Metaheuristic Optimization for Enhancing Cybersecurity Frameworks: An Overview of Methods and Impacts

Shahid Mahmood[1,*]
[1]School of Finance and Economics, Jiangsu University, Zhenjiang, People's Republic of China
Email: shahidnajam786@live.com

Abstract

The increasing number of cyber security threats, notably ransomware and malware, make traditional methods ineffective, hence the need for intelligent methods. This literature review delves into the latest advancements in cyber security technologies that leverage artificial intelligence (AI), machine learning (ML), and deep learning (DL) to enhance system defenses. Key focus areas include improving ransomware detection, developing more effective intrusion detection systems (IDS), securing Internet of Things (IoT) networks, and strengthening cryptographic methods. The reviewed studies highlight how AI-driven techniques—such as convolutional neural networks (CNNs), long short-term memory (LSTM) networks, and adversarial training—automate the detection of threats, optimize cyber security measures, and offer real-time responses to evolving risks. Innovative frameworks like Zero Trust Architecture (ZTA) and AI further bolster security by offering automated threat mitigation and anomaly detection. Furthermore, new metaheuristic algorithms are integrated into IDS systems to enhance the detection rate and minimize false positives. The advanced approaches show how AI could solve the constantly emerging challenges in cyber security and focus on a continuous development approach to make cyber security scalable, robust, and transparent when considering complex attacks.

Keywords: Cybersecurity; Artificial intelligence; Machine learning; Ransomware detection; Intrusion detection systems; Internet of Things; Cryptographic systems

1. Introduction

Metaheuristic optimization has become one of the essential techniques in solving subsequent computational problems and improving cybersecurity. This problem is especially noticeable as the digital world expands; new threats require the evolution of security measures: more effective, versatile, and, at the same time, less resource consuming. Some common approaches to managing cybersecurity threats can be slow and ineffective because the threats are constantly changing. Therefore, metaheuristic algorithms capable of searching large solution spaces and avoiding being trapped within local optima are enticing solutions. Researchers have shown that they have a lot of promise in enhancing the capabilities of cybersecurity systems, particularly in terms of the detection of threats, response mechanisms, and prognostic properties [1].

Therefore, metaheuristic optimization algorithms can be divided into population-based and single-solution-based, each type addressing the strengths and weaknesses of the other regarding specific problem types. These algorithms are designed to intelligently explore the search space and balance between exploration (searching new areas) and exploitation (refining current solutions). For instance, the Dipper Throated Algorithm (DTO), a recently developed metaheuristic, has shown excellent performance in feature selection and classification tasks, particularly in the medical field, such as Electrocardiogram (ECG) classification, where accurate detection is critical for patient outcomes . Similarly, the integration of metaheuristic models that hybridize different combinations has also been proven useful in difficult classification problems such as breast cancer diagnosis, showing that they can accurately classify complex, non-linear, high-dimensional datasets [2].

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

I like this aspect of metaheuristics because of the flexibility these algorithms possess, with an example being used in antennae design. For instance, recent innovations in artificial intelligence have been employed to enhance the design of T-shaped monopole antennas to achieve higher performance in contemporary communication systems [3]. In addition, metaheuristics were used to predict and model metamaterial antenna bandwidth, giving better models for such applications as wireless communication and radar Metaheuristic solutions have the scope of solving a vast number of engineering problems, as presented in the following applications.

Metaheuristic algorithms are widely discussed in cybersecurity; they are mainly used to improve the efficiency of machine learning in the systems of threat detection and response. Real-life situations such as risk detection in the supply chain using dynamic voting classifiers show that the algorithms are useful in high-risk category environments. In a similar context, the application of metaheuristics in agricultural image analysis has enhanced the efficiency of weed detection in those images captured by drones and, at the same time, has enhanced the rate of detection in large datasets also [5]. Making precise predictions is also vital in other fields, such as energy, where hybrid Long Short-Term Memory (LSTM) models optimized by metaheuristics have been used to forecast direct normal irradiation for solar power projects in hyper-arid regions such predictive ability is very important for energy resource management and demonstrates the versatility of these techniques.

Moreover, metaheuristic algorithms like the Chaotic Harris Hawks Optimization (HHO) algorithm have proven effective in solving unconstrained function optimization problems, further solidifying their relevance in cybersecurity and broader optimization challenges [8]. Recently, new methods such as the Waterwheel Plant Algorithm (WWPA) and the Al-Biruni Earth Radius (BER) algorithm [10] have been introduced, expanding the arsenal of optimization techniques available for solving complex problems. These algorithms have been tested within practical contexts, and examples include disease classification where Monkeypox disease has been classified using deep convolutional neural networks, showing promise of the algorithms in pandemic responses [6].

