International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Security Protocols Using Artificial Intelligence to Prevent Internet of Things Attacks

[1]Mukesh Rajput, [2]Feon Jaison, [3]Aaditya Jain, [4]Rajeev Mathur

Submitted:18/04/2023 **Revised:**14/06/2023 **Accepted:**22/06/2023

Abstract*:* Intelligent towns and cities, medical care, and automation in industries have all reaped countless benefits from the Internet of Things (IoT) devices quick proliferation. Although anomaly detection is essential for safeguarding the integrity and dependability of IoT systems, the widespread implementation of connected devices also brings new security problems. Bird Swarm-Optimized artificial neural networks (BSO-ANN) are a unique anomaly detection framework presented in this study for IoT contexts. The BSO approach enables the model to look for an ideal network configuration that improves anomaly detection accuracy by mimicking the collective actions of birds in a swarm. The BSO-ANN approach's ability to detect anomalies was assessed using the UNSW-NB15 dataset. The findings show that the BSO-ANN algorithm detects several types of irregularities in IoT systems with impressive precision, recall, accuracy, and f1-measure parameters. This work can act as a basis for creating sophisticated anomaly detection methods to defend IoT networks against new security risks.

Keywords:*Internet of Things (IoT), anomaly detection, security risks, Bird Swarm-Optimized artificial neural networks (BSO-ANN)*

1. Introduction

Academic institutions and the ICT sector have recently become interested in IoT. IoT systems influence many aspects of our daily life, such as home surroundings, transportation, and health care. IoT security threats can result in significant privacy issues and financial harm [1]. The growth of IoT is accompanied by the appearance of several difficulties. These issues can happen as an exception to the aberrant network traffic flow or as a network anomaly. Impressive results could be caused by a sudden mob, a connection failure, or fluctuations in network traffic. At the same time, assaults like probing and flooding attacks and assaults like R2L and U2R attacks can also provide anomalous security results [2].

Performance anomalies or security anomalies are also possible. For network managers in both scenarios, anomaly detection is a crucial duty. To spot irregular traffic flows or the causes of additional handling abnormalities, network operators, in particular, need a fast mechanism for immediately identifying aberrant unidentified trends in traffic data [3]. With regard to the IOT, an anomaly is often defined as the observable results of an unexpected change in a system's condition that goes beyond its worldwide or local norm. Several important discoveries about the presence of IoT data are made in this description.Since the Internet of Things collects the majority of its data represents the common operational characteristics of that particular system, it may be assumed that the data is "normal" in most cases. A system's "normal" operation may be defined differently over time for various reasons.Simple procedures that manage the tracking system are displayed in the data generated by an IoT deployment [4].

This study introduces the Bird Swarm-Optimized Artificial Neural Networks (BSO-ANN), a novel framework for anomaly identification in IoT scenarios.The remainder of the paper is divided into subsequent parts. Part 3 contains the proposed method explained. Part 4 includes the results and analysis. While Part 5 discusses the conclusions.

2. Related Works

Researchers give a thorough overview of IoT intelligence for security, based on technology and extensive learning algorithms that conclude from unstructured data to defend IoT devices from various cyberattacks proactively. They conclude by highlighting the related research questions and potential future directions that fall within the purview of our investigation. In general, the goal of this paper is to act as a technical resource and manual for cybersecurity researchers and professionals working in the IoT space [5]. This research, created with the improvement of Deep Learning techniques (Deep Belief Networks), offers an

