ISSN: 2959-6386 (Online), Volume 2, Issue 3

Journal of Knowledge Learning and Science Technology

Journal homepage: https://jklst.org/index.php/home

Unifying Assurance A Framework for Ensuring Cloud Compliance in AIML Deployment

Samir Vinayak Bayani[1], Sanjeev Prakash[2], Jesu Narkarunai Arasu Malaiyappan[3]

[1]Broadcom Inc, USA

[2]RBC Capital Markets, USA

[3]Meta Platforms Inc, USA

Abstract

Intrusion poses a significant challenge in Cloud networks, necessitating the development of efficient mechanisms to mitigate intrusions and enhance system security. To address this, we propose a novel Artificial Bee-based Elman Neural Security Framework (ABENSF). This framework involves rescaling the raw dataset using preprocessing functions and integrating an optimal fitness function based on artificial bees into the feature extraction phase to identify and extract attack features. Additionally, the monitoring mechanism in ABENSF enhances network security by proactively preventing attacks. By employing tracking and monitoring functions, known and unknown attacks can be effectively thwarted. We validate the proposed framework using the NSL-KDD dataset in Python software and conduct a comparative analysis to assess its performance against existing techniques. Our results demonstrate that the developed model outperforms other methods in terms of attack prevention and overall security enhancement.

Keywords: Attack prevention; Security framework; Cloud computing; Neural Network; Internet of Things; Cloud storage

Article Information:
Article history: Received: 01/11/2023 Accepted:3/11/2023 Online: 12/11/2023 Published: 12/11/2023
DOI: https://doi.org/10.60087/jklst.vol2.n2.p472

[i] ***Correspondence author: Samir Vinayak Bayani***

Introduction

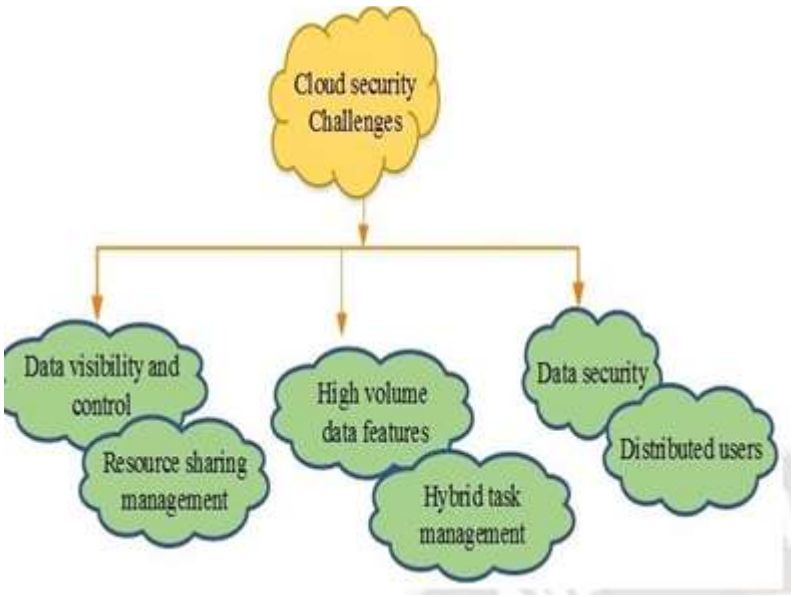
The concept of cloud computing has evolved from distributed software architecture [1]. Similar to traditional computing, cloud computing is designed to ensure resource availability across various categories [2]. Through immersive virtualization, cloud computing has become a genuine computing platform that allows dynamic, scalable, and elastic reconfiguration of computing resources as needed [3]. It enables the expansion of resources without requiring in-depth knowledge of new systems, training new employees, or developing new software [4].

Cloud service providers (CSPs) offer software computing, infrastructure, and platforms, including Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) [5]. These services can be deployed in various models such as community, hybrid private, and public clouds [6]. IaaS offers compelling options for High-Performance Computing (HPC) and empowers cloud users to customize all aspects of their resources on the cloud. Major players in the IaaS sector include Amazon and Microsoft Azure cloud [8].

