Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTERNET OF THINGS CONSUMER ELECTRONICS CYBERSECURITY APPROACH BASED ON DEEP LEARNING

MORARJEE KOLLA[1], PRAVEENA BAI DESAVATHU[2], K NARAYANA RAO[3], NALLA SIVA KUMAR[4], HANUMANTHA RAO BATTU[5], JOHN T MESIA DHAS[6], SUBRAMANYAM KUNISETTI[7]

[1]Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad - 500075, Telangana, India
[2]Department of Electronics and Communication Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India
[3]Department of Computer Science and Engineering, Rise Krishna Sai Prakasam Group of Institutions, Ongole, Andhra Pradesh, India
[4]Department of Computer Science and Engineering, Aditya University, Surampalem, Andhra Pradesh, India
[5]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Deemed to be University, Vaddeswaram, Guntur, Andhra Pradesh, India
[6]Department of Artificial Intelligence and Data Science, School of Computing, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology (Deemed to be University), Vel Nagar, Chennai, Tamilnadu, India
[7]Department of Computer Science and Engineering (Data Science), RVR&JC College of Engineering, Guntur, India.
E-mail: [1]morarjeek@gmail.com, [2]praveena.d@pvpsiddhartha.ac.in, [3]narayanarao2@gmail.com, [4]sivakumar.nalla@adityauniversity.in, [5]hanuma9999@yahoo.com, [6]jtmdhasres@gmail.com, [7]subramanyamkunisetti@gmail.com.

ABSTRACT

Protecting linked devices from potential weaknesses and dangers is the primary goal of security in the Internet of Things (IoT) consumer electronics. The collection, transmission, and storage of sensitive information by these smart devices necessitates stringent security measures to prevent hacking, data breaches, and unauthorized access. To ensure the security and privacy of user data, it is essential to utilize strong encryption, secure authentication procedures, and to update software regularly. Users can start and operate drones anytime, anywhere, and they offer a bird's-eye view. Criminals and cybercriminals, however, have begun to exploit drones maliciously. These attacks are extremely dangerous and destructive, and they happen frequently and with a high probability. Therefore, the requirement for investigative work and preventative measures necessitates a desire for protection. Drones equipped with deep learning (DL) for intrusion detection can take control of complex NN structures, enhancing security monitoring in ever-changing outside settings. These drones can fly alone, armed with high-tech sensors and computing power, to scan the sky for dangers like suspicious activity, unapproved people or vehicles, and then label them accordingly. Drones equipped with DL techniques can instantly recognize and respond to complicated patterns and irregularities, paving the way for proactive security measures. An improved method for drone platforms based on mathematical modeling, known as MGOADL-CS, which stands for Mountain Gazelle Optimization with Attention to Deep Learning for Cybersecurity, is presented in this paper. By identifying assaults with the help of optimal DL models, the MGOADL-CS approach seeks to enhance cybersecurity in the drone's environment through the use of BC technology. Starting with input data normalization, the MGOADL-CS method employs a linear scaling normalization (LSN) strategy. When it comes to dimensionality reduction, the MGOADL-CS method relies on an improved tunicate swarm algorithm (ITSA) based feature selection strategy. By the way, cyberattacks are detected and classified using the attention long short-term memory neural network (ALSTM-NN) model. At last, the ALSTM-NN model's hyperparameter values are fine-tuned using the MGO-based hyperparameter tuning procedure. In order to showcase the improved attack detection outcomes of the MGOADL-CS method, a comprehensive simulation set is completed using the NSL dataset. The accuracy

rating of 99.71% demonstrated by the performance validation of the MGOADL-CS method was higher than that of previous approaches.

Keywords: *Internet of things, Cons Cybersecurity, Unmanned aerial vehicles, Optimization of mountain gazelles, Deep learning*

1. INTRODUCTION

As wireless connection becomes more commonplace and chipsets and sensors become smaller, the rising popularity of the Internet of Drones (IoDs) becomes apparent [1]. New developments in robotics and unmanned aerial vehicles (UAVs) have led to the creation of small, miniature drones such as micro drones and quadcopters. A significant advantage of these small drones is their ability to quickly access all of the monitoring systems for physical things [2]. It finds use in a wide range of fields, including defense, SAR, disaster relief, transportation, distribution, precision agriculture, and industrial monitoring, among others. Drones and other unmanned aerial vehicles (UAVs) have been flying for some time now. Drone technology has exploded in popularity as a result of smaller UAVs offering a plethora of benefits in areas such as distribution, privacy, and shipping [3]. However, similar to Intrusion Detection Systems (IDSs), these drones pose serious privacy and security risks. Smart drones are a relatively new area of study that makes use of the Internet of Things (IoT) in conjunction with wireless sensors that could be installed on smaller drones [4]. In light of the rapid development of the Internet and other communication technologies, the topic of network security has lately emerged as a prominent area of study. Network intrusion detection systems (NIDSs) and firewalls are among the solutions it employs to supply security and network resources [5].

