

A Hybrid Adversarial Intelligence Framework Integrating Ag-Gan Classification And Ntru-Aes Cryptography For Adaptive IOT Cyber Defense

Chethan M S^{*1}, Channakrishnaraju²

¹Research Scholar, Department of Computer Science and Engineering, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

²Assistant Professor, Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka, India.

³Professor and HOD, Artificial Intelligence and Machine Learning, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

*Corresponding Author Email: chethanms@gmail.com

Abstract

Development of CNs (Computer Networks) and IoT (Internet of Things) has drawn more attention to cyber security. Based on recent internet usage, a number of malware apps have become increasingly common, which pose a severe threat to computer security. Recently, a number of centralized mechanisms have been recommended for the detection of assaults in the IoT. However, because of the various requirements of IoT devices, including resource constraints, scalability and reduced latency these approaches were failed to yield significant outcomes. Therefore, hybrid N-th degree Truncated polynomial Ring Units-Advanced Encryption Standard (NTRU-AE) cryptography-based encryption algorithms and improved GAN-based cyber-attack detection systems have been designed to enhance network security. The suggested methodology gathers the IoT data and employs two-factor authentication (2FA) to verify the IoT data with two different types of authentication factors. After verification, authenticated data is utilized for preprocessing and feature selection. The suggested K-means clustering (KMC) approach removes inaccurate and missing data during pre-processing, and the embedding strategy extracts the most important features for each attack. After that, the relevant data is fed into a GAN classifier based on AG, resulting in an accurate prediction regarding whether a cyber-threat is detectable or normal. If the prediction is normal, a hybrid NTRU-AES cryptographic technique is used to secure and protect normal data; if not, the procedure is terminated. The system performs better computationally than the examined current methods, according to performance evaluation and security analysis. Experimental results achieved are as follows: encryption time, decryption time, and accuracy are 0.07 ms, 0.056 ms, and 95.73%. Thus, the encryption and optimized classifier based on NTRU-AES and AG-GAN improves the security of IoT data.

Keywords- AG-GAN, Cyber security, embedding approach, IoT data, K means cluster-ing, NTRU-AES, two-factor authentication

1. Introduction

Prevalence of IoT and modern society's dependence on digitization have contributed to a significant increase in threats and attacks in recent years [1]. Attacks using malware, ransomware, zero-day vulnerabilities, cryptography, unauthorized access, denial of service (DoS), phishing, social engineering, and other techniques, as well as attacks on Internet of Things devices, are more prevalent these days [2]. The numerous technological demands of today may render traditional, well-known security solutions

ineffective, including firewalls, user authentication, encryption, and antivirus software [3] [4]. The main problem in these systems is that they are usually operated by a small group of security analysts, as a result, data management is done on as-needed basis, making it impossible for the system to function intelligently in accordance with the needs [5] [6]. Artificial intelligence (AI) techniques are applied in the process of creating a data-driven intrusion detection (ID) model and resolving ID challenges. Several approaches to machine learning (ML) that rely on classification techniques, such as Artificial

Neural Network (ANN), Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), and Bayesian Network (BN)[7, 8]. However, there are certain challenges with utilizing ML to forecast cyberattacks, including imbalanced datasets, poorer detection rates, slower response times, and a higher rate of false alarms. Furthermore, the transfer of data between devices in an IoT network requires secure data transmission. The number of keys used in the cryptography process determines the data level of security. Existing cryptographic approaches used to provide security include blowfish, DES and ECC [9, 10]. The following are the primary objectives of the suggested approach:

- An IoT framework based on AG-GAN and improved NTRU-AES cryptography is developed to provide an improved security for authorized user data in IoT sector.
- Raw IoT data is validated with 2FA, then preprocessed with KMC and selected using an embedded approach to reduce noise and improve key characteristics.
- Selected relevant features are fed into an AG-based GAN classifier to effectively predict a cyber-attack or normal.
- NTRU-AES cryptography-based encryption has been designed to secure the normal authenticated data in IoT.

The following sections comprise this work. In Section 2, a review of multiple articles that discuss modern methods for improving network storage system security is provided. In Section 3, the methodology explanation's mechanism is briefly described. In Section 4, the suggested framework for results and performance matrices is described. Section 5 provides a description of the final work.