In addition to the medical and engineering fields, metaheuristics assist with environmental issues. For instance, in agricultural research, metaheuristic-operated models have been employed to estimate the daily evapotranspiration rates under semi-arid weather circumstances. These are useful for efficient water supply management in regions with high drought rates hence, metaheuristic approaches have helped to enhance the design and optimization of metamaterial antennas, which is one of the essential components of modern wireless communication [13]. Such approaches have also been used in smart city governance since traffic congestion can be avoided using soft GRU-based recurrent neural networks for efficient traffic flow patterns, providing better and real-time planning solutions for smart cities [7].

Metaheuristics have also been applied in environmental control because models developed with metaheuristics have been used to predict water quality. For instance, machine-learning models alongside the grid search method and metaheuristic optimization have been used to improve water quality prediction. At the same time, the algorithms explicitly show their capability to handle large and complex environmental data From the article, experience has also shown that metaheuristic techniques have been effectively applied to multi-objective optimization problems of even greater difficulty in industrial engineering The recent development of the Puma Optimizer

In the field of network security, metaheuristic-based optimization has been essential, for example, in feature selection for intrusion detection systems. These systems have been designed to monitor and prevent possibly fraudulent activities and have been enhanced significantly by hybrid metaheuristic algorithms to improve the detection of possible threats At the same time, changes based on optimized solutions of the proposed Dipper Throated Algorithm have been proposed to improve metamaterial antenna design which proves the constant development of such methods to address practical tasks in engineering. In the same way, metaheuristic algorithms are applied to deep learning models for the prediction of customer churn in the telecommunication industry, and they significantly enhance these predictions, where customer loyalty seems to be a critical factor [8].

Wireless sensor networks are another area where these algorithms have made a huge difference, specifically in using metaheuristic algorithms. For instance, Stochastic Fractal Search (SFS) combined with Particle Swarm Optimization (PSO) has been used to enhance the performance of K-Nearest Neighbors algorithms in such networks, improving both efficiency and accuracy Also, metaheuristics utilized for solving the energy efficiency problem in buildings, based on the hyperparameter optimization of multilayer perceptron models, show great prospects in energy saving and increasing resource-saving indicators

Wireless sensor networks have also experienced an improvement in their efficiency through the use of the Al-Biruni Earth Radius Optimization algorithm, which optimizes how such networks oversee resource and data utilization In education, metaheuristics have been used in selecting the best prediction models to estimate students' performance and enhance the predictiveness of these models; more light is shed on the aspects that influence students' performances in academic pursuits In addition, metaheuristic methods have also been applied in enhancing the predictive features for molding student performance across environments and computational studies that compare different learning algorithms for the performance of school data [9].

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

Metaheuristic optimization has also worked for cases protecting environments, such as satellite image classification for oil spills using machine learning. This application shows that these techniques could help towards environmental sustainability because event detection of pollution can be achieved more efficiently and effectively. Finally, in infrastructural maintenance, metaheuristics have been used in pothole detection in asphalt roads using deep learning models, which enhanced road safety and maintenance by providing an accurate real-time detection system [10].

Metaheuristic optimization methodologies are gaining more significant importance in numerous fields and application areas, including computer security, environmental monitoring, and infrastructure systems. Due to their ability to fine-tune sophisticated systems and learn from environmental changes, these algorithms are becoming critical tools for approaching some of the current global issues. The future contribution of metaheuristic algorithms to technology and innovation is expected to be higher and continue with steady improvements.

2. Literature Review

The nature and frequency of cyber threats have evolved with higher levels of sophistication and are constantly growing, especially ransomware and malware, making traditional solutions and approaches to security insufficient. This literature review explores recent advances in cybersecurity technologies, particularly those leveraging artificial intelligence (AI), machine learning (ML), and deep learning (DL). Various studies focus on enhancing ransomware detection, improving intrusion detection systems (IDS), securing Internet of Things (IoT) networks, and strengthening cryptographic systems. Such advanced techniques prove how AI can work in terms of threat identification, enhancing security measures of systems and eradicating new-age cyber threats. Combining these insights, this review underscores the need for the present and future constant creation of novel cybersecurity approaches.

The diversified types and strains of ransomware threats have posed new challenges to earlier microbiological safety solutions that required more of a biological approach. Discusses a multi-modal AI-based solution to improve ransomware attacks' detection, analysis, and prevention. By integrating machine learning (ML), deep learning (DL), and natural language processing (NLP), the approach provides a comprehensive defense against sophisticated ransomware tactics. Supervised and unsupervised ML algorithms identify ransomware signatures and anomalous behaviors, with convolutional neural networks (CNNs) detecting patterns in file structures and network traffic. In contrast, long short-term memory (LSTM) networks analyze system activities to identify potential attacks over time. NLP extracts indicators of compromise (IOCs) from unstructured data, such as phishing emails and dark web forums. Among the other features, sentiment analysis and topic modeling help improve prediction accuracy. Adversarial training as well as defensive distillation solve adversarial robustness. Using accuracy, precision, recall, F1-score, and ROC-AUC metrics, the proposed approach reveals the possibility of minimizing the consequences of ransomware attacks and the time required to solve them.