Platform as a Service (PaaS) facilitates the deployment, management, and scaling of new applications. It provides features such as managed storage solutions, data services, and a robust environment for deploying and operating new applications [9]. In Software as a Service, application services are delivered via cloud infrastructure and are

provided and billed on a subscription basis [10]. With the advent of wireless system-assisted computing, numerous real-world scenarios have been collected and stored in the cloud [11]. The cloud's capacity is leveraged to analyze these datasets and derive effective solutions, often utilizing machine learning algorithms [12].

Data collected from various sources is transmitted to base stations to optimize radio efficiency. In scenarios where base stations are deployed in new locations, historical data may not be available. In such cases, real-time data collected from the system is used as surrogate historical data for learning purposes [15]. Historical data often contains attributes such as user numbers, Channel State Information (CSI), and International Mobile Subscriber Identification Numbers (IMSIs), some of which may be irrelevant for resource allocation purposes. Therefore, data preprocessing techniques are applied to extract relevant information without compromising data quality [16]. However, there may be imperfections in data measurements, transmission, storage, and feature vectors, resulting in partial and incomplete datasets [17]. Typically, 70 to 90% of the feature vectors are allocated to the training set [18].



The productivity model and associated solutions were deployed to the base stations [19]. At the base station, the measured data were used to create new characteristic vectors. These vectors temporarily stored the data before being forwarded to the cloud [20]. One of the primary security concerns in cloud computing is unauthorized access to data within the virtualized infrastructure, particularly when multiple operations are hosted on the same server. Additionally, cloud services may become inaccessible due to errors and crashes [21, 22]. Various security models,

including neural networks [24] and boosting mechanisms [25], have been implemented in the past. However, security challenges persist due to the complexity of the data. Therefore, the present study aims to develop an optimal solution for predicting malicious activities in trained cloud IoT networks.

Literature Review

Several recent studies have explored the intersection of cloud computing and machine learning.

Cloud computing represents a significant technological advancement, offering benefits such as online storage, scalability, and accessibility. However, its widespread adoption also brings security challenges. Mohammad et al. [25] proposed a machine learning-based approach to address security and data transmission issues in cloud computing. Their method leverages big data analysis to enhance security and data transmission rates. While big data analysis offers advantages such as high accuracy and performance, it also entails high service costs and unexpected outages.

In the healthcare sector, cloud computing has become integral to improving healthcare service delivery. Abdelaziz et al. [26] introduced a cloud-based healthcare model employing Parallel Particle Swarm Optimization for virtual machine selection. This model facilitates chronic kidney disease analysis and prediction using neural network (NN) and linear regression (LR) methods. Despite the benefits of cloud data centers for healthcare services, data breaches and verification delays remain significant challenges.

The development of sustainable smart cities necessitates effective expertise management and development. Iatrellis, Omiros et al. [27] proposed a cloud-based IT approach to enhance personnel and technical workforce management. This approach integrates cloud-based IT systems with expert systems to provide relevant competencies to smart cities. However, concerns persist regarding data integrity and illegal data usage.

The emergence of the Internet of Things (IoT) has introduced new challenges, including security issues similar to those in cloud computing. Stergiou et al. [28] highlighted the security challenges facing IoT and cloud computing,

particularly concerning wireless telecommunication systems. Despite the potential benefits of wireless networks for IoT applications, challenges such as power dependence, high costs, and technical complexity remain.

These studies underscore the importance of addressing security and data management challenges in cloud computing, healthcare, smart cities, and IoT applications through innovative machine learning-based approaches.

The primary contributions of this study are outlined as follows:

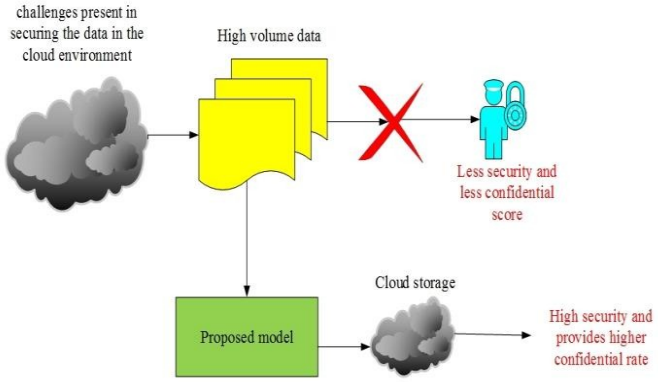
- Initially, IoT cloud intrusion data was collected and imported into the Python environment.
- Subsequently, a novel ABENSF (Artificial Bee-based Elman Neural Security Framework) was developed, incorporating essential feature extraction and parameters for forecasting malicious events.
- Furthermore, noise present in the data was filtered out during the initial preprocessing phase.
- Following noise filtering, the features were analyzed, and malicious features were accurately classified.
- Upon identification of malicious features, appropriate measures were taken to mitigate their impact on the network cloud environment.
- Finally, the robustness of detection was evaluated using metrics such as precision, accuracy, F-measure, recall, and error rate.

System Model And Problem Statement

Ensuring the security of cloud networks is paramount for safeguarding user data privacy in wireless network environments. While numerous security models have been introduced in the past to uphold the privacy of cloud systems, the unstructured nature of each user's data has introduced a range of complexities in data security. Fixed security protocols often fail to adequately address the security needs of unstructured user data, resulting in lower confidentiality scores for cloud-based IoT systems. These challenges have prompted the present study to develop an optimal security solution.

The existing models have been plagued by insufficient security measures and low confidentiality scores. To address these shortcomings, the proposed model aims to achieve a higher level of security. While existing models store large amounts of data in cloud environments, they often fail to provide adequate security measures for this data. In

contrast, the proposed model focuses on enhancing security by leveraging IoT datasets. The system model depicting the problem is illustrated in Fig. 2.



Proposed Methodology

The proposed methodology involves the implementation of the novel Artificial Bee-based Elman Neural Security Framework (ABENSF) in IoT cloud wireless networks. The objective of this model is to detect and prevent both known and unknown attacks effectively. By integrating the artificial bee function, the model achieves superior attack prediction and mitigation outcomes. Additionally, intrusion-based wireless cloud data is utilized to validate the effectiveness of the model. To assess the robustness of the proposed model, several unknown attacks are launched, and security parameters are meticulously observed. The proposed architecture is illustrated in Fig. 3.