2. Related Work

Numerous studies on the subject of IoT-based cyberattack detection and cryptography utilizing recent techniques are examined below:

Dey et al. [11] demonstrated an intelligent cyber security threat detection system that optimizes features using an ensemble feature selection method based on metaheuristics and uses ensemble learning-based classifiers to identify cyber threats. AlZubi et al. [12] created machine learning techniques and a cyber-physical system to identify cyber-attacks in the healthcare sector. To securely transmit health information, the Attack Detection Framework with cognitive machine learning assist has been presented with an attack prediction ratio of 96.5%, accuracy

ratio of 98.2%. Avci1 and Koca [13] presented a feature-selection and machine learning-based approach for detecting network intrusions. The study examined the effectiveness of four machine learning algorithms in the framework of intrusion detection: Random Forest (RF), K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree (DT).

Mousavi et al. [14] devised a hybrid cryptographic technique to protect private information in Internet of Things (IoT)-based smart irrigation systems. It combines the Rivest cipher (RC4), Elliptic-Curve Cryptography (ECC), and Secure Hash technique (SHA-256). This work uses the ECC approach to encrypt the RC4 key, and then generates cryptic data from the resulting SHA-256 hash. To increase data integrity, RC4 cipher text is encoded using the SHA-256 technique. Chowdhury et al. [15] created DeCrypt, an enhanced version of 3DES, an encryption technique. Feistel cipher techniques with an infinite block length have an alternative in DeCrypt. The purpose of DeCrypt is to secure encryption from Sweet-32 and Fulfill in the Middle attacks. Memory of about 32 GB is needed to unlock 64-bit block size algorithms like DES, 2-DES, DES-X, 3-DES, Twofish, and Blowfish.

Several cyber threat prediction techniques have been developed to achieve high security in network storage systems, according to the aforementioned article. Despite the fact that these current approaches have certain shortcomings, such as the inability to categorize all cyber-attack cases [11, 13], the need for improvement [12,15], the high cost [14], and the increased difficulty of designing the task [15]. A novel approach and sophisticated techniques were developed to address these kinds of problems. The working process of the proposed AG-GAN based NTRU-AES model is discussed in the upcoming section.

3. Methodology

Cybersecurity is a process that aims to prevent unauthorized users from accessing servers, network applications, data, etc. Security and privacy concerns are getting worse as network-related applications expand. In order to create an efficient intrusion detection system (IDS), numerous studies are carried out. The traditional methods, however, are unable to identify the unknown network threats. Because of

this, an enhanced cyber-security framework known as Adaptive Gray wolf optimization-based GAN (AG-GAN) was created in this paper to accurately detect cyber-attacks. Figure 1 depicts the suggested architecture.

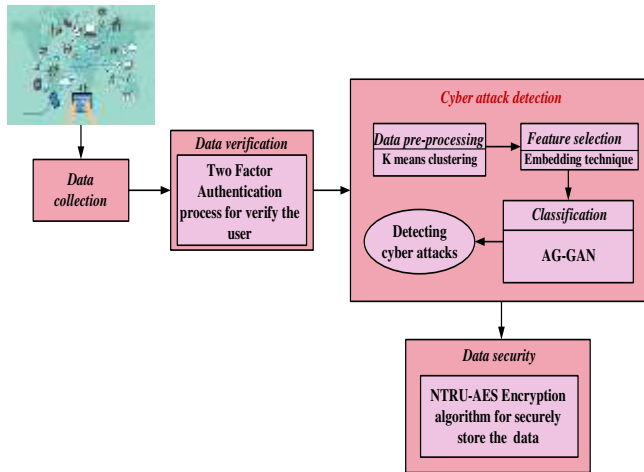


Fig. 1.Diagram for the Proposed Methodology.

Figure 1 shows IoT datasets that were obtained from standard sources and subsequently validated using the 2FD technique. Three steps comprise the validated data: data preprocessing, feature selection, and attack classification. Initially, KMC was used as a preprocessing step to remove errors from the raw input dataset. Subsequently the embedded approach is used to select the most significant attack features. Lastly, an AG-based GAN algorithm is fed the chosen features in order to distinguish between normal and attack. Hyper parameters in GAN classifiers including batch size and learning rates can be optimally tuned using AG thus improving accuracy and lowering error rates. Then, authorized normal user data are encrypted using advanced NTRU-AES based cryptography to provide robust protection. AES stands for actual data encryption, while NTRU is used to generate the secret key for better security. The following are the mathematical functions of the suggested model:

3.1 Data Verification

Data verification is necessary to evaluate the dependability, quality, and accuracy of the information gathered and used by IoT devices. Authentication process in the suggested paradigm consists of the following two stages such as login and authentication. Login and Authentication: The protocol comprises two layers known as two-factor authentication, which verify the identity of the

person submitting the request based on the username/password and OTP. Following a successful authentication process, the user gains access to the cloud.