Global cyber threats have been reported to be rising in both frequency and severity and, therefore, require more strategic cybersecurity solutions. According to the work done in [11], intelligence for cybersecurity risk management is conducted using frameworks that form a basis for management solutions that contradict risk by evaluating existing cybersecurity data. Other structures, including the MITRE ATT&CK, provide up-to-date countermeasures in response to the attacker's capacity; however, they do not utilize hackers in constructing cyber threat intelligence. To partially fill this gap, the researchers created ATT&CK-Link, a new information technology artifact enriched with a transformer and multi-teacher knowledge distillation architecture. This framework extends hacker threats to the MITRE, a regularly applied framework. The paper illustrates how these hospital systems can use ATT&CK-Link to prevent hacker threats to their cyber infrastructure. This framework makes it possible for effective cybersecurity professionals to develop strategic, operational and tactical cyber threat intelligence. Similarly, ATT&CK-Link helps reinforce the knowledge base of information systems by providing structures with mechanisms for focused cybersecurity measurement, analysis, and broader text analysis investigation as part of real parallel multi-vector distillation and classification.

As the threat actors' process evolves, so does the threat environment, making it necessary to shift the cybersecurity strategies. Zero Trust Architecture (ZTA) has become a robust model based on the principle of "Never Trust, Always Verify," demanding intelligent access control and threat mitigation. Artificial Intelligence (AI), particularly Machine Learning (ML), offers significant potential to augment ZTA by automating threat detection and enabling real-time responses. This work examines the solution of AI-embedded threat detection under ZTA architectures, where ML algorithms are employed to recognize anomalies and provide responsive countermeasures. It highlights the limitations of traditional security models in combating sophisticated attacks like social engineering and advanced persistent threats (APTs). ML is best used for segmenting and analyzing big data security sets to identify anomalous or deviant user behavior. In addition, AI responds to incidents automatically and moves for threatening hunting in ZTA. The study also acknowledges the challenges of integrating AI, emphasizing the need for high-quality training data and explainable AI (XAI) to ensure transparency [12].

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

The Internet of Things (IoT) interconnects physical and virtual objects embedded with sensors, software, and technologies that exchange data over the Internet. Despite IoT's benefits by establishing connections and personalizing billions of devices and people, it presents severe threats to security. Due to the exponential growth in the use of IoT devices, they are a favorite of hackers who aim at spying on users and intruding on their privacy. Because of such features and constraints of IoT, one can see some of the threats unique to this domain,, including confidentiality, authentication, access control and privacy. This paper measures and discusses the threats in IoT and categorizes them based on the layers of the IoT model. They include countermeasures, mitigation measures, and other related topics: An examination of selected common application layer protocols commonly applied on IoT networks, their security threats/vulnerabilities,, and some of their main constraints[13].

The increasing prevalence of Internet of Things (IoT) systems has raised significant security concerns, with cyber-attacks such as denial-of-service attacks, malware infections, and phishing posing serious risks. Using security mechanisms based on machine learning is suggested for overcoming the mentioned challenges, underlining the need for the models' high stability and several defensive actions. The study employs the Ridge Classifier as a strong weapon for finding arrangers in IoT systems. It provides the ability to detect and prevent cyber-attacks in real-time with the help of a comprehensible array of secure network data. Experimental findings reveal that the system's effectiveness for threat identification and prevention is very high, with a rate of accuracy recorded at 97 percent. This effectiveness strengthens the governmental and business networks and makes important data safe from malicious threats. The study emphasizes that it is impossible to ensure the so-called 'secure-by-design' IoT networks without the use of Machine Learning-based security instruments and that the proposed technique of the 'Ridge Classifier' model comprehensively insulates IoT networks against cyber threats in terms of data and network integrity, confidentiality, and availability[14].

Network cyber threats have targeted many intrinsic system vulnerabilities; thus, network intrusion detection is a critical component of the cybersecurity field. Intrusion detection systems (IDSs) using machine learning (ML) have been developed to make decisions with minimal human intervention. While ML-based IDS advancements have surpassed traditional methods, they still face challenges in achieving high detection rates (DR) and low false alarm rates (FAR)[15]. This paper proposes a meta-heuristic optimization algorithm-based hierarchical IDS to enhance the identification of different attacks and safe computing spaces. The approach consists of three stages: data pre-processing, feature extraction, and data division; choosing the best hyperparameters of the ELM using two new meta-heuristic algorithms; and sorting of binary models using a hierarchical anomaly detection system. The proposed IDS effectively and efficiently does multi-classification, and the average accuracy, DR, and FAR were estimated to be 98.93%, 99.63% and 99.19%, with a FAR of 0.01 on the UNSW-NB15 and CICIDS2017 dataset [16].

