Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-B, pp. 1399–1411
DOI : 10.47974/JDMSC-2286

AI-driven cybersecurity-based hybrid approach using blockchain for smart grids

Noora Kadhim Al-Bermani *
Department of Ceramic and Building Materials Engineering
College of Materials Engineering
University of Babylon
Babylon
Iraq

Ali Kadhim Bermani †
Department of Network
College of Information Technology
University of Babylon
Babylon
Iraq

and

Department of Computer Techniques Engineering
College of Engineering and Technologies
Al-Mustaqbal University
Babylon
Iraq

Abeer Raad §
Department of Medical Instruments Techniques
Technical Institute of Al-Mussaib
Al-Furat Al-Awsat Technical University
Babylon
Iraq

* *E-mail:* `mat.noorakadhim@uobabylon.edu.iq (Corresponding Author)`
† *E-mail:* `ali.k.bermani@uomus.edu.iq`
§ *E-mail:* `abeer.hassan.ims@atu.edu.iq`

Mehdi Ebady Manaa ‡
Department of Network
College of Information Technology
University of Babylon
Babylon
Iraq

and

Department of Intelligent Medical System
College of Sciences
Al-Mustaqbal University
Babylon
Iraq

Abstract

Power systems have become more efficient, reliable, and sustainable as smart grids are increasingly integrated into them. Developing innovative security solutions is often required to counter evolving cyber threats because traditional security mechanisms lack real-time protection. The purpose of this paper is to propose a blockchain-based hybrid optimization approach for enhancing smart grid security and resilience. To improve decision-making, resource allocation, and attack mitigation, the framework incorporates artificial intelligence (AI) to detect anomalies in real-time, blockchain technology to store unrestricted data, and a hybrid optimization algorithm to make decisions in real-time. Adaptive Vulture Optimization Algorithm (AVOA) and Convolutional Neural Networks (CNN) combine to reduce computational overhead and maintain detection accuracy effectively. According to the proposed approach, which is compared to existing models, including ML-ID, HHT, and THD, it achieves superior performance, with a detection rate of 99.17%, a reduction in computation time, and enhanced scalability. These results demonstrate that AI-Blockchain hybrid frameworks are effective in protecting smart grids against emerging cyber threats, making them a reliable and scalable security solution.

Subject Classification: *93E10, 94A13.*

Keywords: *Smart grid security, AI-driven cybersecurity, Blockchain-based security, Hybrid optimization algorithm, Anomaly detection in IoT.*

1. Introduction

Through smart grid adoption, modern power systems have become more efficient, reliable, and sustainable. It should be noted, however, that IoT devices, automation, and advanced communication networks have also presented significant cybersecurity challenges for smart grids. Power grids are at risk of

‡ *E-mail:* **mahdi.ebadi@uomus.edu.iq**

being compromised by cyber threats like data breaches, malware attacks, and unauthorised access [1]. Cybersecurity mechanisms are often unable to provide real-time protection due to cyber threats that are constantly evolving. A blockchain-based hybrid optimisation approach based on AI for smart grids is proposed to address these challenges. An integrated framework that integrates artificial intelligence (AI), blockchain technology, and hybrid optimisation algorithms enhances data integrity, security, and system resilience[2]. AI-based threat detection makes it possible to monitor and detect anomalies in real time, while blockchain ensures tamper-proof data storage and decentralised data security. As a result of the hybrid optimisation approach, smart grid environments are able to make better decisions, allocate resources, and mitigate attack strategies significantly more effectively.

There has been a significant transformation in the energy market due to a sharp increase in electricity demand and the need to reduce greenhouse gas emissions. In the future, fossil fuel-dependent power systems will increasingly integrate renewable energy sources (RES) into their power generation systems, which will pose a challenge to grid stability. Achieving these goals requires the integration of technologies, such as smart grids, distributed generation, storage, and electric vehicles (EVs). Produced and consumed energy usage can be monitored, automated, and communicated in real-time with the help of SGs, improving energy management and reliability. The decentralisation of power and reduction of transmission losses are two advantages of distributed generation [3]. Achieving system flexibility by advancing EV infrastructure and energy storage technologies is essential to managing renewable energy sources' intermittent nature [4], [5]. However, the transition would not be complete without cybersecurity. A growing number of cyberattacks threaten energy systems as a result of digitisation and interconnection, posing a threat to disruptions and damage to the infrastructure [6].

