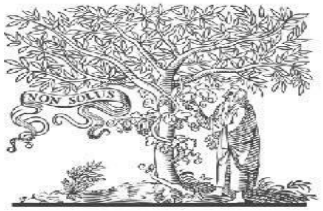
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 06th Oct 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 10

10.48047/IJIEMR/V12/ISSUE 10/04

Title **DEEP LEARNING BASED CYBERATTACK DETECTION IN MOBILE CLOUD COMPUTING**

Volume 12, ISSUE 10, Pages: 26-32

Paper Authors **Mr. D. Shine Rajesh, G.Jini Mol, Dr.Sumaiya Samreen**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DEEP LEARNING BASED CYBERATTACK DETECTION IN MOBILE CLOUD COMPUTING

[1] Mr. D. Shine Rajesh, [2] G.Jini Mol, and [3] Dr.Sumaiya Samreen
[1] Department of IT ,Malla Reddy Engineering College for Women (Autonomous),
shinerajesh@gmail.com
[2] Department of CSE, Arunachala college of engineering for women,
jinimolacew@gmail.com
[3] Department of IT ,Malla Reddy Engineering College for Women (Autonomous).
sumaiyasamreen_it@mrecw.in

Abstract
The convergence of mobile apps and cloud computing has propelled Mobile Cloud Computing into the spotlight, attracting significant attention from academia and industry alike. Concerns surrounding the security of mobile cloud applications primarily revolve around data integrity, user privacy, and service availability. Taking a preventive approach to address security issues, early detection and isolation of cyber risks in the mobile cloud computing system is essential. Our research introduces a cutting-edge framework that utilizes deep learning to detect cyber-attacks in the mobile cloud environment. The proposed model employs BMO-DBN, a deep belief network (DBN) optimized using the barnacles mating optimizer (BMO) method, for cyber-attack detection. Through empirical evidence, we substantiate that our suggested framework not only distinguishes various types of cyber-attacks but also achieves a remarkable level of accuracy.
Keywords: Cyber Security, Mobile cloud computing, deep learning approach, cyber-attacks detection, deep belief network

I INTRODUCTION

Cyber security encompasses a range of procedures, methods, tools, and technologies that work together to protect computer systems, networks, software, and data from unauthorized access, ensuring their availability, confidentiality, and integrity. Various cyber security measures exist at the application, network, host, and data levels, contributing to the protection of electronic information resources. Safeguarding critical digital assets is crucial as cyber attackers continue to outpace existing defences, posing a significant risk to their security.

II RELATED WORK

[1] A challenging dataset is used to evaluate the recommended technique for validity, and the findings show improved performance. [2] Quantum support vector machines (QSVM), k-nearest neighbours (KNN), linear discriminant and quadratic discriminant long short-term memory (LSTM), and auto encoder algorithms are examples of machine learning and deep learning methods. According to experimental findings, the KNN and LSTM algorithms were 98.55% and 97.28% accurate at categorising objects into binary categories. [3] Utilizing the intermediate observer approach, attack

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

reconstruction and state estimation of the attacked CPPS are completed.

III. PROPOSED METHOD

A framework for using deep learning technology to detect and prevent cyber-attacks. A deep belief network (DBN), which is then optimised using the barnacles mating optimizer (BMO) method and utilised as a cyber-attack detection tool, is trained using a training dataset. As a technique for detecting cyber-attacks, BMO-DBN, a deep belief network (DBN) improved by the barnacles mating optimizer (BMO) method, is used.

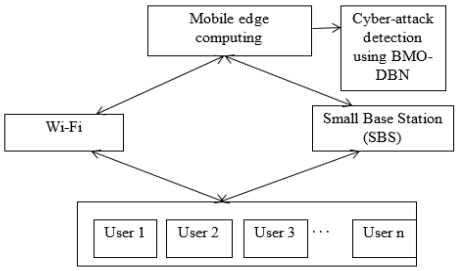


Figure 1. The overall work of the proposed model.

Additionally, SBS and Wi-Fi system resource application has been improved, increasing system throughput. The BMO-DBN model's operational procedure is depicted in Fig. 1.