The increasing use of the Internet, with its inherent vulnerabilities, has necessitated the adoption of Intrusion Detection Systems (IDS) to ensure network security. Presents IDSs as important systems that recognize intrusions, invasions, and network failures [17]. The intrusion detection problem is posed as classification, and selecting the features is important for classification techniques [18]. Several conventional approaches exist, including Neural Networks, Fuzzy Logic, Data Mining, and Metaheuristic techniques. A novel approach is introduced using the Horse Herd Optimization Algorithm (HOA) for feature selection in network intrusion detection. The Adjustment Hopping Oscillator is currently incorporated into a discrete quantum, inspired, and multi-objective optimizer. MQBHOA, this algorithm incorporates quantum-computing components to optimize the exploration-exploitation trade-off. The K-Nearest Neighbour (KNN) classifier is used, and the method is tested on NSL-KDD and CSE-CIC-IDS2018 datasets[19]. The results compare favorably to previously evaluated algorithms and show a 6% increase in feature selection and classification accuracy – 99.8% for intrusion detection.

Internet services and applications have become more popular, potentially escalating cyber crusades, unauthorized application utilization, and threatening service accessibility and consumer privacy. A network Intrusion Detection System (IDS) is designed to detect abnormal traffic behaviors that firewalls might miss. Some measures include feature selection,, which is a process of narrowing narrowing down data dimensions to eliminate irrelevant data that adds value to IDS. This paper presents a modified Grey Wolf Optimization (GWO) algorithm to improve IDS efficacy in detecting normal and anomalous network traffic. The enhancements include the intelligent filter and wrapper integrated smart initialization phase to promote informative features initially. Additionally, the Extreme Learning Machine (ELM) is used for high-speed classification, with GWO employed to optimize ELM's parameters. In general attacks detection tested on the UNSWNB-15 dataset, the proposed model produced accuracy, F1-score and G-mean of 81%,78% and 84%, respectively, and crossover and false positives of less than 30%.

Rapid developments in Internet of Things (IoT) systems have led to widespread integration into daily life, particularly in areas like healthcare, where real-time monitoring can significantly affect outcomes. According to [20], concerning the issues that hinder IoT interoperability on a larger scale, one of the challenges is sustainability, especially in healthcare services, which has to provide accurate organization of services without negatively influencing the environment. Security remains fundamental to the survival of IoT systems, and early detection and tackling challenges remain compulsory [21]. The present research explores the IoT security concern using machine learning optimized with a modified Firefly

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

algorithm applied to the context of Healthcare 4.0 IoT devices. Metaheuristic solutions are found to be optimal and powerful in solving NP-hard problems with acceptable speed and precision to support sustainable systems. Machine learning models used in experiments included a range of models trained on IoT structure's synthetic datasets, enhanced by improved Firefly metaheuristics. Shapley's Additive explanations (SHAP) analysis was used to identify key factors contributing to security issues. Testing and comparison experiments reveal meaningful enhancements to solve the issues mentioned above [22].

In recent years, rapid advancements in smart devices have led to an exponential increase in the data generated, known as Big Data (BD), which traditional analytics techniques struggle to handle. The increase in these data also leads to new opportunities for attack methods such as SQL injection attacks, Operating Systems fingerprinting attacks, and malicious code execution during data analysis [23]. This paper explores Machine Learning (ML) and Deep Learning (DL) models capable of identifying and mitigating known and unknown attacks. These techniques use traffic data sets for training and testing to make wise decisions for an attack in a large network environment. The paper also proposes a DL and ML-based Secure Data Analytics (SDA) architecture to classify input data as normal or attack-related. Threat modeling is used to identify challenges to expand a detailed taxonomy of the SDA and encompasses surface area, efficiency, latency, accuracy, and reliability. Lastly, comparing existing SDA proposals enables users to select the most appropriate solution according to its benefits [24].

Cybersecurity has gained significant attention due to the widespread adoption of the Internet of Things (IoT), the rapid growth of computer networks, and the increasing number of related applications. As highlighted in [25], detecting cyber-attacks or anomalies in networks and developing effective intrusion detection systems (IDS) is becoming increasingly crucial. This paper introduces "IntruDTree," a machine learning-based security model designed to build an intelligent IDS. The model categorizes the security features based on the priority level and builds a generalized detection tree model from the most relevant features. This approach facilitates the increase of pass rates of other unseen cases and reduces computational costs regarding feature dimensions. The impact of the IntruDTree model was also investigated through experiments on cybersecurity datasets, where several performance measures such as precision, recall, F1-score, accuracy, and ROC values were used in the evaluations. Further, IntruDTree was evaluated against conventional machine learning techniques such as naive Bayesian, logistic regression, support vector machine, and k-neighbor and exhibited the best result.