2. Related Work

Due to the rapid expansion of smart grid technologies, energy efficiency, reliability, and renewable energy integration have improved dramatically. Smart grids, however, have also become vulnerable to new vulnerabilities as a result of digital transformation, especially in the realm of cybersecurity. Machine learning has become increasingly important in safeguarding against sophisticated cyber threats as smart grid infrastructure becomes more complex. Recent studies have shown that machine learning algorithms can detect, prevent, and mitigate cyber-attacks in smart grids by using data analytics and real-time monitoring. As part of this section, existing literature on the role machine learning plays in securing smart grids is systematically reviewed, identifying current research trends, challenges, and future directions. A comprehensive understanding of machine learning's potential impact on cybersecurity in smart grid systems is gained through the integration of insights from prior studies. AI in the SG system can be used to address the above cybersecurity issues [7]. Artificial intelligence is based on a variety of mechanisms, including machine

learning (ML) and reinforcement learning (RL) [8]. With AI and ML, SG improves security processes and assists security analysts in identifying, prioritising, responding, and remediating new threats faster. An intrusion detection system has been proposed by Oliveira et al. in this regard. To detect intrusions, the author evaluated different machine learning models, including random forests (RF), multilayer perceptrons (MLP), and long-short-term memories (LSTM) [9]. Kalman filters are used to detect false data injection attacks [10]. XGBoost (extreme gradient boosting) is then used to develop an advanced approach for attack classification. The next step is to apply a reinforcement learning approach to detect online cyberattacks [11].

3. Proposed Methodology

This paper uses two types of datasets.

Network Traffic Data: Simulations of normal and anomalous network traffic within cognitive cities are carried out using datasets like [12]. Cyber threat detection models rely on these data to train and test.

Blockchain Transaction Data: A cognitive city uses blockchain transactions from the [13] as its basis for simulating blockchain transactions. The data helps test the ability of the blockchain to maintain data integrity and transparency and support secure communications and transactions.

3.1. Feature extraction and feature selection

This technique is described in detail in Extraction of URL features using the Ngram method [14-19]. Extractions of URL information are combined with data set features like UCI. After selecting the basic features, the next step is feature selection. Every feature vector in the proposed approach has either one or zero elements. When a feature number equals zero, it is not selected; otherwise, if it equals one, it is selected. A matrix of equations is proposed to represent each feature vector (8). Vultures or feature vectors are represented by n in this matrix. Because the UCI data set contains 30 features, Equation (1) describes the matrix. Feature vectors or vultures are the initial populations in these equations.

$$P = \begin{bmatrix} P_{1,1} & \cdots & \cdots & P_{1,j} & P_{1,d-1} & P_{1,d} \\ P_{2,1} & \cdots & \cdots & P_{2,j} & P_{2,d-1} & P_2, d \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_{n-1,1} & \cdots & \cdots & \cdots & P_{n-1,d-1} & P_{n-1,d} \\ P_{n,1} & \cdots & \cdots & P_{n,j} & P_{n,d-1} & P_{n,d} \end{bmatrix} \quad (1)$$

$$P = \begin{bmatrix} P_{1,1} & \cdots & \cdots & P_{1,j} & P_{1,29} & P_{1,30} \\ P_{2,1} & \cdots & \cdots & P_{2,j} & P_{2,29} & P_2, 30 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_{n-1,1} & \cdots & \cdots & \cdots & P_{n-1,29} & P_{n-1,30} \\ P_{n,1} & \cdots & \cdots & P_{n,j} & P_{n,29} & P_{n,30} \end{bmatrix} \quad (2)$$

In the proposed method, feature vectors are evaluated using an objective function, which can be done using Equation (3):

$$Cost(P_i) = \alpha.\frac{1}{m}.\sum_{i=1}^{m}(\bar{Y}_i - Y_i)^2 + \beta.\frac{||P_i||}{||d||} \quad (3)$$

It is determined that $\frac{1}{m}.\sum_{i=1}^{m}(\bar{Y}_i - Y_i)^2$ is an index of phishing attack detection errors and $\frac{||P_i||}{||d||}$ is a measure of how much the dimensions of the collection have been reduced.