3.2 Preprocessing- KMC model

KMC performed significant effort to remove redundant and duplicate data from the dataset, reduce noise, fill in missing values, and resolve irregularities. By grouping similar data into clusters according to the initial centroids of those clusters, KMC is an effective clustering method. Calculating cluster centroids involves using Euclidean distances. The first procedures include random partitions, data redistribution to clusters with the closest centers, and calculations of the current cluster centers. Finally, reassignments that cannot be continued are terminated. Thus, local intra-cluster variances, or sums of squares expressing differences between the features of the data and the cluster are minimized. Pre-processed datasets can reduce training phase execution times, memory usage, and resource consumption.

3.3 Embedded feature selection

Embedded techniques integrate the advantages of wrapper and filter techniques. Algorithms with their own internal feature selection techniques implement it. There are two fundamental steps in it:

- Gradient Boost Leveraging trees as a filter, each attribute is ranked according to its significance. The objective is to decrease the computational cost during the warping step and minimize the impact of noise. The number of times a feature is selected for splitting determines its relative relevance, which is then weighted by the squared improvement to the tree following each split, as shown in Equation (1):

$$\hat{I}_j^2(T) = \sum_{t=1}^{J-1} \hat{I}_t^2(v_t = j) \quad (1)$$

Where variables v_t and $\hat{I}_t^2$ corresponds to the improvement criteria in squared error in space of the regression tree R , respectively, and the sum is over the non-terminal nodes t of the J terminal node trees T

- Following that, the wrapping approach is employed to provide the model-based feature selection with the important features score. For instance, the wrap approach reduces the computational requirements when dealing with large amounts of data.

3.4 Classification based on AG-GAN

In order to generate additional data examples related to minority classes, the GAN model is utilized. In each stream of measurements M , there is a training dataset $X \subseteq R^{M \times T}$ and in each stream with N measurements and T streams, there is a testing dataset $X^{test} \subseteq R^{N \times T}$. In order to produce additional data that matches the minority class examples, the GAN model is utilized. To effectively learn from X , the s_w sliding window's size is used. Multivariate time series with a step size of s_s are used to create the multivariate subsequence $X = \{x_i, i = 1, 2, \dots, m\} \subseteq R^{s_w \times t}$. The number of subsequent is indicated as $m = \frac{M-s_w}{s_s}$. The notation $Z = \{z_i, i = 1, 2, 3 \dots, m\}$ represents the random space of the multivariate sub-sequences set. As shown in Eq (2), the discriminator and generator in the two-player minimax game are trained using the GAN model with Z and X .

$$\min_{G, D} \max_{D} V(D, G) = \mathbb{E}_{x \sim p_{data}(X)} [\log D(x)] + \mathbb{E}_{z \sim p_Z(z)} [\log (1 - D(G(z)))] \quad (2)$$

Wherein $G(z)$ the designed false data is provided by the noise vector, $D(x)$ is the probability that an actual model formed by the discriminating neural networks is real, and $D(G(z))$ is the predicted probability of a fake instance being authentic. It is stated that the generator learns to create actual samples after it reaches equilibrium. A GAN training tool called the Adaptive Gray Wolf Optimization Algorithm (AG) [16] optimally tunes the learning rate and batch size to improve detection accuracy. Grey wolf optimization (GWO) approach is one of the best population-based methods [16]. GWO promotes information sharing within the wolf population by modeling its leadership structure and hunting mechanism behavior after real wolves in the wild.

3.5 Hybrid NTRU-AES Cryptography

In order to provide a reliable and secure solution for IoT, this work presents a hybrid cryptographic architecture that combines the characteristics of AES for data encryption with NTRU for key exchange. Each algorithm is explained in detail in the section that follows.

