ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20241130002158
Original scientific paper

Quantum Chameleon Swarm Optimizer-Based Feature Selection with Deep Learning for Intrusion Detection in Blockchain-Enabled IoT Environments

Usha SUBRAMANIAM*, Sudhakar THIRUVENKATASAMY, Eatedal ALABDULKREEM, Nuha ALRUWAIS

Abstract: As the number of networked devices continues to rise, Internet of Things (IoT) settings are becoming increasingly susceptible to cyberattacks. As a result, intrusion detection systems (IDS) are becoming increasingly important in these environments. In order to identify unwanted access or abnormalities, an effective IDS observes the interactions between devices, the traffic on the network, and the behavior of users. Additionally, it enforces stringent access limits, encryption, and real-time monitoring. When it comes to protecting the integrity of IoT devices and data, prompt detection and reaction to security issues are very necessary. Blockchain technology, which has a distributed and tamper-proof ledger, offers a secure basis for IoT systems. However, it necessitates the implementation of complementing cybersecurity procedures. An approach known as Quantum Chameleon Swarm Optimizer-based Feature Selection with Deep Learning for Intrusion Detection (QCSOFS-DLID) is presented in this paper for use in Internet of Things scenarios that are enabled by Blockchain technology. An approach known as QCSOFS-DLID incorporates Blockchain technology for the purpose of ensuring secure communication, feature selection (FS) through the utilization of the proposed algorithm for the purpose of detecting attacks. Blockchain technology is used in the QCSOFS-DLID strategy to ensure that IoT systems have secure communication protocols. A Convolutional Variational Autoencoder (CVAE) model is utilized for the purpose of detecting intrusions, while the QCSO technique is utilized for the purpose of effective feature selection. Through the utilization of the Coot Optimization Algorithm (COA), the hyperparameters of the model are fine-tuned. In this study, the QCSOFS-DLID approach is assessed using the BoT-IoT dataset. The experimental findings reveal that the method's performance is superior to that of existing state-of-the-art methodologies through comparison. Blockchain technology, feature selection, and deep learning are all successfully integrated into this strategy, which aims to improve intrusion detection and further strengthen security in Internet of Things environments.

Keywords: Blockchain; Deep learning; Internet of Things (IoT); Intrusion Detection System (IDS); Quantum Chameleon Swarm Optimizer (QCSO)

1 INTRODUCTION

The Internet of Things (IoT) is a significant contributor to the advancement of the medical business. Moreover, it serves as a crucial and fundamental source of information pertaining to healthcare, as physical devices gather essential data through various sensors and subsequently transmit this information in real time to healthcare resources via internet connectivity [1]. The storage of clinical large data in a network system, reliant on cloud-client servers susceptible to single-point failure, along with centralised resource management, leads to a compromise of confidentiality [2-4]. To facilitate the creation of botnets utilising the Internet of Things, it is assured that Internet of Things devices may be readily compromised and manipulated remotely. These botnets and attacks result in the leakage of sensitive data, as well as violations and breaches in extensive systems facilitated by the Internet of Things [5]. Ransomware, distributed denial-of-service (DDoS), denial-of-service (DoS), and botnet attacks represent prevalent forms of assaults on IoT platforms. This may result in considerable research efforts in the domain of security and authentication complexity for Internet of Things-enabled medical systems [6]. The exploration of medical applications utilising machine learning (ML) has progressed rapidly. Only a limited number of machine learning algorithms are employed in illness diagnosis, whereas others are applied in intrusion detection systems (IDS) to uncover security vulnerabilities [7]. The limited resources for evaluations in IoT devices necessitate the implementation of IDS techniques.

Blockchain has emerged as a decentralised and extremely secure environment that is readily accessible. The data exhibits immutability, tamper-proofing, integrity, secrecy, traceability, and privacy, all without requiring third-party engagement. It is [8]. A significant number of research personnel have recognised the BC application as an effective security measure for medical systems. Given that BC holds importance in the medical domain, it may engage in issues that extend beyond conventional considerations of openness and security [9]. The intrusion detection system (IDS) must be intelligent and efficient to identify and mitigate both known and undiscovered threats, specifically through anomaly detection, to ensure network security. Although it has a higher false alarm rate (FAR), anomaly detection can identify both novel and established security breaches [10]. Machines and computers can attain Artificial Intelligence (AI) by learning from a database with minimal human interaction; IDS can leverage this potential. Machine learning (ML) and deep learning (DL) are subfields of artificial intelligence (AI) with the potential to enhance the development and efficacy of intrusion detection systems (IDS) [11]. The classification and identification of network traffic using a machine learning approach relies on manually extracted features. The DL methodology, in conjunction with its neural network (NN), is tasked with extracting features from the database and subsequently performing classification and identification. Nonetheless, deep learning possesses the capacity to augment and boost the detection accuracy of the system compared to machine learning [12].