The coefficients of alpha and beta are usually combined into one, with alpha being assigned randomly and beta being determined by alpha. Equation (4) led to the formulation of an objective function:

$$Cost(P_i) = \alpha.\frac{1}{m}.\sum_{i=1}^{m}(\bar{Y}_i - Y_i)^2 + (1-\alpha).\frac{||P_i||}{||d||} \quad (4)$$

As in the Equation and objective function, $\bar{Y}_i$ and Y_i represents the value of the class and the value predicted for the page type. There is a code 1 for phishing and a code 0 for legal pages. A data set has a number of columns, or primary features that make up the feature vector $||P_i||$.

A proposed method for evaluating phishing attacks requires m samples. In general, feature vectors that minimise this objective function are considered optimal. Below are some defaults of the AVOA algorithm:

- Each stage of a vulture's life is devoted to finding the best prey or solution.
- One time the algorithm is run, two groups of vultures are selected. As far as vultures are concerned, there are two kinds: the most worthy and the second most worthy, and the weakest vultures are in the other category.
- Each group finds food differently, and they are also capable of finding food in different ways.
- According to the AVOA algorithm, vultures' search and flight energy are reduced by hunger. A local search for food involves them moving toward the prey in order to compete with two vultures near the food.
- In the absence of food, vultures behave aggressively and stay away from prey. Almost the entire problem space is covered and explored here, and an exploratory global search is conducted.

For simplicity, we assume a 50% chance that a vulture-like X_i would move toward one of the two optimal vultures [15]:

$$P_i = \frac{F_i}{\sum_{i=1}^{n} F_i} \quad (5)$$

A vulture's fitness F_i is calculated by comparing it with a vulture-like p_i, and a vulture's probability of choosing an optimal vulture for the population is calculated by P_i. Vultures are optimised as they are less hungry, less aggressive, and fly more because they have more access to food, according to the vulture algorithm. Hunger makes vultures more aggressive and willing to fight for food

and makes them more determined to succeed. A vulture moves according to one of two suitable solutions at random. As vultures increase their hunger and decrease their satiety, equations (6) and (7) are applied to model their behaviour [15]:

$$t = h \times \left(\sin^{w}\left(\frac{\pi}{2} \times \frac{iter}{MaxIter}\right) + \cos\left(\frac{\pi}{2} \times \frac{iter}{MaxIter}\right) - 1\right) \quad (6)$$

$$F = (2 \times rand + 1) \times z\left(1 - \frac{iter}{MaxIter}\right) + t \quad (7)$$

The vulture algorithm aims to have solutions searched locally over time rather than globally. In the Vulture algorithm, this issue requires vultures to fly toward two optimal vultures in order to fight. A measure of vulture satiety is based on the F function. According to the algorithm's repetitions, the population will attempt to find an optimal local search solution, which will result in a decreasing routine during the last iteration. These equations have two variables: iter and MaxIter. Iter represents the number of iterations in the AVOA algorithm. The value of t in these equations varies from 0.5 to 1, depending on the situation, according to a random step generation function for flight. With increasing t, F deteriorates, and iterations decrease. As a result of two iterations of the AVOA algorithm, BestVulture1 and BestVulture2, two optimal solutions are produced each time. With the global search mode, a vulture roams anywhere in the problem space, since it has expressions $|F| > 1$. For vultures that have random numbers smaller than p_i Equation (8) will be used for vultures whose random numbers are greater than p_iEquation (16) will be used [15]:

$$P(i+1) = R(i) - D(i) \times F \quad (8)$$

$$D(i) = |X \times R(i) - P(i)| \quad (9)$$

A vulture's current location is $P(i)$, a vulture's new location is $P(i+1)$, and RI represents a random location, including BestVulture1 and BestVulture2, and i is the algorithm's repetition counter [15]:

$$P(i+1) = R(i) - F + rand(ub - lb).rand + lb) \quad (10)$$

In terms of feature space or optimisation problems, upper and lower bounds are referred to as "ub" and "lb", respectively. It is possible that a hungry vulture will $|F| \leq 1$, which leads to two possible scenarios. $|F| \geq 0.5$ has shown some local search results in this instance.