3.1 CYBERATTACK DETECTION USING DBN MODEL

Cyber-attack detection using DBN, with $u = \{u_m\}$'m nodes in the visible layer and $v = \{v_n\}$ nodes in the hidden layer, and RBM is pre-trained in this configuration. The provided set of visible variables (u) equals 'um' and the specified set of hidden variables $v = \{v_n\}$. The weights for each feature vector are randomly determined by Gibb's sampling in the con-transitive divergence (CD) algorithm. The hidden and obvious nodes are taken to be binary stochastic elements, according to our assumption. The bipartite graph composed of visible and hidden nodes has no visible-visible or hidden-hidden linkages. There aren't any links between the layers; only between layers. Figure 2 shows how the RBM is given the input data and instructed to re-represent them.

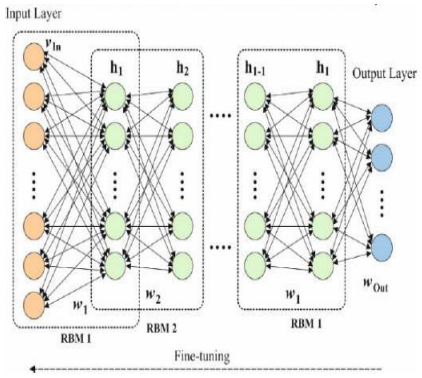


Figure 2: The Architecture of DBN.

Figure 2 illustrates how all RBMs create a visible layer with visible units $v = \{v_1, v_2, \dots, v_i\}$ and a hidden layer with hidden units $h = \{h_1, h_2, \dots . h_j\}$. the energy function's model parameters for DBN $\theta = [W, b, a]$ are given as:

$$E(v, h; \theta) = -\sum_{i=1}^{I}\sum_{j=1}^{J} \omega_{ij} v_i h_j - \sum_{i=1}^{I} b_i v_i - \sum_{j=1}^{J} a_j h_j \quad (1)$$

where J, b_i and a_j denote the bias conditions of the visible and hidden units, respectively, and ω_{ij} denotes the link weight among visible unit v_i and the entire number is I as well as hidden unit h 's entire number is J. Based on the energy

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

function $E(v;\ h;\theta)$ a combined sharing full unit is computed as follows:

$$p(v,h;\theta) = \frac{\exp(-E(v,h;\theta))}{Z} \qquad (2)$$

Where the separated function $Z = \sum_{h;v} \exp(-E(v,h;\theta))$ is. The following formula is used to compute the conditional possibilities for the hidden and visible units h and v:

$$p(h_i = 1|v;\theta) = \delta\left(\sum_{i=1}^{I} \omega_{ij} v_i + a_j\right) \quad (3)$$

$$P(v_i = 1|v;\theta) = \delta\left(\sum_{J=1}^{J} \omega_{ij} h_i + b_i\right) \quad (4)$$

Where $\delta(x) = 1/1 + \exp(x)$ where δ is a logistic function. The RBMs are taught to maximise the potential of all possible outcomes. By stacking numerous RBMs, a DBN is produced, with the result of the l^{th} layer serving as the input for the $l + 1^{th}$ layer. Pre-training and fine-tuning are the two steps of DBN that are broken down into the training model. Initial RBM sustains the information using a visible layer, which is converted into a concealed layer that is widely used in RBM. After layer-to-layer unsupervised training is finished, the classification layer of DBN is used to sustain the features that were automatically discovered by DBN. Finally, fine-tuning is put into practise in the classification layer to enhance DBN. The softmax layer is then employed for categorization.

3.2. BMO ALGORITHM

It is expected that the contender for a solution in the proposed BMO is barnacles.

I) Initialization

Where the following expression can be made for the population vector:

$$x = \begin{bmatrix} x_1^1 & \ldots. & x_1^N \\ \vdots & \ddots & \vdots \\ x_n^1 & \ldots. & x_n^N \end{bmatrix} \qquad (5)$$

Where n is the population size, or number of barnacles, and N is the number of control variables. The upper and lower bounds of the issue to be solved are as follows, and they affect the control variables in Eq 5.

$$ab = [ab_1 \ldots., ab_i] \qquad (6)$$

$$lb = [lb_1 \ldots\ldots lb_i] \qquad (7)$$

Where the i^{th} variable's upper and lower bounds are denoted by ab and lb. The best answer up to this point is found at the top of the vector X after first evaluation of the vector X and sorting.

