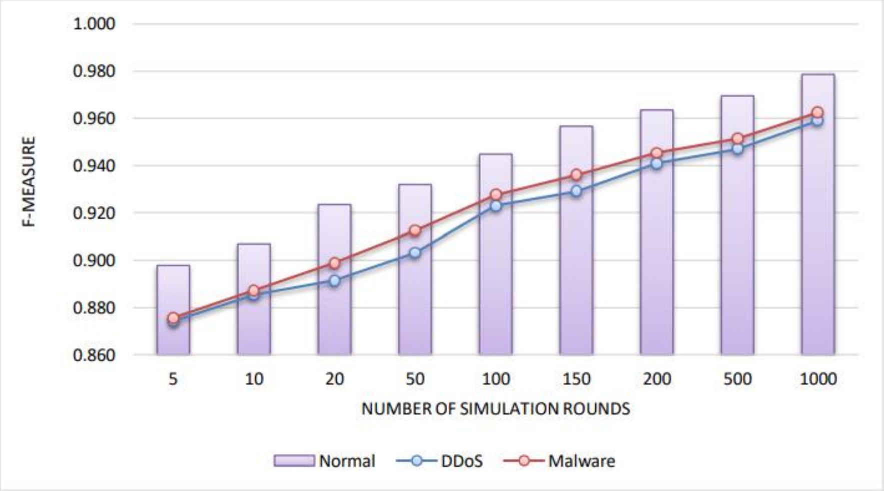

Figure 4. F-measure Analysis of Cyber Security Approach

F-measure, which is the harmonic mean of recall and precision, is often thought to follow the same trend as recall and precision. Initially, during analysis conducted for five simulation rounds, f-measures of 0.874, 0.876, and 0.898 were observed for DDoS, malware, and normal, respectively. The f-measure then rises to 0.959, 0.962, and 0.979 for DDoS, malware, and normal, respectively, until the end of 1000 simulation rounds. Figure 4 presents a graphic representation of the f-measure variation for each of the three situations for each simulation round that was employed in the experiment. Figure 5 displays a comparative comparison of DDoS attack detection accuracy. It has been found that the accuracy of

DDoS attack detection utilising hybrid technique is 94.68% when a study of simulations with 10 nodes is carried out, 87.54% when Dong et al. are used, and 90.17% when Jaber and Rehman are used.

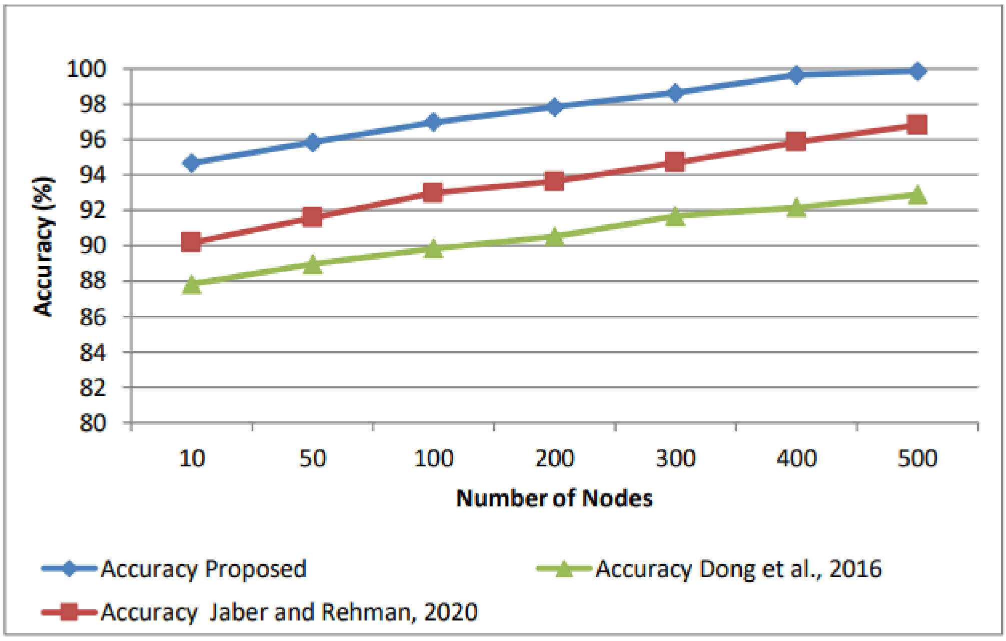

Figure 5. Accuracy comparison of DDOS Attack detection

We used the most recent and well-established ML and DL model to evaluate our model's accuracy. This was demonstrated with exceptional precision in the experiment using the NIC dataset. The suggested model is shown in Figure 6 next to the traditional model.