Some have taken advantage of NIDSs to keep an eye on network traffic for any signs of malicious or suspicious activity. In 1980, the main idea of intrusion detection systems was conceived, and since then, several IDS products have been created to meet the needs of network security [6]. The next step is to increase the number of new attacks; identifying them is no easy task. Consider a scenario where a company relies on data from a particular node but is at risk due to a vulnerability in that node [7]. Signature-, anomaly-, or specification-based approaches are the three main types of intrusion detection systems. Knowledge-based, statistical-based, and machine learning (ML)-based anomaly detection methods are further subdivided into this category [8]. Emerging novel aerial solutions are a direct outcome of the exponential growth of communication and sensor downsizing technologies. Various industries can benefit from these devices' enhanced monitoring and surveillance capabilities [9]. Their adaptability makes them useful in many contexts, from efficient logistics to rapid response to emergencies, highlighting their revolutionary potential. Verifying the safety of these technologies is becoming more important as our dependence on networked devices grows. In order to safeguard vital infrastructure in this dynamic environment, it is possible to enhance cybersecurity procedures by utilizing advanced modeling methodologies like DL [10].

This research presents MGOADL-CS, a method for improving the drone's platform through mathematical modeling, which combines deep learning for cybersecurity with optimization for mountain gazelles. By identifying assaults with the help of optimal DL models, the MGOADL-CS approach seeks to enhance cybersecurity in the drone's environment through the use of BC technology. Starting with input data normalization, the MGOADL-CS method employs a linear scaling normalization (LSN) strategy. When it comes to dimensionality reduction, the MGOADL-CS method relies on an improved tunicate swarm algorithm (ITSA) based feature selection strategy. By the way, cyberattacks are detected and classified using the attention long short-term memory neural network (ALSTM-NN) model. At last, the ALSTM-NN model's hyperparameter values are fine-tuned using the MGO-based hyperparameter tuning procedure. In order to showcase the improved attack detection outcomes of the MGOADL-CS method, a comprehensive simulation set is completed using the NSL dataset. Below is a list of the main contributions of the MGOADL-CS method.

•The MGOADL-CS approach efficiently normalizes input data using the LSN method, confirming consistent feature ranges. This normalization improves the performance of subsequent models by mitigating biases related to different scales. Standardizing the data also eases more accurate learning and enhances convergence during training.

•The MGOADL-CS technique utilizes the ITSA model for feature selection, which effectively assists in dimensionality reduction. This methodology detects the most relevant features, improving the model's performance by removing noise and irrelevant data. Streamlining the feature set eases more effective training and better generalization in subsequent analyses.

•The ALSTM-NN model is implemented by the MGOADL-CS technique for the detection and classification of cyberattacks, employing the merits of both attention mechanisms and LSTM networks. This incorporation enables the model to concentrate on the data's significant features and temporal dependencies, enhancing the detection accuracy. By effectively analyzing sequences, it improves the method's capability to detect and classify diverse cyber threats in real time.

•The ALSTM-NN method performs MGO-based hyperparameter tuning to optimize the values of the ALSTM-NN model, confirming that the network performs at its best. This tuning process systematically alters parameters to improve the accuracy and effectiveness of the model. Fine-tuning these hyperparameters substantially improves the technique's capability to detect and classify cyberattacks effectively.

•This ALSTM-NN approach integrates normalization, advanced feature selection, an advanced NN model, and a hyperparameter tuning process to enhance cyberattack detection and classification accuracy and efficiency. The novelty is in its incorporation of these methods, which not only streamlines the data processing pipeline but also improves model interpretability. This methodology sets a new standard for robust cyber defence strategies by addressing feature relevance and model optimization.