An intrusion detection system (IDS) is crucial for identifying complex network attacks. Anomaly-based IDS (AIDS) systems have increasingly utilized machine learning (ML) and deep learning (DL) algorithms [26]. Nevertheless, the literature presents some shortcomings, including random choice of sequences, utilization of outdated data sets and superficial method validation. This paper also compares and contrasts various algorithms, parameters, and testing criteria in currently available AIDS studies using different datasets and attack types. Ten well-known supervised and unsupervised ML algorithms are used to estimate successful AIDS solutions. These include supervised methods like artificial neural networks (ANN), decision trees (DT), k-nearest neighbor (k-NN), and unsupervised methods like k-means and self-organizing maps (SOM). The analysis also discusses algorithm tuning and training parameters about classifier assessment.[27] In contrast to previous works, this work assesses 31 ML-AIDS models using true positive/negative rates, accuracy, precision, recall, the F1-score, and training/testing time. Despite being a highly imbalanced multiclass CICIDS2017 dataset, k-NN-AIDS, DT-AIDS, and NB-AIDS models were more effective in detecting web attacks than others.

The rise in computer networks and internet attacks has become a significant concern for service providers, leading to the increased need for effective intrusion detection systems (IDSs) to mitigate network intrusions. while IDSs have been crucial in identifying network attacks, many existing models struggle with high false alarm rates and difficulty in detecting certain attack types, particularly User-to-Root (U2R) and Remote-to-Local (R2L) attacks. These attacks sometimes pose lower detection algorithm accuracy in the current IDS model. To address these challenges, this paper proposes a bidirectional Long-Short-Term-Memory (BiDLSTM) based IDS designed to improve detection accuracy and reduce false alarms. The proposed model was trained and tested NSL-KDD, a standard IDS development dataset. Experimental results confirm the usefulness of the BiDLSTM model, which, besidesbesides having higher accuracy, precision, recall, and F1-score compared with traditional LSTM or some other state-of-art models, has also significantly lowered the number of false alarms. Furthermore, using the proposed BiDLSTM model, it was possible to detect the U2R and R2L attacks with improved detection accuracy relative to models based only on LSTM.

Wireless sensor networks (WSNs) are widely used across industries for monitoring, data transmission, and gathering tasks, especially within the Industrial Internet of Things (IIoT). However, due to the small sensor nodes (SN) involved, resource management aimed at energy efficiency is a key challenge. Power consumption for the interpretation, transmission and storage of data between the sensors should be minimal to enhance the operation of the network. In addition to energy efficiency, the aspects of network security, namely intrusion detection and prevention, constitute a significant issue. This work introduces the Meta-Heuristic-Based Secure and Energy-Efficient Routing (MHSEER) protocol for WSN-IIoT, which optimizes forwarding decisions based on hops, connection integrity, and remaining energy.

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

To enhance security, the protocol incorporates counter-encryption mode (CEM) for data encryption. The protocol operates in two stages: the first is applicable for secure data routing using heuristics, and the second is CEM for security enhancement. When compared MHSEER with other protocols such as Sectrust-RPL and HBEER, the performance is enhanced greatly by boosting throughput to 95.81%, reducing packet drop ratio,h, packet delay and energy consumption and faulty pathways to 5.12%, 0.10ms, 0.0102mJ and 6.51%, respectively.

The Internet of Medical Things (IoMT) security is crucial, as it connects various medical devices to enhance patient care and real-time monitoring. Proposed high-security frameworks that include attribute-based access control, encryption and privacy. However, many of these models are either too complex or not flexible enough for real-time processing, for their security performance relies heavily on internal parameters that cannot be changed in response to a new threat. These drawbacks are the main reason for developing an improved hybrid metaheuristic model for better security of IoT in healthcare. The model first employs blockchain technology but can dynamically change internal hashing and encryption as required. By combining Elephant Herding Optimization (EHO) and Grey Wolf Optimization (GWO), the model optimizes security and quality of service in blockchain-based IoMT systems [28]. The forward fitness functions are secure, and the service quality is good against threats like DDoS, man-in-the-middle, masquerading, and Sybil attacks. The other is the dual fitness functions. In this proposed model, the average results of state-of-the-art models have been compared, and the results obtained from the proposed model are increases in network consistency by 8.7%, throughput by 6.4% and packet delivery by 8.2%. In contrast, attack detection and mitigation are 9.4% higher. The potential of the model to be used in real-time healthcare use cases can be inferred from these results.

The Internet of Things (IoT) refers to a network of physical objects communicating with other devices through the Internet. Which states that security plays a significant role in IoT-based communication since it is hard to standardize the devices in the network. These systems have been described as interconnects; it remains difficult to guarantee security, identity, permission, and privacy. This paper proposes a novel Chaotic Bumble Bees Mating Optimization (CBBMO) algorithm for secure data transmission integrated with a trust-sensing model (CBBMOR-TSM) to address these issues. The use of the concepts of chaos in enhancing the rate of convergence of the CBBMO model increases the rate of convergence of the classical Bumble Bees Mating Optimization. The model's primary objective is to design a trust-sensing system for capturing malicious nodes and guarantee secure routing. The trust values of IoT nodes will be computed using direct and indirect trust to identify threats. Security routing is then done using the CBBMO algorithm to determine the best path for transmitting data. The model's performance was tested extensively, showing superior results with a higher average Packet Delivery Ratio (PDR) of 0.931 and a lower average Packet Loss Ratio (PLR) of 0.069, outperforming other methods such as TRM_IOT, OSEAP_IOT, and MCTAR-IOT, which had higher PLRs of 0.219, 0.161, and 0.110, respectively.

