# Enhanced IoT Security and Intrusion Detection Using Optimized Hybrid Deep Learning and Advanced Encryption Techniques

Yashraj Mishra
M.Tech Scholar
Department of Computer Science & Engineering
Oriental Institute of Science and Technology
Bhopal, Madhya Pradesh, India
yashrajmishra100@gmail.com

Sanjay Pal
Professor
Department of Computer Science & Engineering
Oriental Institute of Science and Technology
Bhopal, Madhya Pradesh, India

***Abstract:*** This study introduces a hybrid deep learning architecture intended to improve intrusion detection and data security on the Internet of Things (IoT) platform. The model integrates Hierarchical Convolutional Neural Networks (HCNN) with a Calibrated Random Forest (RF) classifier, leveraging the spatial feature extraction and structured decision-making power. For better accuracy and lower complexity, the Enhanced Harris Hawks Optimization Algorithm (EHOA) is employed for feature selection. The system handles IoT network traffic via K-Means Clustering, label encoding, and normalization for proper input preparation for model training. Evaluation is done through principal metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and PR-AUC. The model attains an accuracy of 83.41%, a precision of 85.29%, a recall of 74.3%, and an F1-score of 79.42%, with a high capability for detection even on imbalanced datasets. Furthermore, a KH-AES (AES-128) encryption mechanism is incorporated to protect data transfer, transforming sensitive traffic into ciphertext encryption while maintaining confidentiality and integrity. The hybrid method provides real-time and scalable anomaly detection while keeping false positives at a low level. With the integration of sophisticated feature selection, deep learning, and encryption, the system provides an efficient solution for managing the intricate security issues found in contemporary IoT networks.

**Keywords:** Internet of Things (IoT), Intrusion Detection System (IDS), Hybrid Convolutional Neural Network (HCNN), Calibrated Random Forest, Feature Selection, Enhanced Harris Hawks Optimization Algorithm (EHOA), Network Security, KH-AES Encryption, Anomaly Detection, Deep Learning, Cybersecurity, K-Means Clustering, Data Preprocessing, Real-time Threat Detection, Imbalanced Data Classification.

## I. INTRODUCTION

IoT security is a very essential part of contemporary cybersecurity measures, meant for safeguarding sensitive data and device functionalities against cyber threats and unapproved access. As IoT continues to become increasingly embedded in everyday life—particularly smart homes and AI-enabled appliances—data accuracy, confidentiality, and privacy have become very relevant. In spite of this, the built-in resource-limited nature of IoT devices renders the application of strong security measures problematic, and such implementations tend to be subject to trade-offs between protection and performance. The presently existing threats range over both the device and cloud layers and encompass code manipulation, terminal vulnerabilities, and business layer access protocol exploitation, which can lead to massive attacks or permission violations [1]. Lightweight cryptographic methods are generally used to address performance requirements but remain vulnerable to Side Channel Analysis (SCA) attacks, generating data in motion concerns that are most susceptible in IoT systems [2]. For smart homes, the convergence of sensitive environmental and behavioural information further intensifies the demand for safe handling of data, since these systems tend to connect to healthcare services and other privacy-related applications [3]. In addition, embracing advanced authentication and encryption methods, although it will improve security, can impair user experience because it adds latency and makes the system less responsive—particularly in real-time, AI-based systems [4]. Mitigating these complex challenges is crucial to constructing robust, scalable, and user-friendly IoT environments.

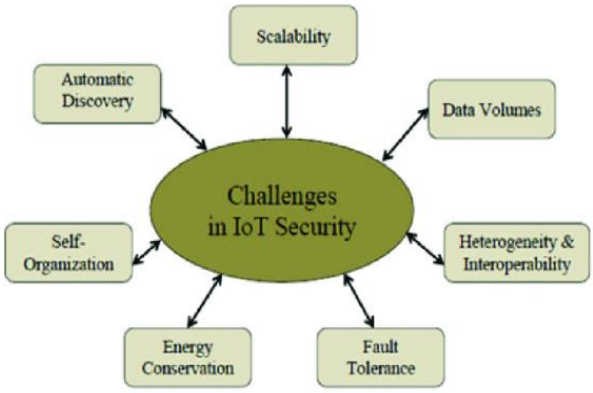


Fig 1. Challenges in IOT Security [5].

Simulation of IoT environments also poses a number of essential challenges, such as security, energy efficiency, heterogeneity, and scalability. Security is a concern due to the passing of sensitive information over interconnected devices, exposing them to cyberattacks; simulations need to model properly both these attacks and attacker behaviour [6]. Energy consumption is also an essential concern since most IoT devices are battery driven, which means simulations need to exhibit realistic energy consumption patterns. The heterogeneity of IoT devices, with varying

manufacturers, standards, and protocols, introduces complexity, requiring simulations that can effectively model this heterogeneity. As IoT networks grow, conventional simulation tools tend to be unable to capture the intricate interactions of large, heterogeneous systems [6].