2. LITERATURE REVIEW

The HAOADL-UAVN method was introduced by Alshammari et al. [11] and is a novel Hybrid Arithmetic Optimizer Algorithm with DL. In the initial step, the input database was prepared into a useful format by standardizing the network data using the min-max normalization technique. In order to quickly reach the convergence state, Kou et al. [12] created an IDS. An attention mechanism, a convolutional neural network (CNN), and a deep AE (DAE) are all components of the approach. It improved training efficiency while reducing the dimensionality of the fresh data. After using convolutional neural networks (CNNs) to extract features, we improved the significant characteristics using the attention mechanism and then classified and recognized the traffic. In their study, Escorcia-Gutierrez et al. [13] presented a new approach to intrusion detection and organization called the Sea Turtle Foraging Algorithm with a Hybrid DL-based IDS (STFA-HDLIDS). This is necessary in order to normalize the incoming data using min-max normalization during data preprocessing. The FS approach also relied on the STFA. This classification process ultimately made use of a DBN-Sparrow Search Optimization (SSO) algorithm. An architecture for prediction was created by Al-Quayed et al. [14]. The methodology uses a multi-criteria approach to enhance cybersecurity. It uses approaches from ML and DL to improve cybersecurity intrusion detection systems. Cybersecurity breaches have been identified and classified using DT and MLP approaches for many dimensions. A comprehensive model for UAV network services enabled by BC was proposed by Li et al. [15] to address these issues. Consistently integrating BC technology into the designed architecture presents issues with privacy protection and identity identification. The creation of Crystal Structure Optimization with DAE-enabled IDS (CSODAE-IDS) was contemplated by Alissa et al. [16]. With this approach, a novel feature selection model called MDHO-FS (Modified Deer Hunting Optimization-enabled FS) was used. The intrusions are being classified by the AE, which is being deployed simultaneously. An application of the hyperparameter approach to the growth of crystal formation dependent on lattice points inspired the CSO model. An EDMOA-DLAD approach, which stands for enhanced dwarf mongoose optimizer, was introduced by Alsariera et al. [17]. As an FS approach that utilizes EDMOA, the EDMOA-DLAD method was primarily developed. A deep variational-AE (DVAE) method is employed by the EDMOA-DLAD method to detect the attacks. Finally, for the best hyperparameter selection in DVAE architecture, the EDMOA-DLAD method employs the beetle antenna search (BAS) technique.

With the use of supervised and unsupervised ML techniques, Da Silva et al. [18] developed an intrusion detection system (IDS) to detect network intrusions and abnormal flights in swarms of unmanned aerial vehicle (UAV) instances. Using a Recurrent NN (RNN) for intrusion detection, Saravanan et al. [19] present the BbAB method, which is based on BC. The BC-based design for UAV network services is introduced by Li et al. [20]. Additionally, the approach incorporates DL models to fortify defenses against cyber-attacks and increase UAV safety. In

order to protect information about network traffic, Aljabri, Jemili, and Korbaa [21] establish a CNN-based intrusion detection system that uses BC technology. A genetic algorithm (GA) is used for feature selection in order to evaluate the trained CNN method. A cross-layer design and a two-stage Stackelberg incentive game optimized by a gradient-based algorithm are used in the federated learning (FL) and BC system for secure data sharing that is presented by Liu et al. [22]. A secure UAV network architecture is suggested by Li et al. [23] that uses DL and BC. This design includes a system for managing UAV cluster identities, a system for real-time situational awareness, and a platform for sharing data securely through BC and smart contracts. In order to build a safe smart grid (SG) network, Kumar et al. [24] combine Digital Twin (DT), Software-Defined Networking (SDN), DL, and BC. The research also includes DT for smart meter monitoring, SDN for low-latency service, a DL model for attack detection, and BC-based authentication. In order to make CRAHNs more resistant to attacks, Dansana et al. [25] describe a BC-based security architecture that guarantees QoS and strong security. A Mayfly Optimizer (MFO) is also integrated into the model for the purpose of optimizing resource use with both active and redundant miners. A hybrid CNN based on BC and the KPCA model is introduced by Awotunde et al. [26]. A multi-party authentication protocol is proposed by Reegan et al. [27]. A lightweight data aggregation method is used by the model, which secures data blocks using a BC model with Merkle trees. In their study, Priyadarshini et al. [28] introduce a model for detecting distributed denial of service attacks that combines bidirectional long short-term memories (LSTM) with convolutional neural networks (CNNs).