2 RELATED WORKS

The FED-IDS framework was created by Abdel-Basset and associates [13]. To train spatial-temporal symbols of vehicle traffic flows essential for identifying various attack kinds, the technique develops a contextualised moderniser system. BC-managed federated training aims to enable numerous edge nodes to provide training that is reliable, decentralised, and assured among participants. To create an effective BC-assisted Internet of Things Healthcare System, Alamro et al. [14] employed an Ant Lion Optimiser alongside a Hybrid Deep Learning (BHS-ALOHDL) application. This method is an application of ALO-FSS, which denotes ALO-based

feature subset selection. The HDL network employs a hybrid of CNN and LSTM models to produce IDs. The demoralisation of the flower pollination algorithm (FPA) has been successfully completed to facilitate optimal hyperparameter adjustment. Kumar et al. [15] developed effective distributed IDs using fog computing to distinguish between distributed denial of service attacks and mining pools in blockchain-enabled Internet of Things devices. The procedure involves training an enhanced XGBoost alongside RF on disseminated fog nodes.

The paper [16] delineates the formulation of a standardised architecture for the collaborative ensemble BC technique (CEBM) applicable to IDs within the Internet of Things ecosystem. Leveraging this basis, the intrusion detection system (IDS) units can safely transmit data and establish an ensemble recognition methodology. This is achieved by integrating diverse machine learning algorithms with optimal outcomes through a verified technique utilising BC. This is executed in the absence of a reliable intermediary. A unique approach termed BC-based IoMT Authenticated Key Exchange (BIoMTAKE) is introduced in [17] to create a private BC-based decentralised environment utilising Hyperledger Fabric. Both a formal and an informal safety assessment have been completed on the planned BIoMTAKE. The formal investigation was executed with the Scyther computer program. Furthermore, cryptography libraries and Hyperledger Fabric are employed to complete the performance evaluation.

Alkadi et al. [20] introduced a Deep Blockchain Framework (DBF) aimed at delivering privacy-centric blockchain solutions and secure distributed identities in the cloud with seamless integrations. To manage sequential system data, the IDs model is implemented using the BiLSTM method, a deep learning technique [19] describes the creation of an innovative Federated-learning framework based on BC. This investigation's architecture integrates the benefits of a Hyperledger Fabric network with Federated Learning. This was executed to attain skill and mastery through the learning process of IDs. By employing the traditional federated learning process, the blockchain network acts as a substitute for the frequently used huge server. Furthermore, the proposed technique leverages the fundamental attributes inherent in BC and FL [21, 22].

3 THE PROPOSED MODEL

Within the context of a blockchain-enabled Internet of Things healthcare framework, the primary focus of this inquiry is the development of an automated and accurate intrusion detection system that makes use of the QCSOFS-DLID approach. For the purpose of identifying and classifying invasions, the QCSOFS-DLID technique employs a combination of BC principles, FS, and hyperparameter-optimized direct learning methods. The BC module, CVAE classification, QCSO-based feature subset selection, and COA-based hyperparameter tuning are some of the subprocesses that are included in this system. Fig. 1 illustrates each step of the QCSOFS-DLID approach, which is a comprehensive process. The transmission of information facilitated by BC.