NTRUEncrypt algorithm's superior performance in comparison to other asymmetric algorithms is a significant advantage [17]. The multiplication of polynomials with a relatively low degree is the primary operation in encryption, which allows the algorithm to operate quickly. Furthermore, the NTRUEncrypt cryptosystem may be used on mobile devices and doesn't require a lot of RAM. Any polynomial A utilized in the cryptosystem can be expressed as follows: The cryptographic system NTRUEncrypt performs operations on the ring $Z[X]/(X^N - 1)$ of polynomials, the degree of which does not exceed $N - 1$. Afterward data is encrypted with the created key by using Advanced Encrypted Standard (AES). This algorithm has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. And also, an important symmetric encryption technique for maintaining security in many areas, including the Internet of Things, is Advanced Encryption Standard (AES) [18]. As the data being processed and shared in the IoT is sensitive, security is essential. The achievement of this security is greatly aided by AES. They're subdivided into four phases. Alter rows, add a round key, mix columns transformation, and swap bytes.

4. Results and Discussion

Enhance IoT data security by protecting data from unauthorized users with an AG-GAN-based optimized deep learning system. The performance of the suggested model is examined using Python software, an Intel Core i7 CPU, and NVIDIA GeForce RTX 3070 GPU, 64GB RAM configuration. Table 1 presents a set of parameters together with their corresponding ranges for the simulation modeling of the suggested and current approaches.

4.1 Dataset description

A network intrusion dataset is UNSW-NB15. The collection includes raw packets from networks. The training set contains 175,341 records, while the testing set has 82,332 records that can be divided into attack and normal categories. In the next section, the effectiveness of the proposed work is illustrated by analysing and contrasting the performance of the NTRU-AES technique with a few other security algorithms that are currently in use. Performance is compared using execution time, information loss, decryption time, and encryption time. RSA 512-AES 128, RSA-ECIES and SHA 512-AES are the current models used for validation.

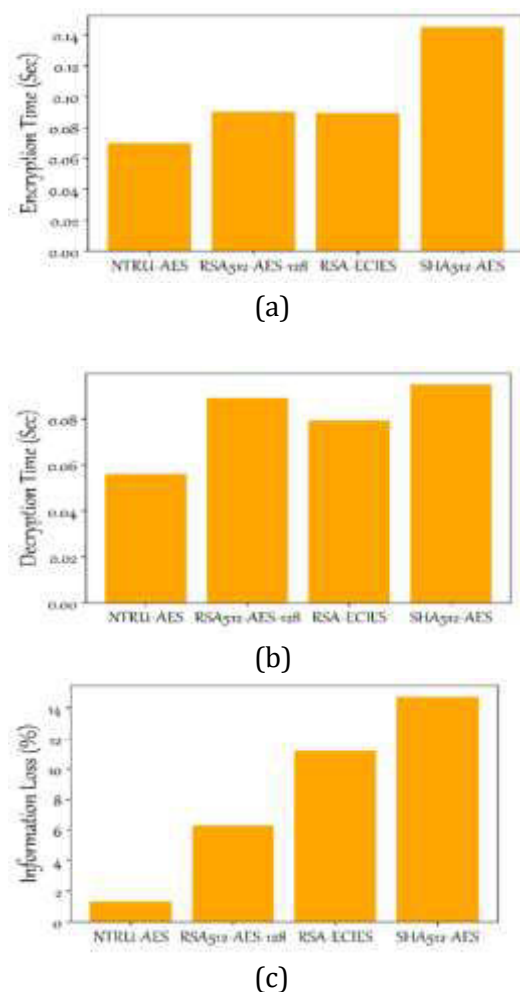


Fig. 2. Evaluation of (a) Encryption time (b) Decryption time and (c) Information Loss.

Figure 2 (a) provides a comparison of encryption time. Graph shows the time for encryption reached for the proposed NTRU-AES algorithm is 0.07 ms and it is lesser when compared to another existing algorithm such as RSA 512-AES 128, RSA-ECIES and SHA 512-AES are 0.09ms, 0.0893 ms, and 0.145 ms

respectively. Figure 2 (b) illustrates decryption time comparison data. The graph shows time of decryption reached for the proposed NTRU-AES is 0.056 ms lesser than every other algorithm 0.079ms for RSA 512-AES 128, 0.1182ms for RSA-ECIES and 0.095ms for SHA 512-AES. Then the information loss is observed and provided in Figure 2 (c). The proposed model NTRU-AES information loss is 1.34% and RSA 512-AES 128 is 4.6%, RSA-ECIES is defined in 11.2%, and SHA 512-AES technique is 14.7%. The suggested model's NTRU-AES encryption time, decryption time, and information loss are less than those of the existing approaches, demonstrating its efficiency.