There are a number of issues with the current hybrid algorithms used in cybersecurity. Methods reliant on min-max normalization may have issues when used to different datasets due to their sensitivity to outliers. Given the intricacy and dependence on intricate feature selection procedures of some models, assistance with generalizability and interpretability may be necessary. Architectures that are enabled by BC may also have challenges with scalability and integration with current systems, which can reduce their efficiency. Some models may experience delays due to computational intensity, while others may struggle to handle increased overhead or differentiate between different types of attacks, especially in datasets that are not balanced. Maintenance requirements may rise due to high complexity resulting from integrating numerous technologies, and optimising hyperparameters in certain ways may only provide optimal outcomes in certain cases. Although these methodologies offer new approaches, they need to overcome these constraints in order to be more effective and practical. Research in cybersecurity nowadays, especially those involving hybrid algorithms and BC integration, frequently necessitates a more thorough examination across many datasets and real-life situations. Scalability, interpretability, and adaptability to different attack patterns are areas where many techniques require assistance. There should also be better ways to confirm real-time performance without compromising security and to control the computational cost. Filling in these blanks might make these novel solutions more effective and useful.

3. THE SUGGESTED APPROACH

This research presents a new MGOADL-CS approach tailored to the drone's operating conditions. The method's stated goal is to enhance cybersecurity through the use of optimum DL models for attack detection. Security is improved with the use of BC technology. Data normalization, ITSA-based feature selection, ALSTM-NN cyberattack detection, and MGO-based parameter tweaking make up its four main operations. The first step of the MGOADL-CS method is to normalize the input data using the LSN approach. LSN is an important technique for preprocessing data that normalizes statistical data by rescaling it to a range between 0 and 1 or -1 and 1, while preserving the relative relationships between the initial values. In this method, the range (the variation between the lowest and highest values) is used to isolate the data points that have had their minimum values subtracted from them. By ensuring that characteristics with different scales or units contribute equally to the analysis, LSN keeps ML approaches free from biases produced by data levels that aren't identical. It is fundamental to data preprocessing in fields as diverse as finance and image processing since it allows for successful model convergence, enhances interpretability, and raises the effectiveness of many procedures.

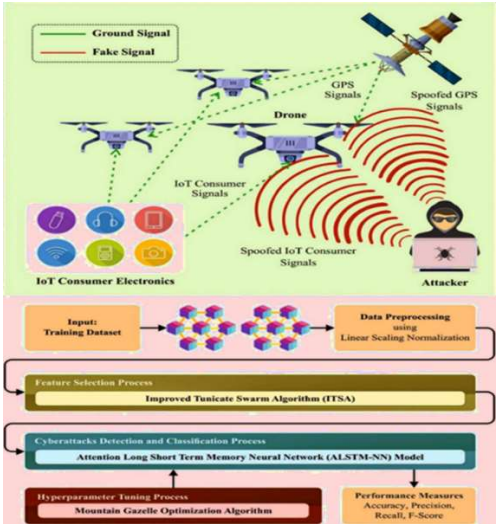

Figure 1: Workflow of MGOADL-CS method

The MGOADL-CS method employs an ITSA-based feature selection strategy for dimensionality reduction [29]. The feature space may be effectively explored and exploited using this technique, making it an ideal alternative for feature selection. This algorithm effectively detects the most significant properties while rejecting the unnecessary ones by mimicking the natural behavior of tunicates. Improved performance of ML approaches, reduced overfitting, and enhanced generalization are all results of ITSA's focus on feature relevance. It has been confirmed that ITSA searches for optimal feature subsets more thoroughly than traditional methods, as it is less likely to experience local optima. In addition, it is well-suited to the high-dimensional datasets often seen in cybersecurity applications due to its computational efficiency, which enables rapid processing. For precise and rapid threat identification, this skill is crucial

.