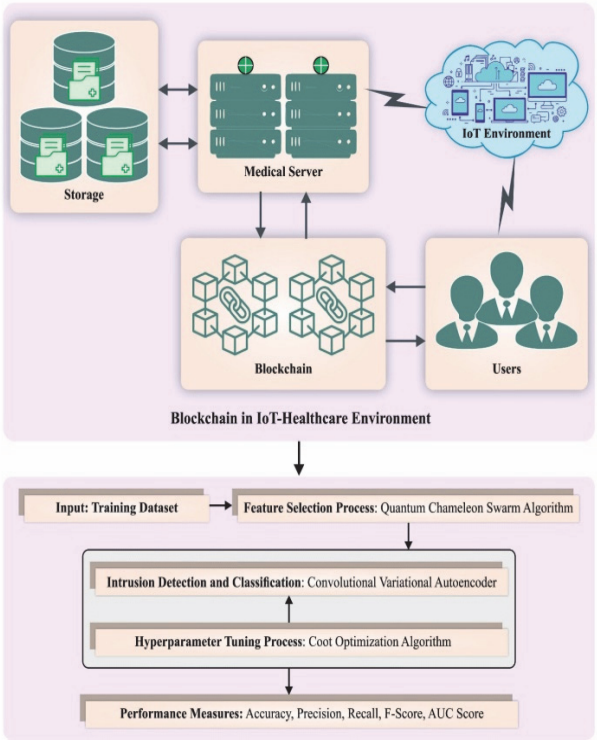

Figure 1 Overall process of QCSOFS-DLID algorithm

A secure communication protocol is utilized inside the Internet of Things (IoT) healthcare sector using the BC technique that is included in the QCSOFS-DLID technology. It is via the utilization of the communication protocol that this is accomplished. Through the implementation of a secure communication protocol that is founded on blockchain technology, it is possible to find a workable solution to the crucial problems of data accessibility, privacy, and integrity that are prevalent in the healthcare industry. Through the utilization of blockchain technology, healthcare organizations are able to guarantee the safe and unchangeable transmission of sensitive patient data across a wide variety of stakeholders, such as patients, hospitals, and insurance providers. By virtue of its decentralised ledger and encryption capabilities, blockchain technology makes it possible to transmit and store data in a safe manner. To establish an immutable chain of blocks, each transaction is cryptographically linked to its predecessor. This chain of blocks can only be modified with the unanimous agreement of all network participants. This generates an access audit record, which safeguards the integrity of patient data while enhancing confidence and accountability.

3.1 Utilisation of the QCSO Algorithm for Feature Selection

The attribute selection technique has been completed utilizing the QCSO algorithm. Chameleons are diagnosed for his or her searching behaviors of their natural environment, which stimulated the biologically-primarily based CSO algorithm. Initially, the optimizer will utilize an n-dimensional space and m chameleon parameters to define its populace inside the search range. Each member occupies a role at a particular generation tt and independently delineates a strategy to the problem as follows: At new release tt, the position of the jjth chameleon is represented as a vector containing nn

dimensions, expressed as: "The position of chameleon jj at iteration tt includes values across all dimensions from one to nn." In this placing: jj stages from 1 to mm, wherein mm denotes the entire variety of chameleons. The generation to be counted is represented with the aid of tt. The problem dimension is indicated by way of nn. The chameleon's region at a particular size is denoted consequently.

The populace is mounted randomly in step with the subsequent components: "The preliminary position of each chameleon is determined with the aid of the decrease certain plus a randomly generated issue extended by the distinction between the upper and lower bounds." The beginning position of the jjth chameleon is represented by a variable. A randomly generated variety among 0 and 1 impacts the initial placement. The upper and lower limits of the quest range define the limits for initialization. The satisfactory of the answer at the chameleon's updated position may be assessed using the fitness characteristic as a criterion. The closing degree is to decorate the nice of the answer by way of updating the prevailing area. If the updated place outcomes in a worse first-rate answer, the chameleon does not circulate relative to its current position. The chameleon's function for the duration of the prey-seeking technique may be adjusted based on the subsequent principle: "If a chameleon perceives an ultimate function, it moves toward it primarily based on an aggregate of its current position, the great solution on the generation, and the global exceptional answer, encouraged by means of random values and manage parameters. If belief isn't always triggered, the chameleon relocates randomly in the seek space." The up to date function at new release $t + 1$ $t + 1$ is decided based on the previous function at tt, the quality solution at generation tt, and the worldwide most fulfilling. Several randomly generated elements affect motion. A time decay factor is introduced to regulate motion over iterations.