1Assistant Professor, School of Engineering and Computer, Dev Bhoomi Uttarakhand University, Uttarakhand, India, Email Id: socse.mukesh@dbuu.ac.in
2Assistant Professor, Department of Computer Science and IT, Jain(Deemed-to-be University), Bangalore-27, India, Email Id: feon.jaison@jainuniversity.ac.in
3Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: jain.aaditya58@gmail.com
4Professor, School of Engineering & Technology, Jaipur National University, Jaipur, india, Email Id: director.soet@jnujaipur.ac.in

intelligent approach or methodology for preventing security breaches. This sophisticated intrusion detection technique examines the harmful behavior occurring within the network and attempts to gain access to it [6]. This Research analyzes FDIA's effects from an IoT standpoint and looks at the efficacy of available FDIA defenses. This chapter's primary contribution is establishing a new line of inquiry for the Internet of Things (IoT) study regarding FDIA identification and safeguarding. Graduate students, academics, and investigators in this subject domain will benefit from reading this chapter [7]. The thorough examination and evaluation of several deep learning- and machine learning-based detection systems for network intrusions (NIDS) are provided in this paper's complete overview.

Furthermore, an IoT case study of medical treatment is provided. The study illustrates the practical use of acquiring principles in this field and the architectural, security, and privacy concerns. Listing the findings gleaned from the literature serves as the analysis's ultimate conclusion. The study also highlights various research issues that need to be resolved for methods to handle uncommon problems to be improved further [8].

This research introduces an artificial neural network-based anomaly behavior evaluation methodology for implementing dynamic IDS that can recognize when a Fog cluster is compromised and subsequently take the necessary steps to ensure interaction accessibility. The analysis outcomes show that, despite the adaptive scheme's complexity, the proposed approach can characterize the usual actions of fog nodes and can also detect anomalies resulting from a several reports, such as abuse, cyber attacks, and system flaws, with a high detection rate and a low rate of false alarms [9]. To ensure the security of the healthcare industry, this article suggests the Internet of Things with Artificial Intelligence System (IoT-AIS). By utilizing IoT technologies, networks of wireless sensors are created. The Internet of Things (IoT) network connects the digital and physical worlds. The data of the patient are encrypted and monitored by IoT-AIS. The cloud-based storage of the encrypted data allows for remote access to the patient data. An individual user interface with single-user access is provided by the IoT-AIS dashboard for each patient so they can manage their information. The suggested paper's simulation research demonstrated that the individual's record for medical treatment might be encrypted and offer individualized access [10]. With a particular focus on Distributed Denial of Service (DDoS) attacks, the study is a multi-layered analysis of various security vulnerabilities in the IoT layers of perception, network, support, and application. The potential for DDoS assaults to bring down their targets makes them a danger to the online environment. It details the various DDoS attack types, how they affect IoT devices, their effects, and mitigating options. In the review study that is being given, intrusion detection models are contrasted with intrusion prevention models to reduce DDoS attacks [11]. This article focuses on research on security in IoT for business, car networks, the digital grid, the digital home, and the digital health. Then they listed the areas that can be altered as technology develops in the future, including computing power providing through the boundary network processing unit (NPU) important device, closely coupling ecological simulation models with their natural surroundings, malicious code detection, intrusion detection, and manufacturing protection, danger identification, troubleshooting, and blockchain technology.

About Intrusion Detection Models [12]. In-depth examination of existing IoT IDS is provided in this survey article, along with an overview of the techniques, deployment strategies, validation methodologies, and datasets that are widely used to construct IDS. Additionally, they discuss how modern IoT IDS detect intrusive threats and guarantee secure IoT connectivity. It also provides taxonomy of IoT attacks and outlines future studies to thwart them to make IoT more secure [13]. This framework's objective is to find each known attacks and 0-day assaults with extreme findings precision and minimal false-alarm rates. Several different forms of assaults and legal IoT network traffic are included in the Bot-IoT dataset, which assesses the proposed HIDS. Comparison to methods for AIDS and SIDS, experiments demonstrate that the suggested hybrid IDS offers a extreme identification rate and a lower rate of false positives [14]. The IoT is introduced in this paper together with its well-known system design, enabling technologies, security problems, and objectives. Our analysis of security flaws and provision of modern security taxonomies are additional features. Software, the internet, and physical layer attack taxonomies for the most pertinent and recent IoT security threats are described. This study examines and comments on the most cutting-edge security countermeasures in the fields of autonomic, encoding, and learning-based techniques, while most earlier surveys focused on just one area of security measures. They also identify security obstacles the research community can overcome to implement security in a heterogeneous IoT context. Finally, they offer various perspectives on potential security solutions and future research topics [15].