4. VALIDATING PERFORMANCE

In order to identify and categorize cyberattacks, the ALSTM-NN approach is used. Because it can identify critical aspects in sequential data as well as temporal connections, this approach is ideal for cyberattack detection. By focusing on key parts of the data, the model becomes more sensitive to patterns that can indicate cyber dangers, all thanks to the attention process. Long short-term memories (LSTMs) excel at handling long-range dependencies, which is crucial for identifying evolving intrinsic attack behaviors. When compared to more traditional approaches, which could miss important temporal data, this integration improves accuracy and resilience. The technique's versatility also makes it effective against a wide range of assault types, providing a one-stop shop for real-time detection in ever-changing settings. Using the NSL dataset, which contains 125,973 cases, the outcome evaluation of the MGOADL-CS methodology is investigated. This method was tested on a computer with an Intel Core i5-8600k processor, a 250 GB solid-state drive, a GeForce 1050 Ti with 4 GB of RAM, and a 1 TB hard drive using the Python 3.6.5 tool. You may find the parameter settings here: 0.01% learning rate, ReLU activation, 50 epochs, 0.5 dropout, and 50 units batch size. The MGOADL-CS approach (with 80:20 and 70:30 TRAS/TESS) produces confusion matrices, which are shown in Fig. 2. The MGOADL-CS method achieved effective recognition with five classes, according to the testing data.

Figure 3 shows the MGOADL-CS model's classifier result analysis on two different sets of parameters: 80/20 and 70/30. The MGOADL-CS model's output with 80:20 and 70:30 is shown in Figures 3a-3c. This chart shows that as the number of epochs increases, the MGOADL-CS model achieves better results. Raising validation (VL) at training (TRA) also shows that the MGOADL-CS model trained well on the test dataset. Finally, the MGOADL-CS model's loss curve at 80:20 and 70:30 is shown in Figures 3b-3d. These findings demonstrated that MGOADL-CS achieves TRA and VL loss with moderated levels. The results show that the MGOADL-CS method does well when trained on the test data.

See the MGOADL-CS classifier results at 80%:20% and 70%:30% in Figure 4. The MGOADL-CS technique's PR result at 80:20 and 70:30 is shown in Figures 4a-4c. The results of these experiments demonstrated that the MGOADL-CS method yields improved PR values. Furthermore, with each class, the MGOADL-CS method has achieved better PR values. To conclude, the MGOADL-CS method with 80:20 and 70:30 is analyzed using ROC in Figures 4b-4d. According to the figure, the MGOADL-CS method yields better ROC values. Additionally, with each class, the MGOADL-CS method can extend richer ROC values.

Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

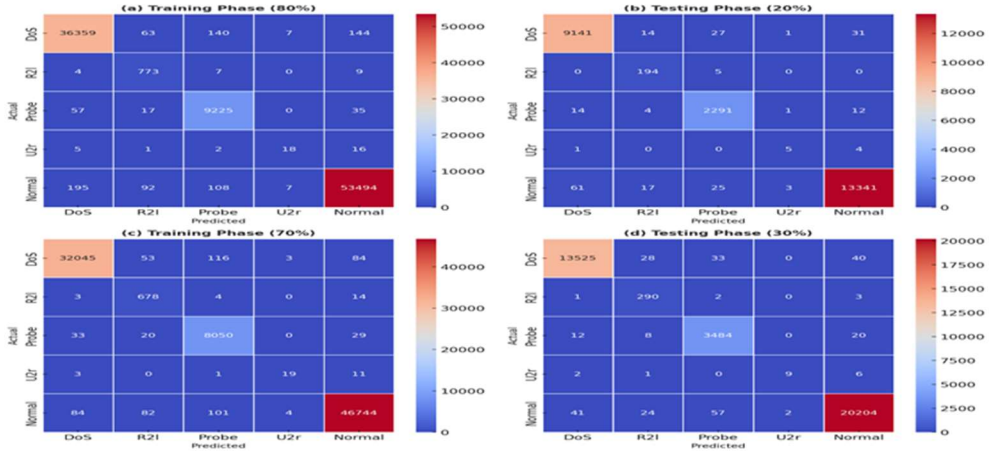

Figure 2: Matrix of confusions (a-b) (c-d) 70% TARS and 30% TESS, and 80% GST and 20% TESS od