The line connecting the satisfactory and worldwide solutions is described as follows: "A mathematical feature determines an intermediate factor between the exceptional and global most beneficial answers, inspired by a random weighting factor." The chameleon's function alongside this path is decided through: "A linear mixture of the intermediate role and a secondary thing influences the new position of the chameleon, ensuring flexibility in movement within the defined range." A point common to all positions on this transformation is described because of the chameleon's present location at iteration tt. Chameleons, using their excellent visual abilties, can become aware of the location in their prey by rotating their eyes thru a full 360-degree variety. The chameleon's new region can be determined by means of the following precept: "The chameleon's new function after rotation is derived from the rotation middle and the centroid of its motion." The updated role is influenced by a centroid cost. The coordinates of the rotation center define the brand new movement direction. The mathematical transformation for rotation is: "The rotation middle is decided through multiplying a rotation matrix by means of a predefined centroid coordinate." The rotation matrix defines the diploma of transformation. The coordinate transformation allows regulate the chameleon's route.

The rotation middle itself is calculated as: "The new center for rotation is derived by subtracting the centroid from the chameleon's position at iteration tt." The chameleon's pace influences its motion in proximity to prey, defined as follows: "The new role of the chameleon is up to date primarily based at the difference between the square of its modern-day pace and its pace from the preceding iteration, divided with the aid of an acceleration factor." Velocity changes from new release $t - 1$ $t - 1$ to tt effect motion. The acceleration issue debts for slow or fast motion modifications. In the context of quantum-based optimization (QBO), each characteristic is represented as a quantum bit, which determines whether the feature is selected or eliminated. The Q-bit is mathematically represented as: "A Q-bit is a quantum representation that exists in a superposition of binary states, mathematically expressed with a complex exponential feature where the sum of squared magnitudes equals one." The perspective related to the Q-bit is up to date based on: "The Q-bit attitude has modified the usage of the arctangent function to adjust its opportunity distribution among zero and 1." The replace of the Q-bit follows: "The Q-bit state at the following iteration is determined with the aid of applying a rotational transformation matrix to its current kingdom" where the rotation transformation matrix is given with the aid of: "A two-dimensional rotation matrix is used to adjust the Q-bit values, making sure controlled rotation is based totally on a most reliable solution." The rotation angle is adjusted based totally on the excellent solution located to date. The transformation ensures efficient optimization over more than one iteration. This textual content successfully translates the mathematical equations into descriptive causes whilst retaining the logical waft of the QCSO algorithm.

The COA algorithm is a unique metaheuristic algorithm based on the integration of population dynamics and randomisation principles [23-25]. During their foraging activities, coots, medium-sized aquatic birds, display behaviour that is described by the mathematical model. When individuals require sustenance, they assemble in huge groups and journey collectively into the wilderness. This is due to the evaluation of the defining characteristics of the coot bird species. Furthermore, the COA mandates the gathering of preliminary random replies, which are subsequently refined based on the two methodologies. The execution and generation of the update protocol and initial solution set are conducted as follows:

$\mathrm{Bound}^{\mathrm{up}}$ and $\mathrm{Bound}^{\mathrm{low}}$ refer to the upper and lower bounds of the initial solution set. These limits denote the extremities of the control variable involved in the optimisation issue. In the instance of $\mathrm{Coot}_{\mathrm{c}}$, where c is a numeral between 1 and S_{Po}, with S_{Po} being the population value, each $\mathrm{Coot}_{\mathrm{c}}$ is produced inside the interval $\left[\mathrm{Bound}^{\mathrm{low}}, \mathrm{Bound}\right]^{\mathrm{up}}$. There exists a low-quality set designated as $\mathrm{MCoot}_{\mathrm{a}}$ and a high-quality set referred to as $\mathrm{LCoot}_{\mathrm{b}}$. Each of the two sets has $\mathrm{N}_{\mathrm{low}}$ solutions and $\mathrm{N}_{\mathrm{high}}$ solutions, respectively.

4 RESULTS AND DISCUSSION

This study validates the findings of the QCSOFS-DLID technique for intrusion detection utilising the BoT-IoT database [26, 27], which comprises 3,673 instances across ten categories, as detailed in Tab. 1.