3. Proposed Method

3.1. Bird Swarm Algorithm

BSA, or the Bird Swarm Algorithm, was developed to address optimization issues. The swarm ideas that were derived from the social intuition in bird groups are where BSA got its start. Birds engage in three different sorts of behaviors: flying behavior, carefulness behavior, and

scrounging behavior (foraging behavior). A few guidelines, like the ones that follow, can be used to reorganize social behaviors:

Step 1: Each bird can switch between vigilant and scavenger behaviors.

Step 2: While searching for food, each bird keeps track of its and the swarm's previous best positions about the food patch. The entire swarm is immediately informed of social information.

Step 3: Each bird must try to fly toward the middle of the swarm while keeping watch. In comparison to birds with lesser saves, those with more protection will be more likely to lie in the middle of the swarm.

Step 4: Birds may be producers or consumers as they fly to another region. A manufacturer would be the bird with the highest sales level, and a scrounger or consumer would have the lowest.

Step 5: Creators seek food, whereas scroungers carelessly follow a creator in seeking food.

The following explains the Bird Swarm Algorithm: through the quest for meals, each of the N virtual birds flies through a D-dimensional space, represented by their positions at time step t as shown by the coordinates x_i^t ($i \in$ [1,…, N].

3.1.1. Forage Methods

Step 2, which explains how birds find food, is translated into the corresponding set of equations:

$$v_{j,i}^{s+1} = v_{j,i}^{s} + \left(o_{j,i} - v_{j,i}^{s}\right) \times D \times rand(0,1) + \left(h_i - v_{j,i}^{s}\right) \times T \times rand(0,1), (1)$$

When $j \in$ [1,…, D], and (0, 1) indicates liberty, values are placed at regular intervals 0 and 1. Cognitive and social are represented by the enhanced coefficients C and S. The ith bird's best previous location is $p_{i,j}$, while the swarm of birds' best last shared position is g_j.

3.1.2. Alertness Behavior

According to Step 3, birds wing forward to the swarm's center, and these motions can be described as follows:

$$v_{j,i}^{s+1} = v_{j,i}^{s} + B1\left(mean_i - v_{j,i}^{s}\right) \times rand(0,1) + B2\left(ol_i - v_{j,i}^{s}\right) \times rand(1,1), \quad (2)$$

$$B1 = b1 \times exp\left(-\frac{oFit_j}{sunFit+\varepsilon} \times M\right), (3)$$

$$B2 = b2 \times exp\left(\left(-\frac{oFit_j - oFit_l}{|oFit_j - oFit_j| + \varepsilon}\right)\frac{M \times oFit_l}{sunFit+\varepsilon}\right), (4)$$

Where $k(k \neq i)$ is an integer with a positive value that is randomly selected from the range of 1 to $N. a1, and\ a2$ represent 2 positive constants in the range [0, 2], it stands for the ith most excellent health value for birds $\in$, and $sum\ Fit$ it is the total of the swarming's top health values. To avoid the division by zero error, there is a constant called. The ith component of the mean swarm position is shown by mean$_j$. A1 and rand (0, 1) weren't supposed to produce a product greater than 1. Here, A_2 shows the immediate impact of the interference caused by advancing near the swarm's core.

3.1.3. Aircraft Behavior

Birds fly to find food and scavenge for meals again. While some individuals try to feed from the meal patch that the creators found, a small number of birds search for food patches. Step 4 allows the separation of the makers and borrowers from the swarm. The operations of the makers and borrower, respectively, can be expressed numerically as:

$$v_{j,i}^{s+1} = v_{j,i}^{s} + rand(0,1) \times v_{j,i}^{s}, (5)$$

$$v_{j,i}^{s+1} = v_{j,i}^{s} + \left(v_{j,i}^{s} - v_{j,i}^{s}\right) \times EK \times rand\ (0,1), \quad (6)$$

In this case, random (0-1) represents a Random number with a Random distribution and a mean of 0, standard deviation $1, k \in [1, 2, 3, \ldots, N], and\ k \neq i. F\ L (F\ L \in [0, 2])$ denotes that the scrounger should follow the creator.