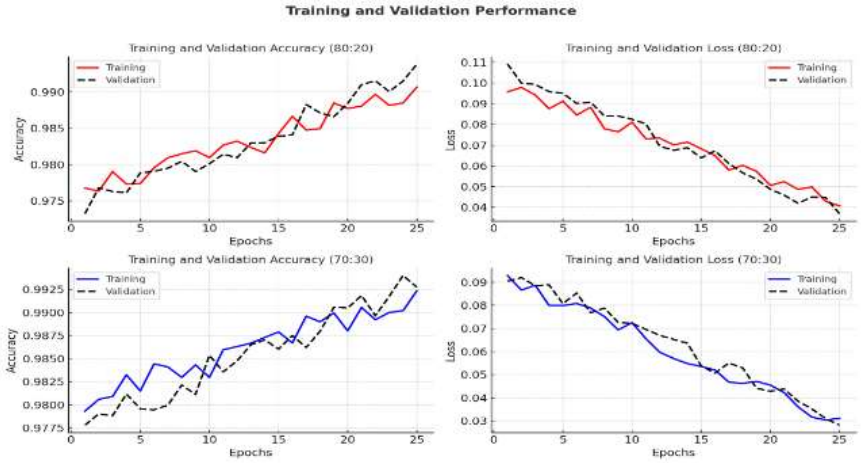

Figure 3. shows the accuracy (a-c) and loss (b-d) curves under 80:20 and 70:30, respectively.

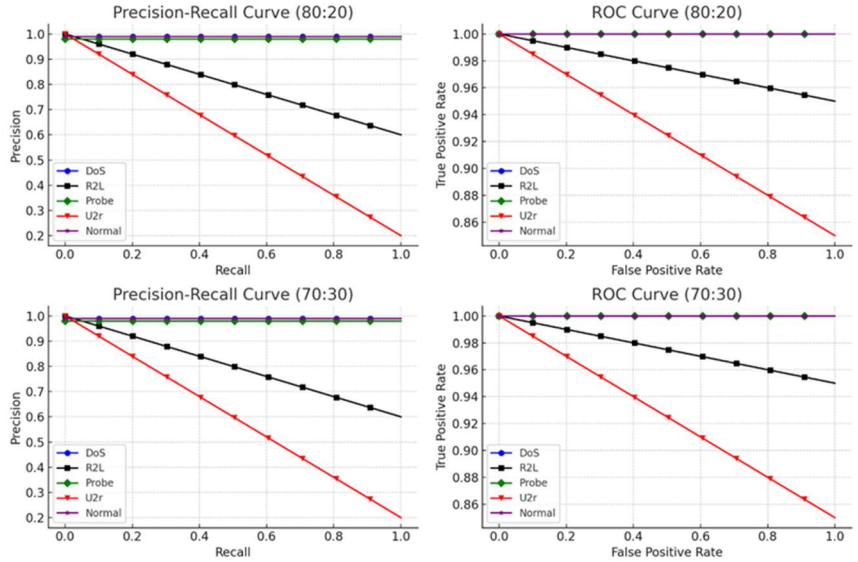

Figure 4. shows the PR and ROC curves for 80:20 and 70:30, respectively.

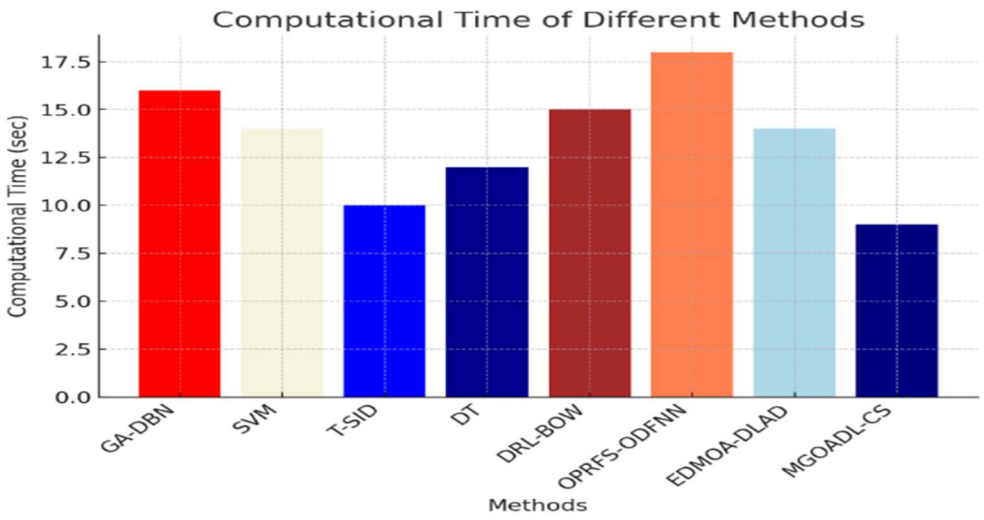

Figure 5. CT scans comparing the MGOADL-CS method to preexisting models.