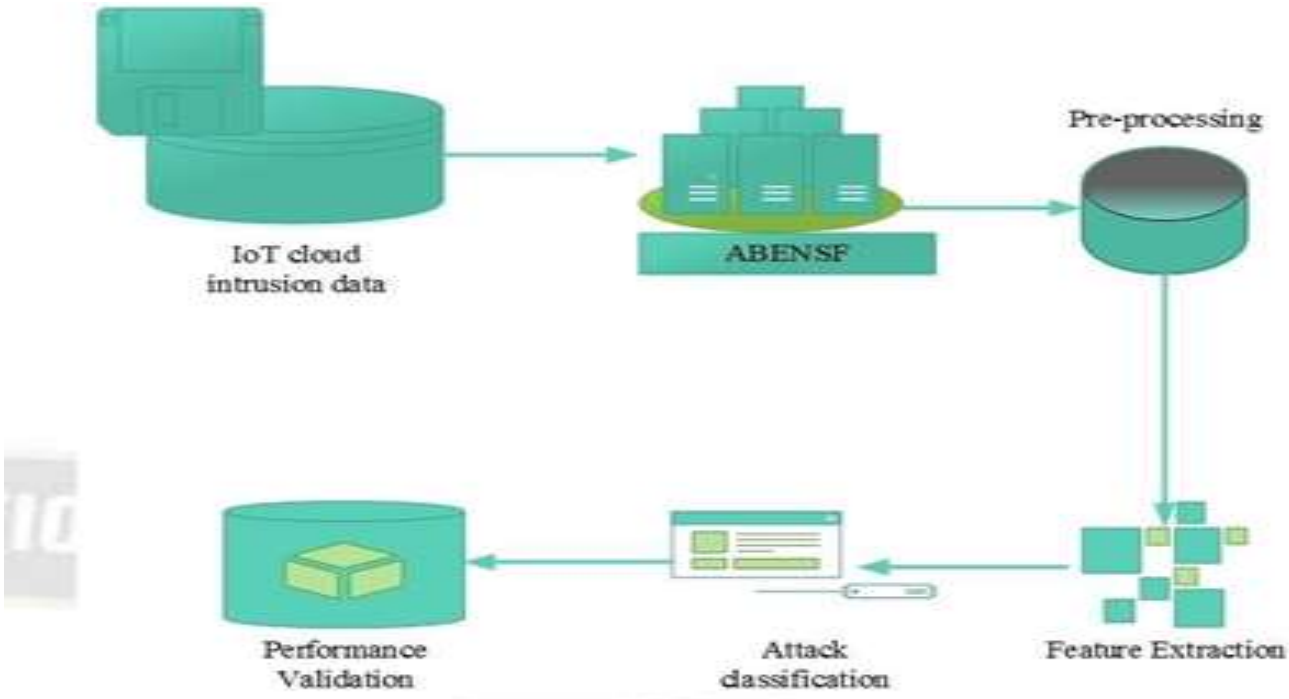


Figure 3. ABENSF Framework

In this study, IoT cloud intrusion data were selected for analysis. The collected data were input into the proposed model, ABENSF. Initially, preprocessing was conducted to eliminate noise features. Following noise removal, feature extraction was performed on the preprocessed data. During this stage, irrelevant and redundant features were extracted, while meaningful features were retained for further processing. Artificial bee optimization techniques were employed to enhance attack prediction and filtering processes. Furthermore, attack classification was carried out after feature extraction. Subsequently, the efficacy of the implemented design was evaluated based on precision, accuracy, F-measure, recall, and error rate.

A. Design of ABENSF Layers

The proposed model was constructed based on the principles of artificial bee optimization and the Elman neural network. It comprises five layers: the input layer, hidden layer, classification layer, optimization layer, and output layer. In the input layer, the IoT-based intrusion dataset was initialized, followed by preprocessing in the hidden layer to eliminate noisy data. Additionally, feature extraction was performed in the classification layer, where irrelevant features were discarded, and the most relevant features were selected based on their fitness assessed by the

artificial bee. The output layer of the model displayed the results based on the chosen features. Figure 4 illustrates the layers of ABENSF.

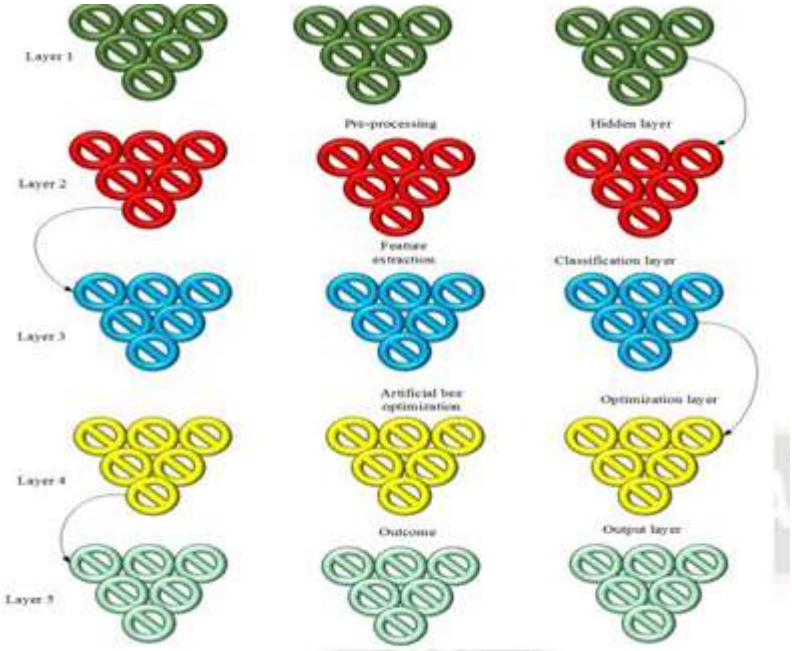


Figure 4. Layers of ABENSF

In this section, we present the results obtained from the implemented model. The proposed model was devised with a focus on enhancing security measures. The performance of the proposed model was evaluated, and a comparative analysis was conducted. Remarkably, the proposed model exhibited a high performance rate compared to other existing models. It is worth noting that the proposed model was developed using the Python platform and executed in a Windows 10 environment.