Table 1 Details on database

Classes	Labels	No. of Instances
Service Scanning	A1	300
OS Fingerprinting	A2	300
DDoS TCP	A3	300
DDoS UDP	A4	300
DDoS HTTP	A5	300
DoS TCP	A6	300
DoS UDP	A7	300
DoS HTTP	A8	300
Normal	A9	300
Keylogging	A10	75
Total No. of Instances		2775

The outcomes of the proposed method, according to an 80:20 ratio of the training to the testing phase, are illustrated in Tab. 2 and Fig. 4. The data indicate that the proposed model is capable of effectively executing the detection procedure. The QCSOFS-DLID method attains average metrics of 97.83%, 97.15%, 97.60%, 97.91%, and 98.20% for accuracy, precision, recall, F-score, and AUCscore for 80% of the training phase, respectively. The proposed technique attains average values of 98.93%, 98.62%, 99.13%, 98.37%, and 98.55% for accuracy, precision, recall, *F*-score, and AUCscore, respectively, when applied with 20% of the testing phase.

We have created accuracy curves for both the training phase and the testing phase, as shown in Fig. 5. This was done in order to evaluate the effectiveness of the QCSOFS-DLID approach, which makes use of an 80:20 ratio of training phase to testing phase. A significant amount of information on the generalization capabilities of the model and its learning development may be gleaned from these curves. When the number of epochs is increased, it is possible to witness a discernible improvement in the accuracy curves of both the training set and the testing set. The fact that the model is now able to recognize patterns in both the training and testing databases is demonstrated by this improvement.

Table 2 Intrusion detection outcome of BAFWO-MLID algorithm on 80:20 of TR set/TS set

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TR Phase (80%)					
A1	98.60	97.21	98.00	97.65	98.44
A2	98.81	97.48	98.60	97.09	98.76
A3	98.77	98.05	97.74	97.80	98.32
A4	98.77	98.36	97.41	97.89	98.1\
A5	98.60	97.44	97.73	97.59	98.28
A5	98.94	98.38	99.01	98.69	98.97
A6	9/.98	99.01	98.60	98.86	98.86
A7	98.87	98.08	98.60	98.39	98.70
A9	98.74	98.38	97.14	97.76	98.04
A10	98.91	99.01	95.75	96.31	96.38
Average	97.83	97.15	97.60	97.91	98.20
TS Phase (20%)					
A1	99.01	99.01	99.01	99.01	99.01
A2	98.74	97.71	97.71	97.71	98.28
A3	98.87	97.85	99.01	98.43	98.93
A4	99.01	99.01	99.01	99.01	99.01
A5	98.87	99.01	97.81	98.30	98.41
A5	99.01	99.01	99.01	99.01	99.01
A6	98.87	97.68	99.01	98.34	98.93
A7	99.01	98.01	99.01	99.01	99.01
A9	99.01	99.01	99.01	99.01	99.01
A10	98.87	99.01	94.76	97.78	97.89
Average	98.93	98.63	98.13	98.37	98.55

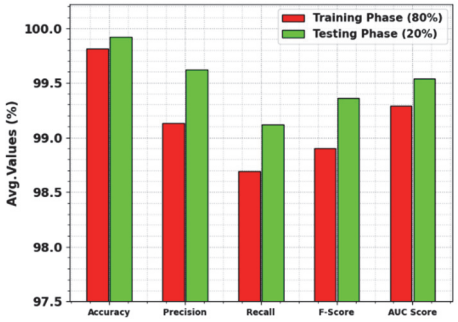

Figure 2 Average of QCSOFS-DLID approach with 80:20 of TR phase/TS phase

Furthermore, Fig. 6 illustrates a summary of the loss values associated with the proposed approach throughout the training period. The decreasing training loss throughout the epochs indicates that the model is progressively optimising its weights to minimise mistakes in both the training and testing values. This loss curve considers the extent to which the model accurately fits the training data.

This is especially significant as it demonstrates that the model is successfully acquiring patterns evident in both datasets. The ongoing decrease in training and testing loss is especially symptomatic of this. Moreover, it demonstrates the model's capacity to adapt in order to minimise the discrepancies between the results of the predicted training labels and the original training labels used during training.