Fig. 5 exhibit the CT analysis of the MGOADL-CS approach. The GA-DBN takes 16.46 seconds, SVM requires 13.70 seconds, T-SID completes in 10.16 seconds, DT takes 12.11 seconds, DRL-BOW needs 14.89 seconds, OPRFS-ODFNN lasts 17.88 seconds, and EDMOA-DLAD takes 16.10 seconds, while the MGOADL-CS technique depicts the shortest computation time at 8.65 seconds.

5. CONCLUSION

In the context of the drone, this article suggests a novel MGOADL-CS method. By identifying assaults with the help of optimal DL models, the MGOADL-CS method seeks to enhance drone environment cybersecurity. It consists of four main steps for normalizing data: feature selection using ITSA, intrusion detection using ALSTM-NN, and parameter optimization using MGO. The first step of the MGOADL-CS method is to normalize the input data using the LSN approach. The MGOADL-CS method employs an ITSA-based feature selection strategy for dimensionality reduction. In addition, cyberattack detection and classification could be accomplished using the ALSTM-NN protocol. Additionally, the ALSTM-NN model's hyperparameter values are adjusted using the MGO-based hyperparameter tuning method. A comprehensive set of simulations is carried out using the NSL dataset to showcase the improved attack detection outcomes of the MGOADL-CS method. The MGOADL-CS method demonstrated a 99.71% accuracy value during performance validation, which was higher than previous approaches. One possible drawback of the MGOADL-CS approach is that it may not be able to scale to handle very large datasets efficiently. Moreover, the findings may not be applicable to different cyberattack scenarios due to the reliance on particular models. Users may be hesitant to put their faith in automated systems if intrinsic models are not easily interpretable. Incorporating more effective data processing models into future work could increase the methodology's scalability. In addition, investigating hybrid models that combine different approaches may enhance resilience and flexibility. Finally, in order to promote acceptance and practicality, additional research on the results' interpretability is essential.

REFERENCES:

[1] Ashraf, S.N., Manickam, S., Zia, S.S., Abro, A.A., Obaidat, M., Uddin, M., Abdelhaq, M. and Alsaqour, R., 2023. IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones.

[2] A. Khazraei, H. Meng, M. Pajic, Stealthy perception-based attacks on unmanned aerial vehicles, arXiv Prepr. arXiv:2303 02112 (2023).

[3] T.T. Khoei, G. Aissou, K. Al Shamaileh, V.K. Devabhaktuni, N. Kaabouch, Supervised deep learning models for detecting GPS spoofing attacks on unmanned aerial vehicles. in: Proceedings of the 2023 IEEE International

Conference on Electro Information Technology (EIT), IEEE, 2023, pp. 340–346.

[4] R.A. Agyapong, M. Nabil, A.R. Nuhu, M.I. Rasul, A. Homaifar, Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning. in: Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, 2021, pp. 01–08.

[5] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A.K. Bashir, F.A. Khan, Securing critical infrastructures: deep-learning-based threat detection in IIoT, IEEE Commun. Mag. 59 (10) (2021) 76–82.

[6] Q. Abu Al-Haija, A. Al-Badawi, High-performance intrusion detection system for networked UAVs via deep learning, Neural Comput. Appl. 34 (13) (2022) 10885–10900.

[7] R.A. Ramadan, A.H. Emara, M. Al-Sarem, M. Elhamahmy, Internet of drones intrusion detection using deep learning, Electronics 10 (21) (2021) 2633.

[8] Y. Sun, M. Yu, L. Wang, T. Li, M. Dong, A deep-learning-based GPS signal spoofing detection method for small UAVs, Drones 7 (6) (2023) 370.

[9] V. Sadhu, K. Anjum, D. Pompili, Onboard deep-learning-based unmanned aerial vehicle fault cause detection and classification via FPGAs, IEEE Trans. Robot. (2023).

[10] Y. Dang, C. Benzaïd, B. Yang, T. Taleb, Deep learning for GPS spoofing detection in cellular-enabled UAV systems. in: Proceedings of the 2021 International Conference on Networking and Network Applications (NaNA), IEEE, 2021, pp. 501–506.

[11] S.M. Alshammari, N.A. Alganmi, M.H. Ba-Aoum, S.S. Binyamin, A.L. Abdullah, M. Ragab, Hybrid arithmetic optimization algorithm with deep learning model for secure Unmanned Aerial Vehicle networks, AIMS Math. 9 (3) (2024) 7131–7151.