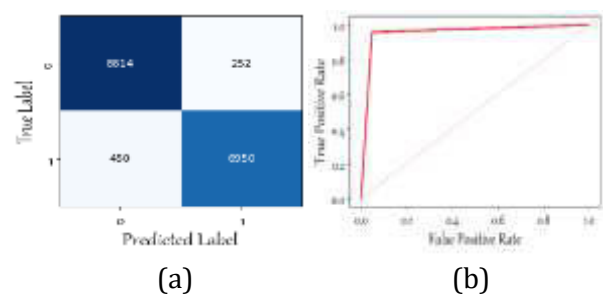


Fig. 3. Analysis of (a) confusion matrix (b) ROC.

The suggested model's confusion metric is depicted in Figure 3(a). A method used to evaluate the accuracy of a classification system is using confusion matrix analysis. Estimating the error matrix is done to identify the regions in which the classification technique fails. Together with the approach used to categorize the classes based on the IoT dataset, it gives a case study of an incorrect class classification. It contains two different classes normal and attack. The predicted values are 8814 and 6950 in that order. The probability curve that plots the TP rate versus the FP rate at various threshold values is known as the ROC curve, and Figure 3(b) shows it. This curve is used as an evaluation tool for classification problems and threat prediction. Demonstrate that the proposed model performs better in terms of cyber-attack prediction classification. It demonstrates that the recommended model performs better in terms of predictions.

Furthermore, the null error rate, false negative rate (FNR), negative predictive value (NPV), false discovery rate (FDR), accuracy, specificity, precision, recall, and selectivity are all measured using the positive and negative rates.

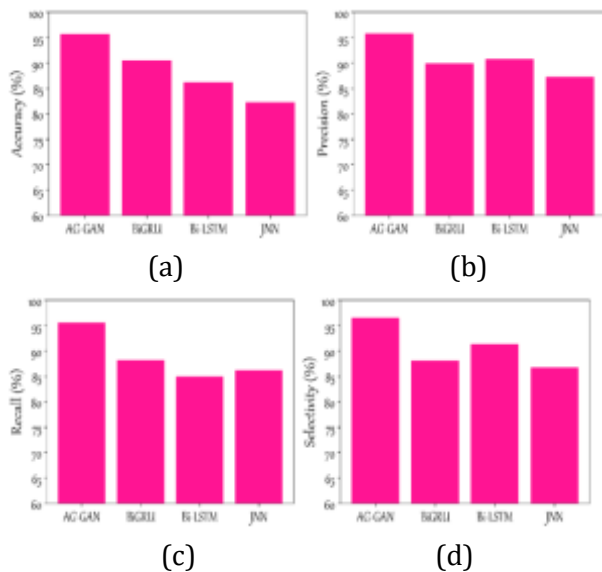


Fig. 4. Examination of proposed and existing model (a) accuracy (b) precision (c) recall (d) Selectivity

Figure 4(a) compares the accuracy metrics of the suggested and current approaches. 95.73% is the accuracy achieved by the proposed AG-GAN. It is high when compared to other existing algorithms called BiGRU, BiLSTM and JNN which has accuracy of 90.56%, 86.2% and 82.3%. Figure 4(b) compares the precision of the suggested and current approaches. The precision achieved by the AG-GAN and the existing methods is 95.82%, 89.92%, 90.78% and 87.3% respectively. Figure 4(c) displays the recall measures for the proposed and existing methods. AG-GAN classifier is used in the proposed approach, which has a recall value of 95.56% and 88.2 %, 85 %, 78.81 % and 86.2 % of recall value which employs classifier such as BiGRU, BiLSTM and JNN. Selectivity graphical representation is shown in the figure 4(d) which has the following proposed and the existing techniques named AG-GAN which has the value of 96.54%, the BiGRU has the range of 88.12%, the BiLSTM has the range of 91.34% and the JNN has the value of 86.75%. The comparison demonstrates that the proposed method outperforms other existing methodologies.