ii) Selection process

When compared to previous evolutionary algorithms like GA, DE, etc., the suggested BMO uses a new strategy for the selection to be mated. As the length of the penises determines whether two barnacles are chosen, pl. Let's imagine that a barnacle's maximum penis length is seven times longer than its size (pl = 7), in which case barnacle #1 can only mate with one of the barnacles #2–#7 at a given iteration. Because it is over the limit, the normal mating process cannot take place if barnacle #1 chooses barnacle #8. Therefore, the sperm cast process (exploration), which will be discussed later, comes before the offspring generation. The straightforward choices

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

that are represented mathematically are as follows:

$$barnacle\_d = randperm(n) \quad (8)$$

$$barnacle\_m = randperm(n) \quad (9)$$

Where n is the population size and $barnacle\_d$ and $barnacle\_m$ are the parents that will be mated. The selection is made at random and satisfies the first assumption in the preceding subsection.

iii) Reproduction

Comparing BMO's proposed reproduction mechanism to previous evolutionary algorithms, it differs slightly. The Hardy-Weinberg principle is being used by the BMO to emphasise the inherited traits or genotype frequencies of the parents in creating the offspring because there are no precise formulae or formulas for calculating barnacle reproduction. The following expressions are suggested to generate new variables of offspring from the parents of barnacles in order to demonstrate the simplicity of the proposed.

$$\text{BMO:} x_i^{N\_new} = p x_{barnacle\_d}^{N} + q x_{barnacle\_m}^{N} \quad (10)$$

where p is the normally distributed pseudo random numbers between $[0, 1]$, $q = (1 - p), x_{barnacle\_d}^{N}$ and $x_{barnacle\_m}^{N}$ are the variables of *Dad* and *Mum* of barnacles respectively which has been selected in Eqn.(8),(9) P and Q are supposed to indicate the proportion of a parent's and parent's characteristics that are passed down to the next generation of offspring. As a result, based on the chance of a random number between 0 and 1, the offspring inherits the behaviours of the parents. The procedure for casting sperm is described as follows:

$$x_i^{n-new} = rand() \times x_{bernacle\_m}^{n} \quad (11)$$

Where [0, 1] is a random number generated by rand (). It should be noticed that Eq. (11) illustrates the barnacle's offspring's straightforward evolutionary strategy. The mother's barnacle produces the new offspring for the exploring phase. This is because Mum's barnacle produces the new offspring because it takes the sperm from the water that the other barnacles have released.

IV EXPERIMENT RESULT

Three real datasets are used in our tests, provide a quick review of common cyber-security in MCC. Next, discuss how to assess the findings of the experiment. It employ three empirical, publicly available datasets to confirm the precision of the deep-learning cyber-attack detection.

4.1 Accuracy

Accuracy is defined as the ratio of correct detection throughout the entire traffic trace as follows: $\frac{TP_i+TN_i}{TP_i+TN_i+FP_i+FN_i}$where TP, TN, FP, and FN stand for "true positive", "true negative", "false positive," and "false negative," respectively. In order to define the average prediction accuracy of the M supported classes, we need to know:

$$Accuracy = \frac{1}{M}\sum_{i}^{M}\frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i} \quad (12)$$

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Algorithms	NSL-KDD	UNSW-NB15	KDD cup
Decision Tree	93.78	97.01	87.91
Multilayer Perceptron	87.91	90.16	96.77
Random Forest Classifier	88.39	94.44	97.02
Proposed BMO with DBN	90.99	97.11	99.23

. Table 1: The Comparison between Our Propose Model with existing methods.

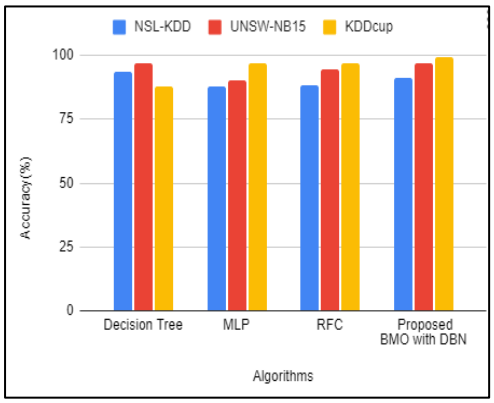


Figure 3: Our proposed model is compared to current approaches.