When $|F| \geq 0.5$, there are two states: if p2 is less than p2, Equation (11) is applied, and if it is greater than Equation (12), Equation (12) must be applied [15]:

$$P(i+1) = D(i) \times (F + rand) - d(t) \quad (11)$$

$$d(t) = R(i) - P(i) \quad (12)$$

A vulture's Distance from Best Vulture1 or BestVulture2 has been calculated according to Equation (9). A hungry vulture attempts to fly towards the second worthy vulture's side.

When Equations (13), (14), and (15) show that $|F| \geq 0.5$ and the casual figure have increased significance over p2, the solutions are updated. [15]:

$$S_1 = R(i) \times \left(\frac{rand \times P(i)}{2\pi}\right) \times Cos\big(P(i)\big) \quad (13)$$

$$S_2 = R(i) \times \left(\frac{rand \times P(i)}{2\pi}\right) \times Sin\big(P(i)\big) \quad (13)$$

$$P(i+1) = R(i) - \frac{S_1 + S_2}{2} \quad (14)$$

The solutions are updated when $|F| < 0.5$ and a casual figure are less than p3. [15]:

$$A_1 = BestVulture_1(i) - \left(\frac{BestVulture_1 \times P(i)}{BestVulture_1 \times P(i)^2}\right) \times F \quad (15)$$

$$A_2 = BestVulture_2(i) - \left(\frac{BestVulture_1 \times P(i)}{BestVulture_2 \times P(i)^2}\right) \times F \quad (16)$$

$$P(i+1) = \frac{(A_1 + A_2)}{2} \quad (17)$$

The solutions are updated when $|F| < 0.5$ and a casual figure are less than p3 [15]:

$$P(i+1) = R(i) - |d(t)| \times F \times Levy(d) \quad (18)$$

$Levy(d)$ Vultures' distances from each other are represented by $Levy(d)$ and DT, respectively.

Vultures attack prey aggressively or the optimal search radius F.

Framework implementation

Using blockchain and artificial intelligence technologies in the simulated cognitive city environment is a multi-step process for implementing the security framework. As part of the blockchain layer, data exchanges and transactions are recorded on a decentralised ledger. Designed to prevent unauthorised changes to the data, this ledger is tamper-proof. With blockchain's cryptographic techniques, data is secure and untampered with. Data is transformed into a fixed-length string of characters using SHA-256 hashing, which makes it virtually impossible to retrieve or alter the original data.

$$H(x) = SHA - 256(x) \quad (22)$$

Modifying the data will generate a completely new hash, allowing tampering attempts to be identified quickly. After that, machine learning models are trained with synthetic data generated from the simulation environment, which is then integrated with the AI layer. Using these models, network traffic is monitored, anomalies are detected, and potential security threats are pinpointed. A sophisticated machine learning algorithm is employed in the framework to detect anomalies in traffic by comparing observed data points to their mean value. An anomalous data point is immediately flagged as anomalous if it exceeds a predefined threshold based on the standard deviation, prompting further investigation and ensuring proactive security measures.

$$A(x) = \sum_{i=1}^{n} |x_i - \mu| > \sigma \quad (23)$$

Anywhere:

- A(x) is a score used to detect anomalies,

- There is a data point called x_i
- In this case, m is the mean,
- Specifies how much the standard deviation differs from the mean.

A layer of integration between the CNN and blockchain ensures the secure transmission of data between the two components and the generation of alerts when threats are detected. A smart contract is used to implement the integration layer, which automates security processes. Based on the Hyperledger platform, these smart contracts are written in Solidity. Data transmitted across the city's networks will be encrypted and protected against interception and tampering by the integration layer based on the blockchain's consensus mechanisms.

4. Results and Discussion

A performance comparison was conducted between the proposed approach and state-of-the-art methods such as ML-ID, HHT, and THD [16], [17], [18]. It outperforms existing approaches with a 99.17% detection rate. With CNNs and AVOA, AVOA's scalability problem is effectively addressed. Figure 1 illustrates how this framework improves accuracy and efficiency.