Figure 3 Accuracy curve of QCSOFS-DLID approach with 80:20 of TR phase/TS phase

Figure 4 LQCSOFS-DLID approach's oss curve with an 80:20 TR/TS phase ratio

Table 3 Intrusion recognition analysis of QCSOFS-DLID approach with 70:30 of TR phase/TS phase

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TR Phase (70%)					
A1	98.35	96.38	95.29	97.83	96.90
A2	98.49	88.26	96.87	94.37	97.22
A3	98.66	97.80	96.82	98.36	97.85
A4	98.89	99.01	97.97	98.49	98.49
A5	98.60	98.25	96.82	97.51	97.87
A5	98.47	97.96	95.26	96.59	97.07
A6	98.39	95.31	96.73	96.02	97.67
A7	98.40	97.80	95.41	96.62	97.15
A9	98.31	96.91	94.80	95.88	96.82
A10	98.66	88.84	93.65	91.16	96.21
Average	98.44	95.67	95.97	95.77	97.33
TS Phase (30%)					
A1	98.47	97.46	95.96	96.60	97.38
A2	97.65	87.80	99.01	93.13	98.25
A3	98.92	99.01	98.22	98.61	98.61
A4	98.83	99.01	9\.21	98.00	98.11
A5	98.47	96.63	96.63	96.63	97.67
A5	98.37	99.01	92.47	95.63	95.74
A6	98.28	96.02	96.02	96.02	97.31
A7	98.47	95.78	97.37	96.57	97.99
A9	98.19	98.02	91.50	94.60	95.26
A10	98.83	88.48	99.01	92.45	98.92
Average	98.43	95.73	96.33	95.96	97.52

The outcomes of the intrusion detection conducted by the QCSOFS-DLID system, employing a 70:30 ratio between the TR phase and the TS phase, are illustrated in Tab. 3 and Fig. 7, respectively. The simulation results indicated that the QCSOFS-DLID system was capable of executing the detection method efficiently. Furthermore, using 70% of the TR phase, the QCSOFS-DLID methodology achieves average accuracy, precision, recall, F-score, and AUC score values of 98.44%, 95.67%, 95.97%, 95.77%, and 98.33%, respectively. The QCSOFS-DLID method attains average metrics of 98.45%, 95.73%, 98.35%, 95.96%, and 97.52% for accuracy, precision, recall, F-score, and AUCscore, respectively, at a TS phase of thirty percent.

To assess the efficacy of the QCSOFS-DLID methodology at a 70:30 ratio between the training (TR) phase and the testing (TS) phase, we have produced accuracy curves for both phases, as illustrated in Fig. 8. These curves provide valuable insights on the model's learning progress and its ability to generalise new knowledge. With the augmentation of epochs, it is evident that the TR and TS accuracy curves are demonstrating symptoms of enhancement. This enrichment illustrates that the model can identify patterns inside both the TR database and the TS database.

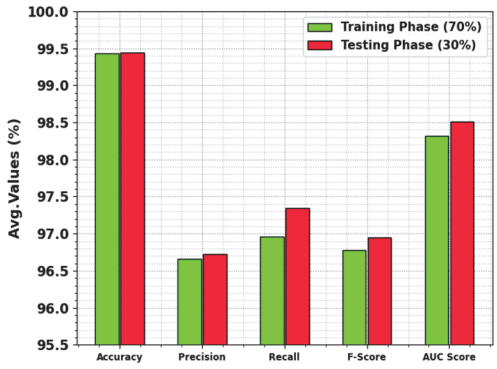

Figure 5 QCSOFS-DLID approach average with 70:30 TR/TS phase

5 CONCLUSION AND FUTURE WORK

In the framework of a blockchain-enabled Internet of Things healthcare environment, the principal aim of this project is to create an automated and precise intrusion detection system utilising the QCSOFS-DLID methodology. The identification and classification of

invasions are achieved through the application of a mix of BC principles, FS, and a hyperparameter-optimized DL model utilising the QCSOFS-DLID approach. This system encompasses subprocesses such as the BC module, CVAE classification, QCSO-based feature subset selection, and COA-based hyperparameter optimisation. The BC method in the QCSOFS-DLID technology employs a secure communication protocol inside the Internet of Things (IoT) healthcare sector. This is achieved through the use of the communication protocol. In the context of the QCSOFS-DLID methodology, the QCSO algorithm is employed to facilitate effective feature selection. The CVAE technique is employed in the realm of intrusion detection alongside classification strategies. In conclusion, the COA is employed to optimise the parameters of the CVAE model. The BoT-IoT dataset facilitates the examination of experimental outcomes associated with the QCSOFS-DLID classification models.