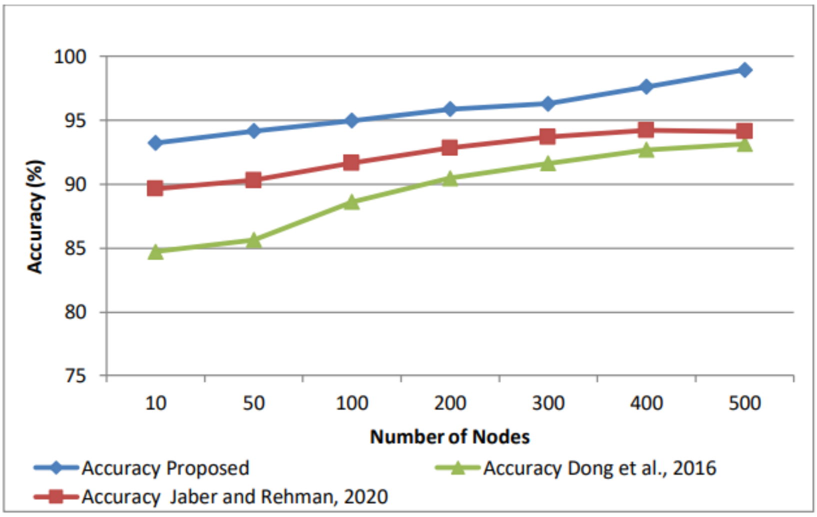

Figure 6. Accuracy comparison of Malware Attack detection

In order to show the viability and potential of utilising machine learning skills for attack prediction and CNN for attack detection through data analytics and deep learning, we conducted an experiment.

4. Conclusions

The accuracy, recall, and f-measure analysis of the suggested cyber security method for malware and DDoS node detection were assessed. The comparative research revealed that the cyber security method was more effective at identifying network attacks. The DL and methods inspired by nature are then combined in a hybrid approach that is suggested. The application of the ABC results in reduced data set sizes and feature selection. The application of ABC is then used to further remove any extraneous features from the data. In the end, the CNN-ABC hybrid is utilised for both the training and classification stages, with CNN being employed for training and 3DCNN for classification. Hundreds of simulation rounds were used in the simulation study to ensure that the hybrid technique exhibited low FPR with high TPR, detection rate, precision, and f-measure. Another preventive technique that is suggested to show throughput and PDR is assessed by changing the number of nodes in comparison to previous studies.

Reference

[1] Lechner, Nadica Hrgarek. "An overview of cybersecurity regulations and standards for medical device software." In *Central European Conference on Information and Intelligent Systems*, pp. 237-249. Faculty of Organization and Informatics Varazdin, 2017.

[2] Lee, Chien-Ding, Kevin I-J. Ho, and Wei-Bin Lee. "A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations." IEEE Transactions on Information Technology in Biomedicine 15, no. 4 (2011): 550-556.

[3] Kodric, Z., Vrhovec, S., & Jelovcan, L. (2021). Securing edge-enabled smart healthcare systems with blockchain: A systematic literature review. Journal of Internet Services and Information Security, 11(4), 19-32.

[4] Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. "Muddling through cybersecurity: Insights from the US healthcare industry." Business horizons 62, no. 4 (2019): 539-548.

[5] Marotta, Angelica, and Stuart Madnick. "Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case." Issues in Information Systems 23, no. 1 (2022).

[6] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[7] Kelly, Brendan, Conor Quinn, Aonghus Lawlor, Ronan Killeen, and James Burrell. "Cybersecurity in Healthcare." Trends of Artificial Intelligence and Big Data for E-Health (2023): 213-231.

[8] Busdicker, Mike, and Priyanka Upendra. "The role of healthcare technology management in facilitating medical device cybersecurity." Biomedical Instrumentation & Technology 51, no. s6 (2017): 19-25.

[9] George, Reny, et al. "Some existential fixed point results in metric spaces equipped with a Graph and it's application." *Results in Nonlinear Analysis* 7.1 (2024): 122-141.

[10] Komisarek, M., Pawlicki, M., Kozik, R., & Choras, M. (2021). Machine Learning Based Approach to Anomaly and Cyberattack Detection in Streamed Network Traffic Data. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12(1), 3-19.

[11] Nifakos, Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. "Influence of human factors on cyber security within healthcare organisations: A systematic review." Sensors 21, no. 15 (2021): 5119.

[12] Kwon, Juhee, and M. Eric Johnson. "Healthcare security strategies for regulatory compliance and data security." In 2013 46th Hawaii International Conference on System Sciences, pp. 3972-3981. IEEE, 2013.

[13] Anderson, Scott, and Trish Williams. "Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?" Computer Standards & Interfaces 56 (2018): 134-143.

[14] Thomasian, Nicole M., and Eli Y. Adashi. "Cybersecurity in the internet of medical things." Health Policy and Technology 10, no. 3 (2021): 100549.