3.2. ANN

The input layer, hidden layer, and output layer are the three different types of layers that make up the ANN model, as depicted in Fig 1. Numerous neuron-like nodes, or nodes, make up each layer. The model's input data are contained in the input layer. The amount of input characteristics is equal to the number of neurons. Every neuron from the intake layer has a weighted connection with several neurons in the second layer. Until the output layer, the second layer's output will pass through the subsequent layers.

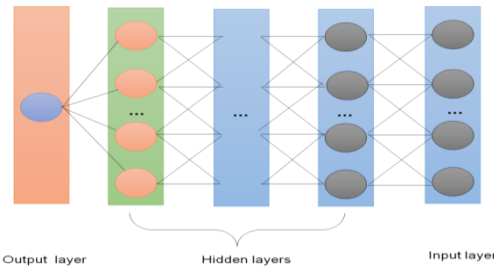

Fig 1. Conventional artificial neural networks have different layers.

Given a three-layer ANN, the weights among the input layers and the unnoticed layer are $U^2(v_1, v_2, v_3)$ and b^1, respectively. An activation function, such as the sigmoid engagement function in Equation 8, transforms the inner product among the weighted matrices and the input data. Until the output layer, each layer receives the mapped values as input. Only one neuron is present in the resultant layer for binary categorization. As seen in equation (7), the feed-forward mechanism can be expressed mathematically.

$$e(V) = U^2 h(U^1 V + c^1) + c^2, \quad (7)$$

$$h(v) = \frac{1}{1} + exp(-v)), (8)$$

W^1And $W^2$are the weight matrix for the input and hidden layers, accordingly, and b^1 and b^2 are bias factors added to the hidden and output layers, respectively. In addition to Softmax, Tanh, and ReLU activation functions, among others, $g(.)$ is a sigmoid activation function.

4. Result

On a PC with a Core i6 3.60 GHz CPU and 8 GB of RAM, performance analysis and model implementation are carried out. This is done in MATLAB 2020a. The dataset utilized is UNSW-NB15. There are 12 targets in this dataset—1 average target and ten attack-based targets. There is also a binary version of the dataset where 2 represents an attack, and 0 describes typical. The binary class form of this dataset will only be studied in this research. The dataset contains a total of 50 attributes that aid in effectively categorizing the targets. 180,269 samples make up the training data, whereas 85,692 pieces make up the test data. Utilizing the output metrics of accuracy, recall, precisions, and F1-score, the recommended method's efficacy would be assessed. With other strategies like LAE-BLSTM [16] and DNN-CSO [17], the effectiveness of the suggested BS-ANN strategy will be analyzed and compared.

The model's capabilities included accuracy as a subset. It is one of the outcome metrics evaluated while evaluating classification methods. The accuracy was calculated using equation (9). The recommended approach performs better in terms of accuracy (figure 2).

$$Accurcy = \frac{TPV+TNV}{TPV+TNV+FPV+FNV} (9)$$

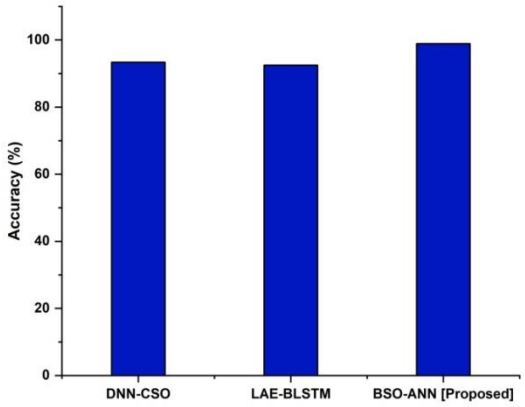

Fig.2. Accuracy

Favorable prediction rates were used to define precision. The ratio of successfully predicted positive observations to fully projected positive values was used to describe it. To calculate precision, use the equation (10). The recommended approach performs better in terms of precision (figure 3).