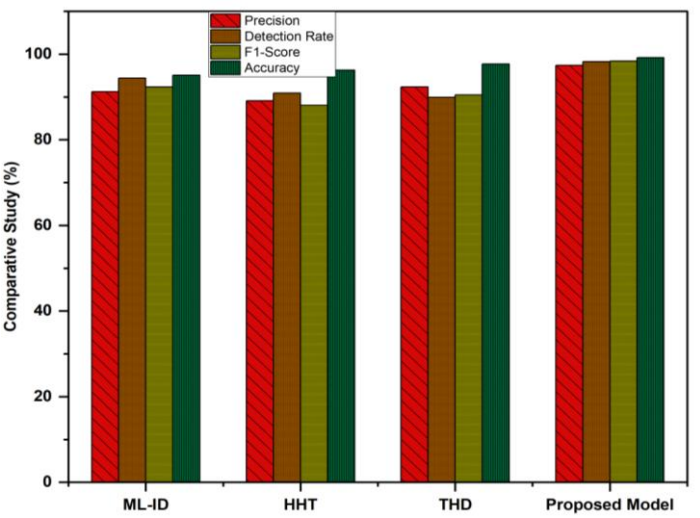

Figure 1
Comparative study of the proposed approach with existing work.

Furthermore, a comparison was conducted between the proposed algorithm and existing techniques to demonstrate how effective it is at reducing computation time. As a result, ML-ID takes 8.55 seconds, HHT takes 6.44 seconds, and THD takes 4.63 seconds, respectively. This technique, however, achieves significantly lower processing times of 2.32 s, proving its superiority over conventional methods as shown in Figure 2.

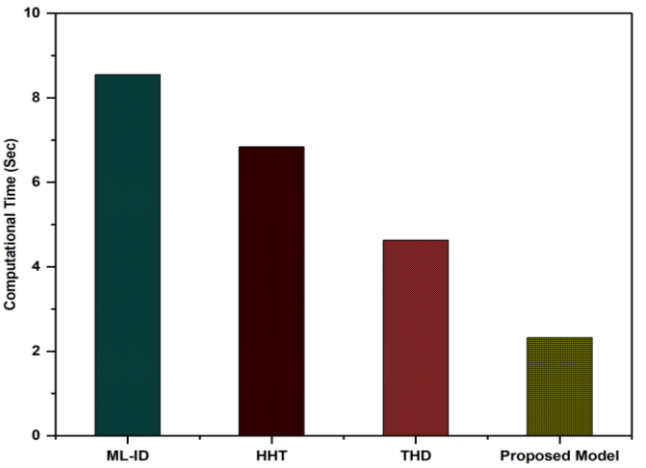

Figure 2

Comparative analysis with computational time (sec) versus existing work

A comparison of the proposed method's training time with existing approaches is presented in Figure 3. Training time is significantly reduced with the proposed approach, according to the results. Training times for ML-ID, HHT, and THD are respectively 115, 160, and 125 seconds, while the proposed method requires just 25 seconds, demonstrating its effectiveness.

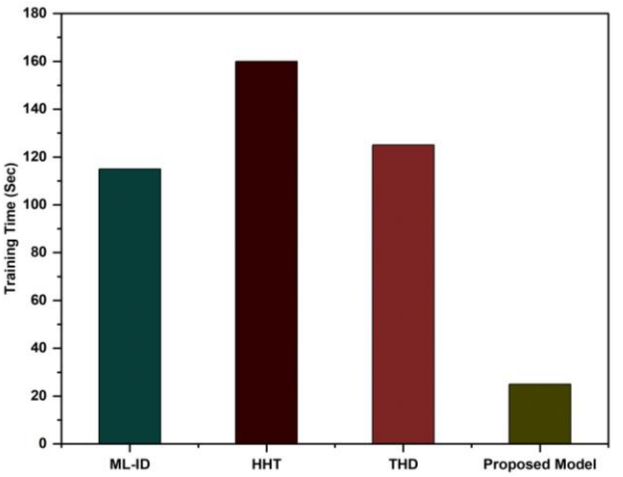

Figure 3

Comparative analysis in terms of training time.