The comprehensive findings indicate that the QCSOFS-DLID technique is markedly more efficient than the presently recognised state-of-the-art methods.

Acknowledgements

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R161), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2025R608), King Saud University, Riyadh, Saudi Arabia.

6 REFERENCES

[1] Kavitha, S., Uma Maheswari, N., & Venkatesh, R. (2023). Intelligent intrusion detection system using enhanced arithmetic optimization algorithm with deep learning model. *Tehnički vjesnik - Technical Gazette*, *30*(4), 1217-1224. https://doi.org/10.17559/TV-20221128071759

[2] Sarac Güleryüz, S., & Koyuncu, M. (2023). Simulation of intensive care bed capacity based on mixture distribution. *International Journal of Simulation Modelling, 22*(2), 221–232. https://doi.org/10.2507/IJSIMM22-2-637

[3] Vinoth Kumar, K. & Thiruppathi, M. (2023). Oppositional Coyote Optimization based feature selection with deep learning model for intrusion detection info gassisted wireless sensor network. *Acta Montanistica Slovaca*, *28*(2). https://doi.org/10.46544/AMS.v28i2.18

[4] Buschiazzo, M., Mula, J., & Campuzano-Bolarín, F. (2020). Simulation optimization for the inventory management of healthcare supplies. *International Journal of Simulation Modelling, 19*(2), 255–266. https://doi.org/10.2507/IJSIMM19-2-514

[5] Thiruvenkatasamy, S., Sivaraj, R., & Vijayakumar, M. (2024). Blockchain assisted fire works optimization with machine learning based in trusion detection system (IDS). *Tehnički vjesnik - Technical Gazette*, *31*(2), 596-603. https://doi.org/10.17559/TV-20230712000798

[6] Ahmed, M. A., Althubiti, S. A., Rao, D. N., Lydia, E. L., Cho, W., Joshi, G. P., & Kim, S. W. (2022). Blockchain assisted intrusion detection system using different flower pollination model. *Computers, Materials &Continua*, *73*(3). https://doi.org/10.32604/cmc.2022.022214

[7] Sharadqh, A. A., Hatamleh, H. A. M., Saloum, S. S., & Alawneh, T. A. (2023). Hybrid Chain: Blockchain-enabled framework for bi-level intrusion detection and graph-based mitigation for security provision inginedge-assisted IoT environment. *IEEE Access*, *11*, 27433-27449. https://doi.org/10.1109/ACCESS.2023.3256277

[8] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal*, *8*(12), 9463-9472. https://doi.org/10.1109/JIOT.2020.2996590

[9] Ashraf, E., Areed, N. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022). Fidchain: Federated intrusion detection system for blockchain-enabled IoT health care applications. *Healthcare, 10*(6), Article 1110. https://doi.org/10.3390/healthcare10061110

[10] Alevizos, L., Eiza, M. H., Ta, V. T., Shi, Q., & Read, J. (2022). Blockchain-enabledin trusion detection and prevention system of APT swithin zero trust architecture. *IEEE Access*, *10*, 89270-89288. https://doi.org/10.1109/ACCESS.2022.3200165

[11] Zhang, X., Mo, T., & Zhang, Y. (2023). Optimization of storage location assignment for non-traditional layout ware houses based on the fire work algorithm. *Sustainability*, *15*(13), Article 10242. https://doi.org/10.3390/su151310242

[12] Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M. A., Mukherjee, M., & Khan, F. A. (2019). Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors*, *19*(14), 3119. https://doi.org/10.3390/s19143119

[13] Vinoth Kumar, K. & Rajakani, V. (2024). Modeling of intrusion detection system using double adaptive weighting arithmetic optimization algorithm with deep learning on Internet of Things environment. *Brazilian Archives of Biologyand Technology*, *67*, e24231010. https://doi.org/10.1590/1678-4324-2024231010

[14] Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S., & Idris, N. B. (2020). Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems. *Electronics*, *9*(7), Article 1120. https://doi.org/10.3390/electronics9071120

[15] Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2021). Federated intrusion detectionin blockchain-based smart transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2523-2537. https://doi.org/10.1109/TITS.2021.3060604