5. Conclusion

Threats from cyberspace are becoming more prevalent. These attacks are too strong for the conventional security measures to handle. Deep learning techniques are being used to solve the shortcomings of traditional security systems. This paper introduces an AG based GAN classifier that

uses the NTRU-AES encryption technique to effectively detect cyber-attacks in the IoT. The results show that the suggested NTRU-AES and AG-GAN algorithms perform better than the more commonly employed current techniques, with encryption and decryption times of 0.07 ms and 0.056 ms, respectively. In addition, introduced scheme performs better than the standard schemes with 95.73% accuracy, 95.82% precision, 95.56% recall, and 96.54% specificity. The proposed architecture improves security and is more effective than the present methods. Nevertheless, present datasets are deficient in complexity and diversity, and often have missing values. Learning models that are distinctive and adapted for security-related reasons are required. Subsequent investigations will concentrate on examining increasingly sophisticated learning methodologies for identifying cyber hazards and enhancing network safety.

References

- [1] Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K., Hong, W.C.: Internet of things: Evolution, concerns and security challenges. *Sensors* 21(5), 1809 (2021).
- [2] Koupaei, A.N.A., Nazarov, A.N.: Security analysis threats attacks mitigations and its impact on the internet of things (IoT). *Synchroinfo Journal* 6(4), 36-41 (2020).
- [3] Djenna, A., Harous, S., Saidouni, D.E.: Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences* 11(10), 4580(2021).
- [4] Aldahmani, A., Ouni, B., Lestable, T., Debbah, M.: Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology* 4, 281-292 (2023).
- [5] Diène, B., Rodrigues, J.J., Diallo, O., Ndoye, E.H.M., Korotaev, V.V.: Data management techniques for Internet of Things. *Mechanical Systems and Signal Processing* 138, 106564 (2020).
- [6] Zhu, X.: Self-organized network management and computing of intelligent solutions to information security. *Journal of Organizational and End User Computing (JOEUC)* 33(6), 1-16 (2021).
- [7] Dina, A.S., Manivannan, D.: Intrusion detection based on machine learning techniques in computer networks. *Internet of Things* 16, 100462 (2021).
- [8] Mohamed Amer, G., Abd El Hay, E.H., Abdel-Baset, I.Y., Abd El Azim Mohamed, M.: Development Machine Learning Techniques to Enhance Cyber Security Algorithms. *MEJ-Mansoura Engineering Journal* 46(4), 36-46 (2021).
- [9] Adeniyi, A.E., Misra, S., Daniel, E., Bokolo Jr, A.: Computational complexity of modified blowfish cryptographic algorithm on video data. *Algorithms* 15(10), 373 (2022).
- [10] Mehta, K., Kumar, Y., Sidhu, H.S.: Cryptographic algorithms for secure internet of things. *Int. J. Control Autom* 13(4), 1010-1018(2020).

- [11] Dey, A.K., Gupta, G.P., Sahu, S.P.: A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. *Decision Analytics Journal* 7, 100206 (2023).
- [12] AlZubi, A.A., Al-Maitah, M., Alarifi, A.: Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing* 25(18), 12319-12332 (2021).
- [13] Avci, I., Koca, M.: Cybersecurity Attack Detection Model Using Machine Learning Techniques. *Acta Polytechnica Hungarica* 20(7), 29-44 (2023).
- [14] Mousavi, S.K., Ghaffari, A., Besharat, S., Afshari, H.: Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing* 12(2), 2033-2051 (2021).
- [15] Chowdhury, D., Dey, A., Garai, R., Adhikary, S., Dwivedi, A.D., Ghosh, U., Alnumay, W.S.: DeCrypt: a 3DES inspired optimised cryptographic algorithm. *Journal of Ambient Intelligence and Humanized Computing* 14(5), 4745-4755 (2023).
- [16] Jabbar, A.M., Ku-Mahamud, K.R.: Adaptive Grey Wolf Optimization Algorithm with Neighborhood Search Operations: An Application for Traveling Salesman Problem. *International Journal of Intelligent Engineering & Systems* 14(6), (2021).
- [17] Cherckesova, L., Safaryan, O., Razumov, P., Kravchenko, V., Morozov, S., Popov, A.: Post-Quantum Cryptosystem NTRUEncrypt and Its Advantage over Pre-Quantum Cryptosystem RSA. In *E3S Web of Conferences* (Vol. 224, p. 01037). EDP Sciences. (2020).
- [18] Arman, S., Rehnuma, T., Rahman, M.: Design and implementation of a modified AES cryptography with fast key generation technique. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 191-195). IEEE. (2020).