Even in today's advanced digital security systems using passwords or PIN codes developed, cryptographic keys are usually the output of stochastic or probabilistic random processes or are derived using complex mathematical transformations. As for these methods, despite their considerable strength, their storage and distribution need proper and costly means. According to to apply biometric data for generating cryptographic keys to avoid difficulties in storing and distributing them. The research focuses on biometric key generation technologies utilizing deep learning models, specifically convolutional neural networks (CNNs), to extract biometric features from facial images. A set of features is then extracted from the audio signals subjected to code-based cryptographic extractors. The performance of different deep learning models and the cryptographic extractor was assessed regarding detection accuracy and false positive rate, and the optimized parameters yielded less than 10% error rate. The low error rate of the generated key makes the generated keys suitable for biometric authentication. Furthermore, the use of code-based cryptographic extractors is secure from quantum attacks and makes the biometric key generation technique more viable in today's IT security systems. The present study contributes to designing safe, effective, and robust authentication techniques due to biometrics and deep learning [29].

This study focuses on side-channel attacks targeting cryptographic devices protected by the Advanced Encryption Standard (AES). The research introduces the assessment of guessing entropy (GE) and the associated uncertainty in machine-learning-based attacks that rely on power measurements. For the first time, GE was evaluated for the entire key, and uncertainty was applied to the side-channel attack, making the device more decisive in terms of vulnerability. The attack employs a multilayer perceptron (MLP) to classify power traces leaked from physically accessible devices, with a public database used to ensure reproducibility. Critical values for resilient state estimation can be used to quantify uncertainty in key byte retrieval and then projected to the total key using Monte Carlo analysis. The findings reveal that the former holds a probability of 10% based on roughly 4000 attack traces, whereas the latter holds for fewer than ten attempts. This means that the side-channel attack could reveal a complete cryptographic key near one in every ten tries across one hundred similar gadgets, underscoring a huge safety vulnerability, especially in IoT settings. The study reflects that the field requires better vulnerability testing and enhanced countermeasures.

With the rise of the Internet of Things (IoT), vast amounts of data that require processing are generated. Although cloud computing usually solves such tasks, they have disadvantages, such as latency and security fields. Fog computing has

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

emerged to complement cloud computing, enhancing the Quality of Service (QoS) by addressing these limitations. However, it is challenging to decide which node to choose because of cloud and fog node heterogeneity; fog nodes are resource-constrained and have limited processing capability. As a result, to fully exploit the fog nodes, this paper develops a secure two-step service placement framework. The first step involves classifying services to determine whether they should be processed on the cloud or fog tier, using an improved adaptive neuro-fuzzy inference system (ANFIS) for prediction. The second step applies a novel metaheuristic-based hybrid algorithm combining a chaotic-based grasshopper optimization algorithm (CGOA) with a genetic algorithm (GA) to schedule services at the fog tier. The proposed CGOA adapts the shortcomings of the basic GOA, such as slow convergence and being a victim of local minima, by using ideas from chaos theory and Opposition-based learning. The cumulative makespan, total functions executed and energy used by the proposed model, upon testing with Google trace dataset, were found to yield better percentage improvements by an average of 9.2% on makespan, 4.25 % on the total functions executed and 2.75 % on the energy dissipation as compared to the existing literature.

Cloud computing is a rapidly emerging distributed computing model that offers utility computing services over the Internet context suitable for large-scale, workflow-based, large-application solutions for business and science. More specifically, the issue of scheduling the multiple workflows that comprise a processing pipeline is critical since it determines execution time and associated costs. This paper presents an enhanced workflow scheduling approach by hybridizing the recent Ant-Lion Optimization (ALO) algorithm with Particle Swarm Optimization (PSO), specifically designed for cloud environments. A security mechanism using the Data Encryption Standard (DES) is also incorporated to secure cloud data during the scheduling process. The proposed hybrid optimization is expected to enhance the scheduling outcome and security compared to other frameworks. The proposed method is validated with the help of the CloudSim tool, which analyzes cost, load balancing, and makespan. The results show that the proposed method outperforms existing approaches such as round robin (RR), ALO, PSO, and GA-PSO, reducing costs by up to 30% compared to RR, with similar load balancing and makespan improvements. The proposed system also shows energy efficiency and system reliability advantages.

The problem that internet users face today is the emergence of various types of viral software, particularly polymorphic viruses that are more flexible than traditional viruses. This is because polymorphic malware modifies some features aimed at escaping detection by traditional models of picking out incidents based on signatures, To address this, the study examines the following machine learning algorithms to distinguish the most accurate algorithm detecting malware. A high detection ratio was used to decide which algorithm was the most effective, and the confusion matrix was used to determine the number of false positives and false negatives to measure the system's efficacy. The work showed that spectrum symmetry could be used to identify malicious traffic and enhance the cyber protection of computer networks based on the comparison of various models such as Naive Bayes, SVM, J48, and RF. The findings revealed that Decision Trees (DT) achieved the highest detection accuracy (99%), followed by Convolutional Neural Networks (CNN) at 98.76% and Support Vector Machines (SVM) at 96.41%. Additionally, DT, CNN, and SVM achieved low false positive rates (FPR) of 2.01%, 3.97%, and 4.63%, respectively, underscoring the importance of advanced detection methods as malware becomes increasingly sophisticated.