The proposed model outperforms existing approaches in terms of performance. AVO was combined with well-established optimisation algorithms, such as the Squirrel Optimization Algorithm (SOA), Spider Monkey

Optimization Algorithm (SMOA), African Buffalo Optimization Algorithm (ABO), and Ant Lion Optimization Algorithm (ALO), to evaluate the effectiveness of integration. In Figure 4, the proposed model is shown to be more efficient when compared with the other.

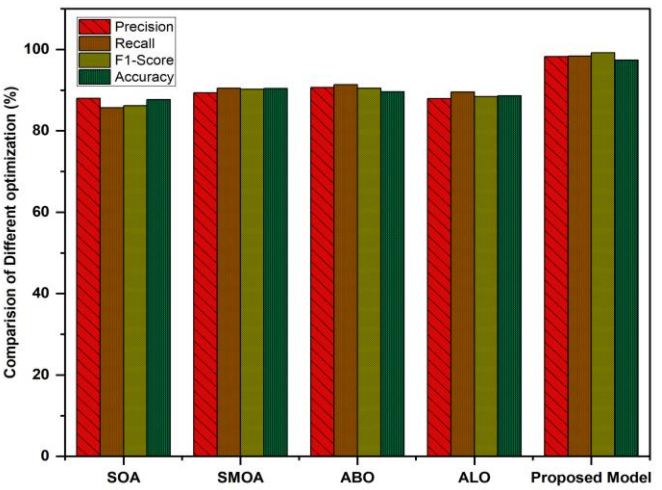

Figure 4
Comparison of the difference optimization versus the proposed model.

In comparison to the proposed work, other approaches require a much longer training period. ABO, ALO, SOA, and SMOA take 6.83, 5.85, 6.4, and 7.1 seconds, respectively. It is estimated that the proposed model will be trained in 2.32 seconds, which is less than any of the other options, as shown in Figure 5.

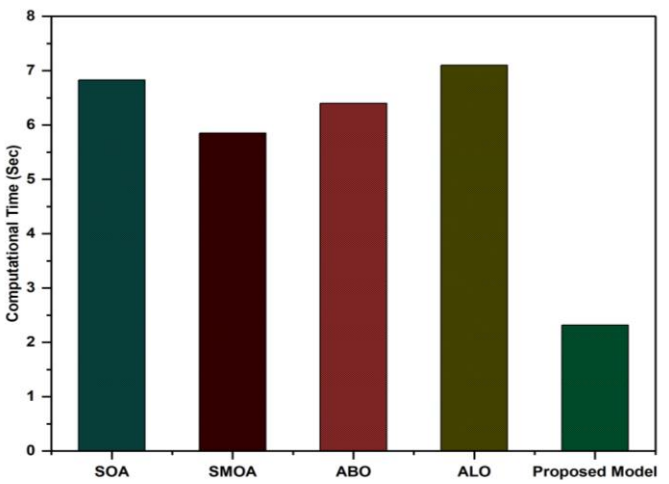

Figure 5
Computational time (sec) versus proposed approach.

5. Conclusion

As part of this study, we introduce a hybrid optimisation framework combining AI with blockchain in order to address cybersecurity challenges associated with smart grids. In this model, artificial intelligence is used to detect anomalies, blockchain is used for data integrity, and AVOA is used for optimising decision-making. Based on performance evaluations, it is confirmed that the proposed method is more accurate at detecting patterns (99.17%), takes significantly less time to compute (2.32s), and has a better training efficiency than conventional techniques. Furthermore, a comparison with existing optimisation algorithms (SOA, SMOA, ABO, and ALO) indicates that the proposed approach is more scalable and computationally efficient. Smart grids can be secured more robustly, scalable, and proactive with this model, which integrates artificial intelligence, blockchain technology, and advanced optimisation techniques. In the future, quantum-resistant cryptography and federated learning models may be investigated to improve the adaptability and resilience of cyber systems.

References

[1] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, "Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system," *Int. J. E-Health Med. Commun.* (IJEHMC), vol. 13, no. 4, pp. 1–15 (2022).

[2] P. Rani, M. S. Naruka, B. K. Rai, D. Kumar, S. Verma, and S. P. Yadav, "Federated learning-based misbehaviour detection for the 5G-enabled Internet of Vehicles," *IEEE Trans. Consum. Electron*. (2023).