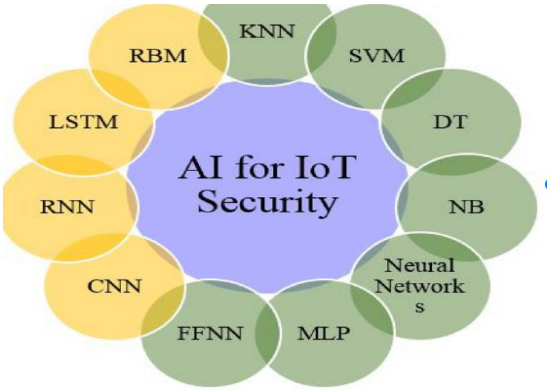


Fig.2 AI for IoT Security [7].

To overcome these challenges, AI has proven to be a useful tool in improving IoT security. AI not only facilitates anomaly detection but also assists in handling privacy by way of uncertainty since plain data masking is not adequate anymore; nevertheless, balancing data utility and anonymization is still an issue [8]. Furthermore, cyber-physical systems that integrate computing and physical processes are vulnerable to attacks at the sensor level and data tampering, which requires effective, real-time defence mechanisms [9].

As IoT systems become more deeply embedded in industries such as health, home automation, and manufacturing, so does the need for strong security mechanisms. Legacy encryption algorithms such as RSA, ECC, and AES have been the cornerstones of securing communication and sensitive information. Yet with new security threats from quantum computers, namely Shor's and Grover's algorithms, come challenges to the security of these systems by laying bare the computational hardness assumptions underpinning them [10]. This has led to increased activity towards quantum-resistant cryptography and lightweight cryptographic primitives that are appropriate for low-resource IoT devices. Lightweight Encryption Algorithms (LEAs) with secure key scheduling, S-boxes, and hardware optimizations like pipelining provide better performance and security against cryptanalytic attacks. LEAs' minimal computational and memory requirement makes them suitable for IoT end-to-end communications, especially where power and processing limitations are high [11][12]. In addition, cryptographic technology is essential not just in IoT security but also in financial ecosystems, such as cryptocurrencies Bitcoin and Ethereum, that utilize ECC, SHA-256, and smart contracts to facilitate secure, decentralized operations [13]. For other applications, such as image encryption, which are prevalent in surveillance and healthcare IoT systems, lightweight chaos-based cryptography using confusion and diffusion techniques is both efficient and secure [14].

Aside from encryption, hybrid deep models are increasingly being used to advance the detection of attacks in adaptive IoT settings. The models that marry the ability to conduct spatial analysis in CNNs with LSTMs' temporal learning ability are optimized via metaheuristics such as the Harmony Search algorithm for higher performance on IoT data [15]. Deep learning assists in the extraction of useful features and detection of sophisticated, dynamic threats in real-time, remedying the limitations of conventional intrusion detection systems (IDS), including high false-positive rates and poor scalability [16][17]. Real-time systems for anomaly detection, fortified by federated learning, edge computing, and ensemble ML methods such as HTM-Bayesian models, are crucial for large-scale IoT and cloud networks with latency, resource scarcity, and privacy being significant factors [18]. In addition, the coupling of blockchain and hybrid deep learning provides greater data integrity and decentralization, especially in delicate areas such as healthcare. Blockchain provides tamper-proof, open, and transparent records of IoT data, enhancing access control and minimizing points of failure in the centre [19]. Challenges, however, exist in scalability of blockchain systems, maintaining data privacy, and being interoperable with current healthcare infrastructures [20]. The deployment of smart IoT environments on the back of AI, CPS, and CC provides predictive maintenance, resource utilization, and decision-making in real-time. Together, these advance digital transformation within industries, maximizes operational effectiveness, minimizes downtime, and facilitates strategic development through data insight [21].

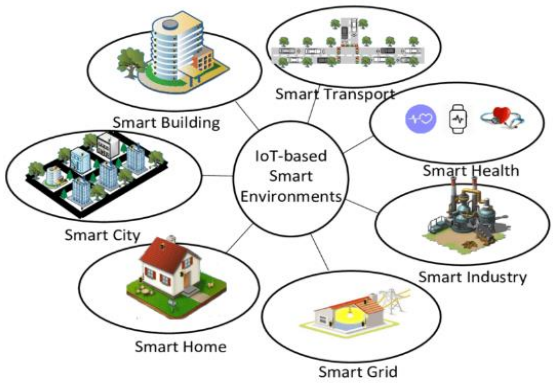


Fig. 3 IoT-based Smart Environments [22].