Malware is constantly changing,; therefore improvised ways of detecting it are required. Dynamic malware detection is proposed to combat the ever-emerging and even more complex internet. As for the problem discussed in the paper, traditional manual heuristic approaches to addressing the enormous volume of malicious programs are no longer sufficient. Based on this, the study demonstrates an automatic behavior-based malware detection and evaluation of threats in an emulation environment using machine-learning algorithms. Such behaviors are logged down, encoded, and quantized into vectors in sparse model forms for further use. Classifiers such as k-Nearest Neighbors (kNN), Decision Trees (DT), Random Forest (RF), AdaBoost, Stochastic Gradient Descent (SGD), Extra Trees, and Gaussian Naive Bayes (NB) were applied to synthesize the results. RF, SGD, Extra Trees, and Gaussian NB classifiers achieved 100% accuracy, with perfect precision (1.00), recall (1.00), and F1-scores (1.00) in the testing phase. The implications explain automatic behavior-based malware analysis when augmented with machine learning for the rapid identification of emerging malware threats to be efficient.

The analyzed publications show the centrality of AI, ML, and DL in present-day cyber security strategies in response to problems such as ransomware or attacks on IoT devices. These technologies enhance stronger, flexible and timely countermeasures to new risks. In addition, they offer solutions that allow various types of protection, such as healthcare, cloud, and industrial networks for businesses at scale. Since the threat moves dynamically, there is a need for the constant development of these fields to help protect structures that are connected to digital technology. More specifically, the next studies need to devote their efforts to enhancing these systems' scalability, soundness, and interpretability to build a step ahead of cyber adversaries [30].

3. Conclusion

This literature review focuses on the current trends in enhancing cyber security technologies through AI, ML, and DL for current cyber threats. From ransomware detection and intrusion detection systems (IDS) to IoT and cloud computing

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

security, these approaches have proven essential in combating increasingly sophisticated and adaptive cyber-attacks. Such integration proves that the application of machine learning models alongside traditional ones increases the overall detection rate, minimizes false positives, and improves system overall system durability. Furthermore, deploying metaheuristic algorithms, adversarial training, and explainable AI (XAI) shows promise in creating more adaptive and robust security solutions. However, due to the ever-changing nature of cyber threats, further research could help maintain their relevance, efficiency and ability to neutralize new threats on a large scale. It is therefore advisable that future endeavors be directed towards enhancing visibility, increasing potential response rates in rinl-time, and continuing to explore other arenas where similar inventions may be applied in otoahead of the causes of cyber security threats.

References

[1] R. Alkanhel, E.-S. El-Kenawy, A. Abdelhamid, A. Ibrahim, M. Alohali, et al., "Network intrusion detection based on feature selection and hybrid metaheuristic optimization," *Computers, Materials and Continua*, vol. 74, pp. 2677–2693, 2022, doi: 10.32604/cmc.2023.033273.

[2] L. Saha, H. K. Tripathy, T. Gaber, H. El-Gohary, and E.-S. M. El-Kenawy, "Deep churn prediction method for telecommunication industry," *Sustainability*, vol. 15, no. 5, Art. no. 5, 2023, doi: 10.3390/su15054543.

[3] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data*, vol. 11, no. 1, p. 105, 2024.

[4] B. R. Maddireddy and B. R. Maddireddy, "Evolutionary algorithms in AI-driven cybersecurity solutions for adaptive threat mitigation," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 2, Art. no. 2, 2021.

[5] B. M. Ampel, S. Samtani, H. Zhu, H. Chen, and J. F. Nunamaker Jr., "Improving threat mitigation through a cybersecurity risk management framework: a computational design science approach," *Journal of Management Information Systems*, vol. 41, no. 1, pp. 236–265, 2024, doi: 10.1080/07421222.2023.2301178.

[6] L. Gudala, M. Shaik, and S. Venkataramanan, "Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: an exploration of real-time anomaly identification and adaptive mitigation strategies," 2021. Accessed: Oct. 11, 2024. [Online]. Available: https://thesciencebrigade.com/JAIR/article/view/222.

[7] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions," *Electronics*, vol. 11, no. 20, Art. no. 20, 2022, doi: 10.3390/electronics11203330.

[8] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Passive rule-based approach to detect sinkhole attack in RPL-based Internet of Things networks," *IEEE Access*, vol. 11, pp. 94081–94093, 2023.

[9] A. Alomiri, S. Mishra, and M. AlShehri, "Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 645–659, 2024, doi: 10.12785/ijcds/160148.