$$Precision = \frac{TPV}{TPV+FPV} (10)$$

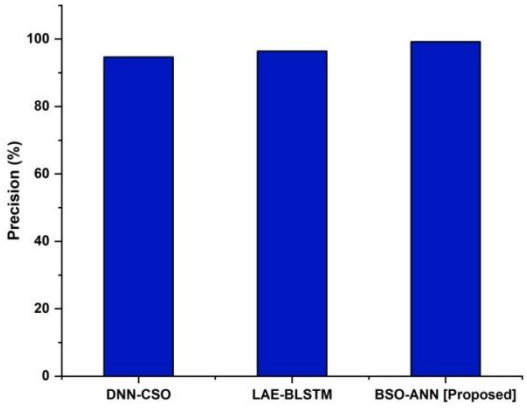

Fig.3. Precision

Both the recall and the sensitivity have similar names. What was precise was the average of each analysis made in the real classes to the favorable projected values. Recall was calculated using the equation (11). The recommended approach performs better in terms of recall (figure 4).

$$Recall = \frac{TPV}{TPV+FNV} \quad (11)$$

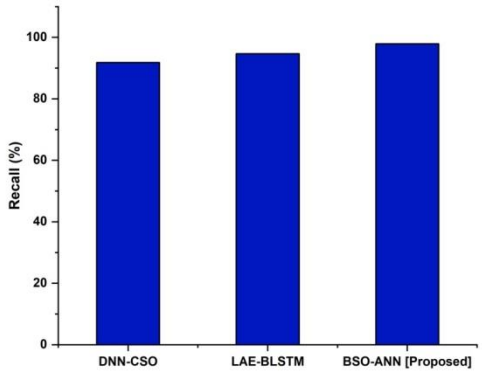

Fig.4. Recall

The precision and recall were estimated harmonically by the F1-score. The outcomes detection of imbalanced data was perfectly measured by this accuracy-related parameter in equation (12).The recommended approach performs better in terms of f1-score (figure 5).

$$F1 - score = \frac{2TPV}{2TPV+FPV+FNV} \quad (12)$$

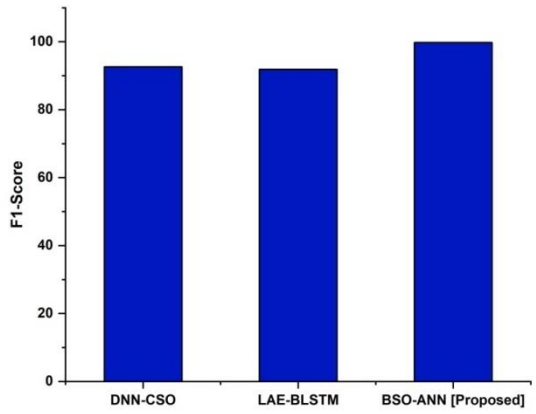

Fig.5.f-1score

The effectiveness of the suggested method for attack detection was evaluated, and its results were compared to those of other methods already in use, such as deep neural networks with chicken swarm optimization (DNN-CSO) and long short-term memory autoencoder-bidirectional long short-term memory (LAE-BLSTM). The BSO-ANN method performed better than all other evaluation standards.