[16] Alamro, H., Marzouk, R., Alruwais, N., Negm, N., Aljameel, S. S., Khalid, M., Hamza, M. A., & Alsaid, M. I. (2023). Modelling of blockchain assisted intrusion detection on IoT healthcare system using antlion optimizer with hybrid deep learning. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3299589

[17] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attack sinblock chain-enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55-68. https://doi.org/10.1016/j.jpdc.2022.04.005

[18] Rajakani, V. & Vinoth Kumar, K. (2023). Barnaclesmating optimizer with Hopfield neural network based in trusion detection in Internet of Things environment. *Tehnički vjesnik - TechnicalGazette*, *30*(6). https://doi.org/10.17559/TV-20211216115635

[19] Tomar, A., Gupta, N., Rani, D., & Tripathi, S. (2023). Blockchain-assisted authenticated key agreement scheme for IoT-based health care system. *Internet of Things*, Article 100849. https://doi.org/10.1016/j.iot.2023.100849

[20] Alkadi, O., Moustafa, N., & Turnbull, B. (2021). A collaborative intrusion detection system using deep blockchain framework for securing cloud networks. In Y. Bi, S. Kapoor, & R. Bhatia (Eds.). *Intelligent Systems and Applications*, *1*, 553-565. https://doi.org/10.1007/978-3-030-55180-3_41

[21] Zaabar, B., Cheikhrouhou, O., & Abid, M. (2022). Intrusion detection system for IoMT through blockchain-based federated learning. *15th International Conference on Security of Information and Networks (SIN)*, 1-8. https://doi.org/10.1109/SIN56466.2022.9970536
[22] Thiruppathi, M. & Vinoth Kumar, K. (2023). Seagull optimization-based feature selection with optimal extreme learning machine for intrusion detection info gassisted WSN. *Tehnički vjesnik - TechnicalGazette*, *30*(5). https://doi.org/10.17559/TV-20211216115635
[23] Elaziz, M. A., Ahmadein, M., Ataya, S., Alsaleh, N., Forestiero, A., & Elsheikh, A. H. (2022). A quantum-based chameleons warm for feature selection. *Mathematics, 10*(19), 3606. https://doi.org/10.3390/math10193606
[24] Memarzadeh, M., Matthews, B., & Avrekh, I. (2020). Un supervise danomaly detection in flight data using convolutional variational auto-encoder. *Aerospace*, *7*(8), 115. https://doi.org/10.3390/aerospace7080115
[25] Nguyen, T. T. T. (2023). Coot bird behavior-based optimization algorithm for optimal placement of thyristor controlled series compensator devices in transmission power networks. *Advancesin Electrical and Electronic Engineering*, *21*(3), 171-183. https://doi.org/10.15598/aeee.v21i1.4515
[26] UNSW Canberra. (n.d.). *BoT-IoT dataset*.
[27] Alosaimi, S. & Almutairi, S. M. (2023). Anin trusion detection system using BoT-IoT. *Applied Sciences*, *13*(9), 5427. https://doi.org/10.3390/app13095427
[28] Chauhan, S., Gangopadhyay, S., & Gangopadhyay, A. K. (2022). Intrusiondetection system for IoT using logical analysis of data and information gainratio. *Cryptography*, *6*(4), 62. https://doi.org/10.3390/cryptography6040062

Contact information:

Usha SUBRAMANIAM, Assistant Professor (Sr.Gr)
(Corresponding author)
Department of Computer Science and Engineering,
University College of Engineering BIT Campus,
Anna University, Tiruchirappalli, India
E-mail: anbuselvamusha2000@yahoo.co.in

Sudhakar THIRUVENKATASAMY, Assistant Professor
Department - Computer Science and Engineering,
Nandha College of Technology, Erode - 638052, India
E-mail: thiruvenkatasamys86@gmail.com

Eatedal ALABDULKREEM
Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University,
P.O. Box 84428, Riyadh 11671, Saudi Arabia
E-mail: ealbdulkaream@pnu.edu.sa

Nuha ALRUWAIS
Department of Computer Science and Engineering,
College of Applied Studies and Community Services,
King Saud University,
Saudi Arabia, P.O. Box 22459, Riyadh 11495, Saudi Arabia
E-mail: nwrowais@ksu.edu.sa