[10] K. A. ElDahshan, A. A. AlHabshy, and B. I. Hameed, "Meta-heuristic optimization algorithm-based hierarchical intrusion detection system," *Computers*, vol. 11, no. 12, Art. no. 12, 2022, doi: 10.3390/computers11120170.

[11] R. Ghanbarzadeh, A. Hosseinalipour, and A. Ghaffari, "A novel network intrusion detection method based on metaheuristic optimisation algorithms," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 6, pp. 7575–7592, 2023, doi: 10.1007/s12652-023-04571-3.

[12] A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A modified grey wolf optimization algorithm for an intrusion detection system," *Mathematics*, vol. 10, no. 6, Art. no. 6, 2022, doi: 10.3390/math10060999.

[13] N. Savanović, A. Toskovic, A. Petrovic, M. Zivkovic, R. Damaševičius, et al., "Intrusion detection in healthcare 4.0 Internet of Things systems via metaheuristics optimized machine learning," *Sustainability*, vol. 15, no. 16, Art. no. 16, 2023, doi: 10.3390/su151612563.

[14] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: a taxonomy and threat model," *Computer Communications*, vol. 153, pp. 406–440, 2020, doi: 10.1016/j.comcom.2020.02.008.

[15] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: a machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, Art. no. 5, 2020, doi: 10.3390/sym12050754.

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025

[16] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[17] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Systems with Applications*, vol. 185, p. 115524, 2021, doi: 10.1016/j.eswa.2021.115524.

[18] A. Sharma, H. Babbar, S. Rani, D. K. Sah, S. Sehar, et al., "MHSEER: a meta-heuristic secure and energy-efficient routing protocol for wireless sensor network-based industrial IoT," *Energies*, vol. 16, no. 10, Art. no. 10, 2023, doi: 10.3390/en16104198.

[19] A. Kanneboina and G. Sundaram, "Improving security performance of Internet of Medical Things using hybrid metaheuristic model," *Multimedia Tools and Applications*, 2024, doi: 10.1007/s11042-024-19188-7.

[20] S. Gali and V. Nidumolu, "An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things," *Cluster Computing*, vol. 25, no. 3, pp. 1779–1789, 2022, doi: 10.1007/s10586-021-03473-3.

[21] O. Kuznetsov, D. Zakharov, and E. Frontoni, "Deep learning-based biometric cryptographic key generation with post-quantum security," *Multimedia Tools and Applications*, vol. 83, no. 19, pp. 56909–56938, 2024, doi: 10.1007/s11042-023-17714-7.

[22] P. Arpaia, F. Caputo, A. Cioffi, A. Esposito, and F. Isgrò, "Uncertainty analysis in cryptographic key recovery for machine learning-based power measurements attacks," *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–8, 2023, doi: 10.1109/TIM.2023.3284933.

[23] S. Singh and D. P. Vidyarthi, "An integrated approach of ML-metaheuristics for secure service placement in fog-cloud ecosystem," *Internet of Things*, vol. 22, p. 100817, 2023, doi: 10.1016/j.iot.2023.100817.

[24] J. Kakkottakath Valappil Thekkepuryil, D. P. Suseelan, and P. M. Keerikkattil, "An effective meta-heuristic based multi-objective hybrid optimization method for workflow scheduling in cloud computing environment," *Cluster Computing*, vol. 24, no. 3, pp. 2367–2384, 2021, doi: 10.1007/s10586-021-03269-5.

[25] M. S. Akhtar and T. Feng, "Malware analysis and detection using machine learning algorithms," *Symmetry*, vol. 14, no. 11, Art. no. 11, 2022, doi: 10.3390/sym14112304.

[26] M. S. Akhtar and T. Feng, "Evaluation of machine learning algorithms for malware detection," *Sensors*, vol. 23, no. 2, Art. no. 2, 2023, doi: 10.3390/s23020946.

[27] S. Fraihat, S. Makhadmeh, M. Awad, M. A. Al-Betar, and A. Al-Redhaei, "Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm," *Internet of Things*, vol. 22, p. 100819, 2023.

[28] F. Alqahtani, "AI-driven improvement of monthly average rainfall forecasting in Mecca using grid search optimization for LSTM networks," *Journal of Water and Climate Change*, vol. 15, no. 4, pp. 1439–1458, 2024.

[29] N. O. Aljehane, H. A. Mengash, M. M. Eltahir, F. A. Alotaibi, S. S. Aljameel, A. Yafoz, and M. Assiri, "Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security," *Alexandria Engineering Journal*, vol. 86, pp. 415–424, 2024.

[30] S. Bajpai, K. Sharma, and B. K. Chaurasia, "A hybrid meta-heuristics algorithm: XGBoost-based approach for IDS in IoT," *SN Computer Science*, vol. 5, no. 5, p. 537, 2024.

DOI: https://doi.org/10.54216/MOR.040105
Received: February 05, 2025 Revised: March 03, 2025 Accepted: May 09, 2025