4. Conclusion

Artificial intelligence (AI)-enabled security methods are becoming essential for thwarting Internet of Things (IoT) threats. The overall attack surface has increased due to the growth of IoT gadgets and their increased connection, rendering conventional security solutions ineffective. AI-based security protocols have many benefits for preventing IoT threats and preserving the availability, integrity, and confidentiality of IoT systems. In this paper, a novel framework for anomaly identification in Internet of Things (IoT) scenarios is introduced: the Bird Swarm-Optimized Artificial Neural Networks (BSO-ANN). The mixes of ordinary contemporary outcomes and current synthetic assault methods employed in this design were created using the UNSW-NB15 dataset. Compared to existing strategies, the suggested strategy detected every assault label with more excellent detection rates. The BSO successfully extracts the dataset's features, and the ANN was utilized to categorize and identify the attacks. Future applications of the proposed anomaly detection model include detecting attacks using multiple datasets for many network architectures, including wireless sensor networks, the Cloud, and High Order Calculators.

References

[1] Iwendi, C., Rehman, S.U., Javed, A.R., Khan, S. and Srivastava, G., 2021. Sustainable security for the Internet of Things using artificial intelligence architectures. ACM Transactions on Internet Technology (TOIT), 21(3), pp.1-22.

[2] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F. and Abdulkadir, S.J., 2022. Detecting cybersecurity attacks in the internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), p.198.

[3] Kuzlu, M., Fair, C. and Guler, O., 2021. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1, pp.1-14.

[4] Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, p.100227.

[5] Thakre, B., Thakre, R., Timande, S., & Sarangpure, V. (2021). An Efficient Data Mining Based Automated Learning Model to Predict Heart Diseases. Machine Learning Applications in Engineering Education and Management, 1(2), 27–33. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/17

[6] Sarker, I.H., Khan, A.I., Abushark, Y.B. and Alsolami, F., 2022. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions, and research directions. Mobile Networks and Applications, pp.1-17.

[7] Balakrishnan, N., Rajendran, A., Pelusi, D. and Ponnusamy, V., 2021. Deep Belief Network

enhanced intrusion detection system to prevent security breaches in the Internet of Things. Internet of Things, 14, p.100112.

[8] Bostami, B., Ahmed, M. and Choudhury, S., 2019. False data injection attacks in the Internet of Things. Performability in Internet of Things, pp.47-58.

[9] Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K. and Hong, W.C., 2021. Internet of things: Evolution, concerns, and security challenges. Sensors, 21(5), p.1809.

[10] Ibrahim, S. S. ., & Ravi, G. . (2023). Deep learning based Brain Tumour Classification based on Recursive Sigmoid Neural Network based on Multi-Scale Neural Segmentation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 77–86. https://doi.org/10.17762/ijritcc.v11i2s.6031

[11] Pacheco, J., Benitez, V.H., Felix-Herran, L.C. and Satam, P., 2020. Artificial neural networks-based intrusion detection system for Internet of Things fog nodes. IEEE Access, 8, pp.73907-73918.

[12] Ghazal, T.M., 2021. Internet of Things with artificial intelligence for health care security. Arabian Journal for Science and Engineering.

[13] Mishra, N. and Pandya, S., 2021. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, pp.59353-59377.

[14] Li, Y., Zuo, Y., Song, H. and Lv, Z., 2021. Deep learning in the security of Internet of Things. IEEE Internet of Things Journal, 9(22), pp.22133-22146.

[15] Khraisat, A. and Alazab, A., 2021. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4, pp.1-27.

[16] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. and Alazab, A., 2019. A novel ensemble of hybrid intrusion detection systems for detecting Internet of Things attacks. Electronics, 8(11), p.1210.

[17] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. and Alazab, A., 2019. A novel ensemble of hybrid intrusion detection systems for detecting Internet of Things attacks. Electronics, 8(11), p.1210.

[18] Popoola, S.I., Adebisi, B., Hammoudeh, M., Gui, G. and Gacanin, H., 2020. Hybrid deep learning for botnet attack detection in the internet-of-things networks. IEEE Internet of Things Journal, 8(6), pp.4944-4956.

[19] Khilar, R., Mariyappan, K., Christo, M.S., Amutharaj, J., Anitha, T., Rajendran, T. and Batu, A., 2022. Artificial intelligence-based security protocols to resist attacks in the Internet of Things. Wireless Communications and Mobile Computing, 2022.