The performance of the deep learning strategy is compared in Table 1. We note that, for the same datasets, the proposed deep learning approach consistently delivers the best performance in terms of accuracy, precision, and recall.

Algorithms	Precision	Recall
Decision Tree	97.01	94.14
Multilayer Perceptron (MLP)	96.77	90.87
Random Forest Classifier	97.02	94.42
Proposed BMO with Deep Belief Network	98.87	99.22

Table 2: The Comparison between Our Propose Model with existing methods.

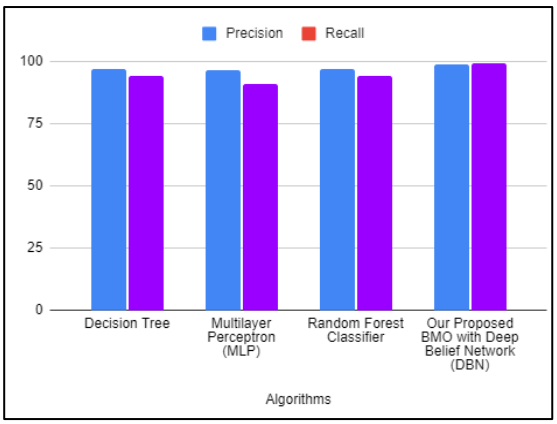


Figure 4: Our proposed BMO with Deep Belief Network (DBN) model Precision and Recall is compared to existing methods

Table 2 compares the performance of the deep learning approach with those of other algorithms, some of which include Decision Tree, Multilayer Perceptron (MLP), and the Random Forest Classifier (RFC) (Figure 4).

CONCLUSION

In this study, we present a BMO using Deep Belief Network (DBN) to identify cyber threats in the mobile cloud environment. In this study, using a deep learning technique, we offer a novel framework for identifying cyber-attacks in a mobile cloud context. A deep belief network (DBN) optimised using the barnacles mating optimizer (BMO) approach is employed in the proposed

model for attack detection employing BMO-DBN as a tool to identify cyber-attacks. Our suggested learning model has outperformed previous machine learning techniques, as shown by experimental findings, and can detect cyber-attacks with high accuracy. The results showed that BMO with Deep Belief Network (DBN) was able to provide very competitive results compared to existing algorithms.

REFERENCES

1. Aldaej, Abdulaziz, Tariq Ahamed Ahanger, Mohammed Atiquzzaman, Imdad Ullah, and Muhammad Yousufudin. "Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective." *Sensors* 22, no. 7 (2022): 2630. https://doi.org/10.3390/s22072630
2. Alzahrani, Mohammed Saeed, and Fawaz Waselallah Alsaade. "Computational Intelligence Approaches in Developing Cyberattack Detection System." *Computational Intelligence and Neuroscience* 2022 (2022).
3. Su, Q., Wang, H., Sun, C., Li, B., & Li, J. (2022). "Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy". Applied Mathematics and Computation, *413, 126639.* doi:10.1016/j.amc.2021.126639
4. Kang-Di Lu;Guo-Qiang Zeng;Xizhao Luo;Jian Weng;Weiqi Luo;Yongdong Wu; (2021). Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System. IEEE Transactions on Industrial Informatics, (), –. doi:10.1109/tii.2021.3053304
5. Dixit, Priyanka; Silakari, Sanjay (2021). Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. Computer Science Review, 39(), 100317–. doi:10.1016/j.cosrev.2020.100317
6. Iqbal H. Sarker; (2021). Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN Computer Science, (), –. doi:10.1007/s42979-021-00535-6
7. Gokhan Altan; (2021). SecureDeepNet-IoT: A deep learning application for invasion detection in industrial Internet of Things sensing systems. Transactions on Emerging Telecommunications Technologies, (), –. doi:10.1002/ett.4228
8. Iqbal H. Sarker;Md Hasan Furhad;Raza Nowrozy; (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science
9. Zeadally, Sherali; Adi, Erwin; Baig, Zubair; Khan, Imran (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access
10. Dasgupta, Dipankar; Akhtar, Zahid; Sen, Sajib (2020). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation: Applications,

Methodology, Technology, (), 154851292095127
doi:10.1177/1548512920951275