Result And Discussion

In this section, we present the results obtained from the implemented model. The proposed model was devised with a focus on enhancing security measures. The performance of the proposed model was evaluated, and a comparative analysis was conducted. Remarkably, the proposed model exhibited a high performance rate compared to other existing models. It is worth noting that the proposed model was developed using the Python platform and executed in a Windows 10 environment.

A. Case Study

The case study provides a comprehensive overview of the operational workflow of the proposed model. Initially, the collected dataset underwent preprocessing to refine and cleanse the data. Subsequently, meaningful features were extracted from the preprocessed dataset to enhance security measures. Detection of potential attacks was conducted based on the extracted features, followed by the removal of identified attacks and subsequent classification. Furthermore, preventive measures were implemented to mitigate the risk of future attacks and ensure system security.

To assess the robustness of the system, an unknown attack, specifically brute force attacks, was simulated to evaluate the security efficacy of the design. The overall performance of the system was evaluated in terms of accuracy, precision, recall, F-measure, and error rate.

In this proposed model, three different protocols were identified, with the ICMP protocol being the most widely used, followed by the TCP protocol, and the UDP protocol being the least utilized. The distribution of users across these protocols is illustrated in Figure 6.

The NSLKDD dataset, encompassing various testing and training functions, was employed in this research to measure system strength and predict intrusion patterns.

In this proposed model, "0" represents benign nodes, indicating normal nodes devoid of any malicious activity, while "1" denotes malicious nodes. Initially, the dataset contained a lower proportion of malicious nodes. However, through pre-processing and feature extraction, the prevalence of malicious nodes decreased, thereby enhancing system security in cloud storage. The node identification process of the implemented design is depicted in Figure 7.

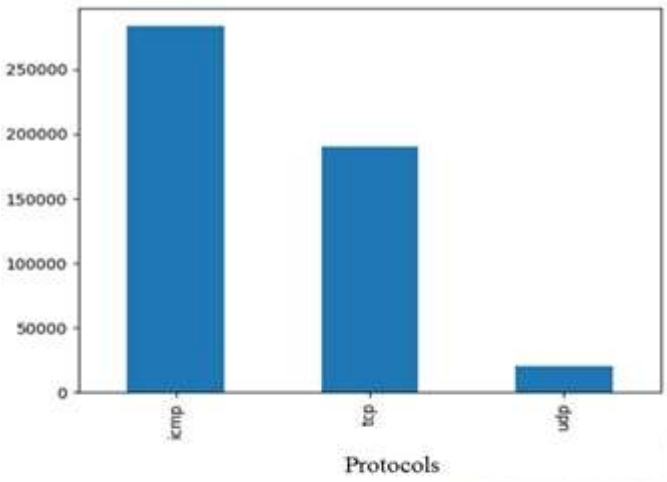


Figure 6. User count in different protocols

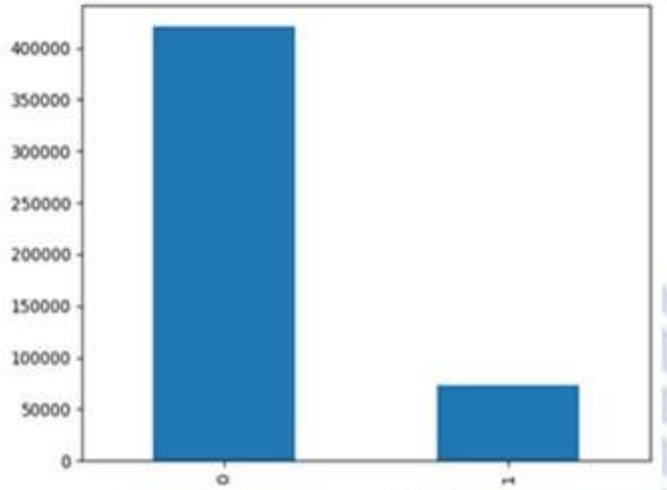
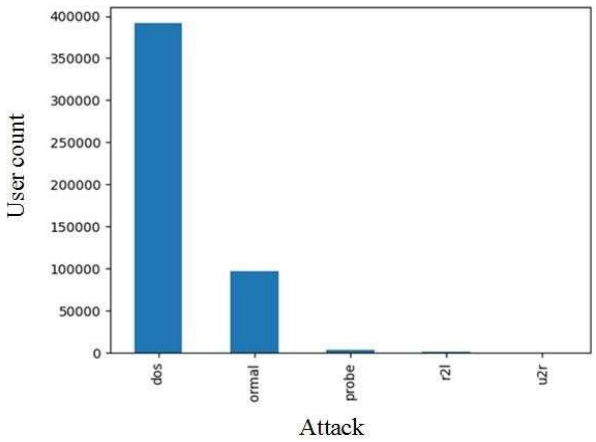