[3] V. Vahidinasab, S. Nikkhah, A. Allahham, and D. Giaouris, "Boosting integration capacity of electric vehicles: A robust security constrained decision making," *Int. J. Electr. Power Energy Syst.*, vol. 133, p. 107229 (Dec. 2021), doi: 10.1016/j.ijepes.2021.107229.

[4] A. Allahham, D. Greenwood, C. Patsios, and P. Taylor, "Adaptive receding horizon control for battery energy storage management with age-and-operation-dependent efficiency and degradation," *Electr. Power Syst. Res.*, vol. 209, p. 107936 (Aug. 2022), doi: 10.1016/j.epsr.2022.107936.

[5] N. Hussain and P. Rani, "Comparative studied based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security," in *Distributed Artificial Intelligence*, CRC Press, pp. 217–236 (2020).

[6] S. Nikkhah, A. Alahyari, A. Allahham, and K. Alawasa, "Optimal integration of hybrid energy systems: A security-constrained network topology reconfiguration," *Energies*, vol. 16, no. 6, p. 2780 (Mar. 2023), doi: 10.3390/en16062780.

[7] A. Kumari and S. Tanwar, "A data analytics scheme for security-aware demand response management in smart grid system," in Proc. 2020 IEEE 7th UPCON, Prayagraj, India, pp. 1–6 (Nov. 2020), doi: 10.1109/UPCON50219.2020.9376458.

[8] A. Kumari and S. Tanwar, "A reinforcement-learning-based secure demand response scheme for smart grid system," *IEEE Internet Things J.,* vol. 9, no. 3, pp. 2180–2191 (Feb. 2022), doi: 10.1109/JIOT.2021.3090305.

[9] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Appl. Sci.,* vol. 11, no. 4, p. 1674 (Feb. 2021), doi: 10.3390/app11041674.

[10] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.,* vol. 1, no. 4, pp. 370–379 (Dec. 2014), doi: 10.1109/TCNS.2014.2357531.

[11] P. Rani, U. C. Garjola, and H. Abbas, "A predictive IoT and cloud framework for smart healthcare monitoring using integrated deep learning model," *NJF Intell. Eng. J.,* vol. 1, no. 1, pp. 53–65 (2024).

[12] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. 2015 MilCIS, Canberra, Australia: IEEE, pp. 1–6 (2015). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7348942/

[13] D. Lin, J. Wu, Q. Yuan, and Z. Zheng, "Modeling and understanding Ethereum transaction records via a complex network approach," *IEEE Trans. Circuits Syst. II: Express Briefs,* vol. 67, no. 11, pp. 2737–2741 (2020).

[14] A. S. Bozkir, F. C. Dalgic, and M. Aydos, "GramBeddings: A new neural network for URL-based identification of phishing web pages through n-gram embeddings," *Comput. Secur.*, vol. 124, p. 102964 (2023).

[15] B. Abdollahzadeh, F. S. Gharehchopogh, and S. Mirjalili, "African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems," *Comput. Ind. Eng.,* vol. 158, p. 107408 (2021).

[16] T. S. Ustun, S. S. Hussain, A. Ulutas, A. Onen, M. M. Roomi, and D. Mashima, "Machine learning-based intrusion detection for achieving cybersecurity in smart grids using IEC 61850 GOOSE messages," *Symmetry*, vol. 13, no. 5, p. 826 (2021).

[17] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert–Huang transform," *IEEE Access,* vol. 9, pp. 29429–29440 (2021).

[18] X. Zhu, W. Wang, S. Pang, C. An, X. Yang, and Y. Wu, "Blockchain-based optimal decision making of dispatchable units in smart grids considering the high uncertainty effects," Sustain. Cities Soc., vol. 76, p. 103418 (2022).

[19] A. S. Abdulbaqi, I. F. Muslim, A. A. A. Al-Ameer, and A. J. Obaid, "Healthcare surveillance based on cloud computing utilizing mobile devices," *J. Discrete Math. Sci. Cryptogr.,* pp. 1–8, [Online]. doi: 10.47974/JDMSC-1566.

Received February, 2025