[12] L. Kou, S. Ding, T. Wu, W. Dong, Y. Yin, An intrusion detection model for a drone communication network in an SDN environment, Drones 6 (11) (2022) 342.

[13] J. Escorcia-Gutierrez, M. Gamarra, E. Leal, N. Madera, C. Soto, R.F. Mansour, M. Alharbi, A. Alkhayyat, D. Gupta, Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment, Comput. Electr. Eng. 108 (2023) 108704.

[14] Al-Quayed, F., Ahmad, Z. and Humayun, M., 2024. A situation-based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0. IEEE Access.

[15] Z. Li, Q. Chen, W. Mo, X. Wang, L. Hu, Y. Cao, December. Converging Blockchain and Deep Learning in UAV Network Defense Strategy: Ensuring Data Security During Flight. In International Conference on Artificial Intelligence Security and Privacy, Springer Nature Singapore, Singapore, 2023, pp. 156–171.

[16] K.A. Alissa, S.S. Alotaibi, F.S. Alrayes, M. Aljebreen, S. Alazwari, H. Alshahrani, M. Ahmed Elfaki, M. Othman, A. Motwakel, Crystal structure optimization with deep-autoencoder-based intrusion detection for secure internet of drones environment, Drones 6 (10) (2022) 297.

[17] Y.A. Alsariera, W.F. Awwad, A.D. Algarni, H. Elmannai, M. Gamarra, J. Escorcia- Gutierrez, Enhanced Dwarf Mongoose optimization algorithm with deep learning- based attack detection for drones, Alex. Eng. J. 93 (2024) 59–66.

[18] L.M. Da Silva, I.G. Ferr˜ ao, C. Dezan, D. Espes, K.R. Branco, June. Anomaly-based intrusion detection system for in-flight and network security in UAV swarm. In 2023. International Conference on Unmanned Aircraft Systems (ICUAS), IEEE, 2023, pp. 812–819.

[19] V. Saravanan, M. Madiajagan, S.M. Rafee, P. Sanju, T.B. Rehman, B. Pattanaik, IoT- based blockchain intrusion detection using optimized recurrent neural network, Multimed. Tools Appl. 83 (11) (2024) 31505–31526.

[20] Z. Li, Q. Chen, W. Mo, X. Wang, L. Hu, Y. Cao, December. Converging Blockchain and Deep Learning in UAV Network Defense Strategy: Ensuring Data Security During Flight. In International Conference on Artificial Intelligence Security and Privacy, Springer Nature Singapore, Singapore, 2023, pp. 156–171.

[21] A. Aljabri, F. Jemili, O. Korbaa, Convolutional neural network for intrusion detection using blockchain technology, Int. J. Comput. Appl. 46 (2) (2024) 67–77.

[22] Y. Liu, P. Liu, W. Jing, H.H. Song, Pd2s: a privacy-preserving differentiated data sharing scheme based on blockchain and federated learning, IEEE Internet Things J. (2023).

[23] Z. Li, Q. Chen, J. Li, J. Huang, W. Mo, D.S. Wong, H. Jiang, A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning, Comput. Stand. Interfaces 90 (2024) 103844.

[24] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, A.N. Islam, Digital twin- driven SDN for smart grid: a deep learning integrated blockchain for cybersecurity, Sol. Energy 263 (2023) 111921.

[25] D. Dansana, P.K. Behera, S.G.K. Patro, Q.N. Naveed, A. Lasisi, A.W. Wodajo, BSMACRN: design of an efficient blockchain-based security model for improving attack-resilience of cognitive radio Ad-hoc networks, IEEE Access (2024).

[26] J.B. Awotunde, T. Gaber, L.N. Prasad, S.O. Folorunso, V.L. Lalitha, Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain, Scalable Comput.:Pract. Exp. 24 (3) (2023) 561–584

[27] A.S. Reegan, P.M. Sivaraja, S. Mamitha, C.B. Rogers, IoT Medical sensor data security and privacy using blockchain based multiparty authentication protocol in WSN, Adhoc Sens. Wirel. Netw. 59 (2024).

[28] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, S. Kumar, SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi- LSTM-CNN. Trans. Emerg. Telecommun. Technol. 34 (11) (2023) e4758.

[29] T. Si, P.B. Miranda, U. Nandi, N.D. Jana, S. Mallik, U. Maulik, H. Qin, Opposition- based chaotic tunicate swarm algorithms for global optimization, IEEE Access (2024)