Figure 7. Identification of nodes (0-benign, 1-malicious)

The proposed model effectively categorizes the various attack types within the NSLKDD dataset. Utilizing the features available in the dataset, the attacks were classified into distinct categories, including DoS, normal, probe, r21, and u2r. Figure 8 provides a visual representation of the attack classification within the initialized dataset.



Reducing the size of the dataset resulted in a decrease in the validation loss. Throughout the iterations, both the validation loss and accuracy were monitored. The validation accuracy steadily increased to 100% after 100 iterations, while the validation loss initially increased before gradually decreasing to reach a level close to 0. Figure X illustrates the trends of the validation loss and accuracy over the iterations.

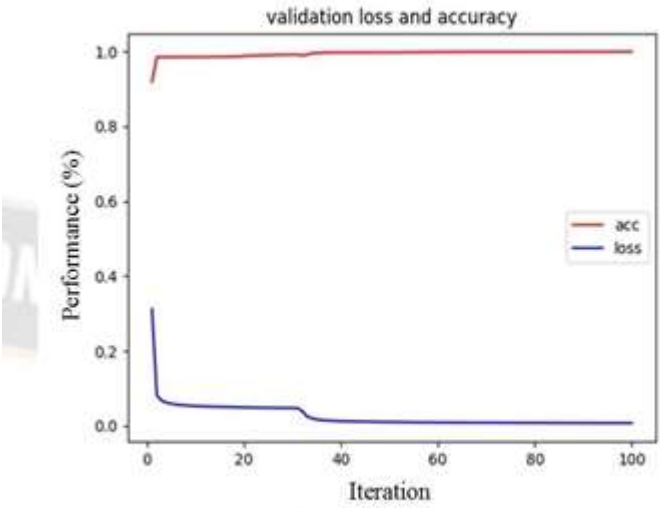
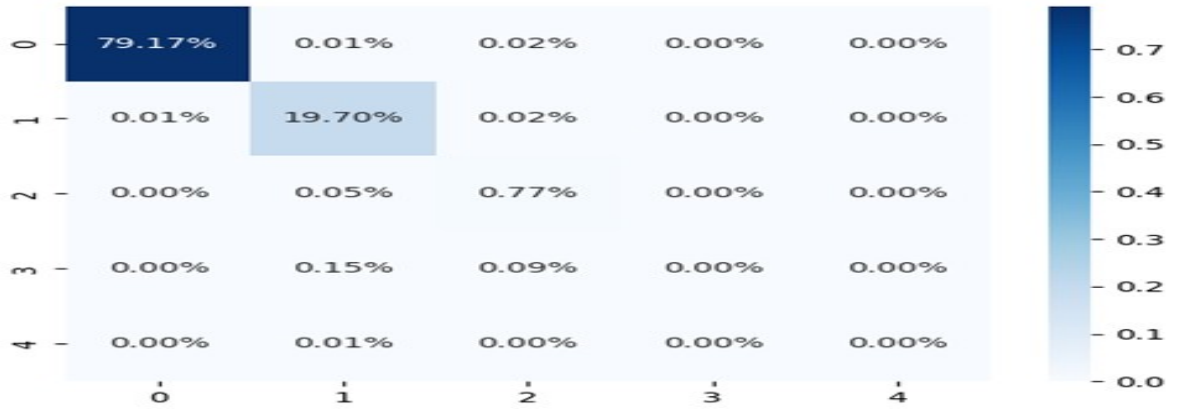


Figure 9. Validation loss and accuracy

The proposed model's classification process was validated using the confusion matrix, which assessed the accuracy of file type classification for each predicted phase. The confusion matrix for the NSL-KDD dataset is depicted in Figure 10.



The correlation matrix was utilized to identify the specific range of attacks within the extensive dataset. Figure 11 illustrates the correlation matrix generated by the proposed model. This matrix represents the overall features contained in the dataset and highlights the highly correlated features, which were subsequently disregarded.

Conclusion

In this study, the ABENSF intrusion detection system was developed with the aim of enhancing security measures. Utilizing an intrusion detection dataset (NSL-KDD), the effectiveness of the proposed approach was evaluated. Initially, the dataset underwent preprocessing to filter out irrelevant data. Subsequently, feature extraction was conducted to identify attack features, with the artificial bee fitness function optimizing this process. Additionally, a monitoring mechanism was integrated to proactively prevent attacks and mitigate intrusion risks.

The robustness of the model was assessed through the launch of an unknown attack (Brute Force Attack). The outcomes were compared and validated through a comprehensive comparative analysis. Furthermore, parameter improvement scores were calculated to gauge the efficacy of the model enhancements. The results indicate a notable improvement across various metrics: accuracy increased by 4%, f-measure by 4%, recall by 4%, and precision by 5%. Remarkably, the developed model achieved an impressively low error rate of 0.0009%.

Conclusively, the developed ABENSF model demonstrates significant enhancements in network security and intrusion avoidance by effectively identifying and mitigating potential attacks.

References :

[1]. Anyoha, R. Exploring the Evolution of Artificial Intelligence. Retrieved from: https://bit.ly/3x2jid7 (accessed on March 3, 2021).

[2]. Marr, B. Unveiling the Remarkable Milestones of Artificial Intelligence. Retrieved from: https://bit.ly/3oLq2s3 (accessed on December 1, 2020).

[3]. West, D.M.; Allen, J.R. Unraveling the Impact of Artificial Intelligence on Our World. Retrieved from: https://brook.gs/3CyGQrp (accessed on December 1, 2020).

[4]. Herpig, D.S. Enhancing the Security of Artificial Intelligence. 2019; p. 48. Retrieved from: https://bit.ly/3nMt2F9 (accessed on September 15, 2020).

[5]. Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; et al. Anticipating, Preventing, and Mitigating the Malevolent Use of Artificial Intelligence. arXiv 2018, arXiv:1802.07228.

[6]. Foremski, T. Investigating Trust Issues with Tech Giants. Retrieved from: https://zd.net/3mCATVe (accessed on May 18, 2021).

[7]. Wang, Y.; Wen, J.; Zhou, W.; Luo, F. Introducing a Novel Dynamic Model for Evaluating Cloud Service Trust in Cloud Computing. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, August 1–3, 2018; pp. 10–15.

[8]. Pillai, A. S. (2023). Advancements in Natural Language Processing for Automotive Virtual Assistants Enhancing User Experience and Safety. *Journal of Computational Intelligence and Robotics*, *3*(1), 27-36.
https://thesciencebrigade.com/jcir/article/view/161

[9]. Sarker, M. (2022). Towards Precision Medicine for Cancer Patient Stratification by Classifying Cancer By Using Machine Learning. *Journal of Science & Technology*, *3*(3), 1-30.
DOI: https://doi.org/10.55662/JST.2022.3301

[10]. Manoharan, A., & Sarker, M. REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION. *DOI: https://www. doi. org/10.56726/IRJMETS32644*.

DOI : https://www.doi.org/10.56726/IRJMETS32644

[11]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.

DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[12]. Hossain, M. I., Bappy, M. A., & Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64

[13]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Fxv3elcAAAAJ&citation_for_view=Fxv3elcAAAAJ:d1gkVwhDpl0C

[14]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.

DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[15]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Implication+of+Artificial+Intelligence+in+Software+Development+Life+Cycle%3A+A+state+of+the+art+review&btnG=

[16]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.

https://patents.google.com/patent/US11762755B2/en

[17]. Miah, S., Rahaman, M. H., Saha, S., Khan, M. A. T., Islam, M. A., Islam, M. N., ... & Ahsan, M. H. (2013). Study of the internal structure of electronic components RAM DDR-2 and motherboard of nokia-3120 by using neutron radiography technique. *International Journal of Modern Engineering Research (IJMER)*, *3*(60), 3429-3432

https://shorturl.at/nCJOQ

[18]. Rahaman, M. H., Faruque, S. B., Khan, M. A. T., Miah, S., & Islam, M. A. (2013). Comparison of General Relativity and Brans-Dicke Theory using Gravitomagnetic clock effect. *International Journal of Modern Engineering Research*, *3*, 3517-3520.
https://shorturl.at/hjm37

[19]. Miah, M. H., & Miah, S. (2015). The Investigation of the Effects of Blackberry Dye as a Sensitizer in TiO2 Nano Particle Based Dye Sensitized Solar Cell. *Asian Journal of Applied Sciences*, *3*(4).
https://shorturl.at/iyJQV

[20]. Miah, S., Miah, M. H., Hossain, M. S., & Ahsan, M. H. (2018). Study of the Homogeneity of Glass Fiber Reinforced Polymer Composite by using Neutron Radiography. *Am. J. Constr. Build. Mater*, *2*, 22-28.
https://shorturl.at/joDKZ

[21]. Miah, S., Islam, G. J., Das, S. K., Islam, S., Islam, M., & Islam, K. K. (2019). Internet of Things (IoT) based automatic electrical energy meter billing system. *IOSR Journal of Electronics and Communication Engineering*, *14*(4 (I)), 39-50.

[22]. Nadia, A., Hossain, M. S., Hasan, M. M., Islam, K. Z., & Miah, S. (2021). Quantifying TRM by modified DCQ load flow method. *European Journal of Electrical Engineering*, *23*(2), 157-163.

https://shorturl.at/csuO3

[23]. Miah, S., Raihan, S. R., Sagor, M. M. H., Hasan, M. M., Talukdar, D., Sajib, S., ... & Suaiba, U. (2022). Rooftop Garden and Lighting Automation by the Internet of Things (IoT). *European Journal of Engineering and Technology Research*, *7*(1), 37-43.
DOI: https://doi.org/10.24018/ejeng.2022.7.1.2700

[24]. Prasad, A. B., Singh, S., Miah, S., Singh, A., & Gonzales-Yanac, T. A Comparative Study on Effects of Work Culture on employee satisfaction in Public & Private Sector Bank with special reference to SBI and ICICI Bank.

[25]. Ravichandra, T. (2022). A Study On Women Empowerment Of Self-Help Group With Reference To Indian Context.

https://www.webology.org/data-cms/articles/20220203075142pmwebology%2019%20(1)%20-%2053.pdf

[26]. Kumar, H., Aoudni, Y., Ortiz, G. G. R., Jindal, L., Miah, S., & Tripathi, R. (2022). Light weighted CNN model to detect DDoS attack over distributed scenario. *Security and Communication Networks*, *2022*.
https://doi.org/10.1155/2022/7585457

[27]. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S. (2022). Optimization of electric automation control model based on artificial intelligence algorithm. *Wireless Communications and Mobile Computing*, *2022*.
https://doi.org/10.1155/2022/7762493

[28]. Devi, O. R., Webber, J., Mehbodniya, A., Chaitanya, M., Jawarkar, P. S., Soni, M., & Miah, S. (2022). The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence. *Scientific Programming*, *2022*.
https://doi.org/10.1155/2022/1473901

[29]. Al Noman, M. A., Zhai, L., Almukhtar, F. H., Rahaman, M. F., Omarov, B., Ray, S., ... & Wang, C. (2023). A computer vision-based lane detection technique using gradient threshold and hue-lightness-saturation value for an autonomous vehicle. *International Journal of Electrical and Computer Engineering*, *13*(1), 347.
https://shorturl.at/ceoyJ

[30]. Patidar, M., Shrivastava, A., Miah, S., Kumar, Y., & Sivaraman, A. K. (2022). An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application. *Materials Today: Proceedings*, *62*, 4880-4890.

https://doi.org/10.1016/j.matpr.2022.03.532