The Internet of Things (IoT) brings together physical devices with internet connectivity, including smart devices, IoT applications, and graphical user interfaces (GUIs). Smart devices, like smart TVs and thermostats, have computational power, while IoT applications gather and process data from sensors, and GUIs—such as smartphones—allow device management. IoT networks often include devices, gateways, and cloud servers to facilitate easy communication and automation. As technological development accelerates, the world's total of IoT devices is expected to grow from 9.7 billion in 2020 to more than 29 billion by the year 2030, reflecting their increasing influence in homes and various industries [23].

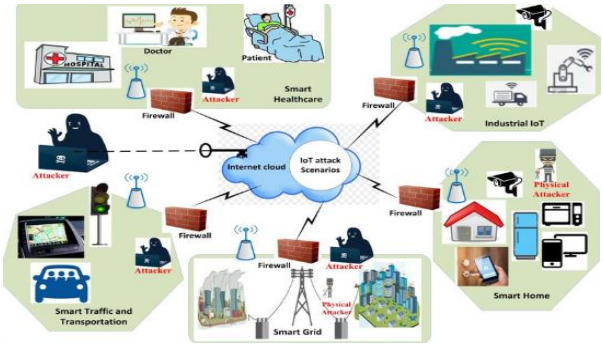


Fig 4 IoT Security Attack Scenarios in Different Application Areas [24].

Security is a core necessity for all IoT applications, especially as they move into high-stakes areas such as smart cities, environmental monitoring, smart grids, and emergency response systems. They need strong security because of the sensitivity of these applications and the consequences of a breach that would range from privacy invasion in smart cities to life-loss errors in emergency systems [25]. As IoT converges with AI in intelligent appliances, it facilitates increased convenience and efficiency but also adds sophisticated vulnerabilities. Assessing IoT security entails assessing performance metrics such as latency, data throughput, and resource utilization, all of which impact real-time responsiveness and energy efficiency [26]. Replicating real-world scenarios to evaluate IoT systems continues to be difficult owing to the intricacy of dynamic environments and variability in available datasets, which impedes large-scale, standardized testing [27]. In the meantime, cybersecurity measures are also developing, with methods like Zero Trust Architecture (ZTA) and Secure by Design focusing on proactive security integration into the software development process, lowering long-term expenses and enhancing resilience in both public and private IT infrastructures [28].

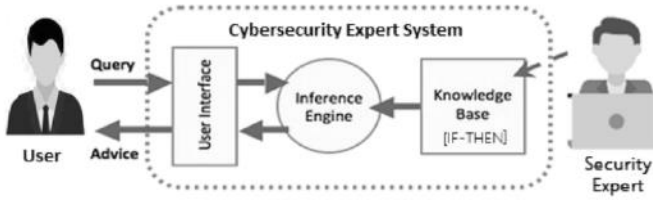


Fig. 5 Model of Cybersecurity [29].

The swift growth of the Internet of Things (IoT) market to $330.6 billion and expected to expand up to $875.0 billion by 2025 has increased worries about the safety of connected devices, especially since they become deeply entrenched in individual and business settings [30]. High-profile hacks like the Mirai botnet have taken advantage of security holes in IoT devices to carry out massive Distributed Denial-of-Service (DDoS) attacks, leading manufacturers to pay closer attention to building security into their products. Testing how well such measures work entails measuring the harm reduction achieved when security measures are implemented, either based on incident reports, cost of damages, or the severity of the vulnerabilities that are addressed. A measurable reduction in such harm is a measure of the success of measures that have been implemented, and therefore outcome-based evaluation is essential in informing future security advancements in the IoT industry.

### A. Objectives

- Develop a hybrid deep learning model to detect cybersecurity threats in IoT networks with high accuracy and low false positives.
- Integrate Convolutional Neural Networks (HCNN) and Calibrated Random Forest (RF) classifiers for precise classification of network traffic.
- Optimize feature selection using the Enhanced Harris Hawks Optimization Algorithm (EHOA) to improve model efficiency and performance.
- Minimize the impact of class imbalance through techniques like class weighting during model training.

## II. LITERATURE REVIEW

**Akshaya, V., et al. (2023) [31]** explained the exponential increases in smart devices and reduced costs of sensors have increased applications using IoT (Internet of Things). There has been an extensive analysis on the Internet traffic detection and classification in the past decade, however this is still a trending subject with respect to IoT. The objective of this work is to enhance attack detection rates in a timely fashion. The security and accuracy of attack detection rates an IDS (Intrusion Detection System) that uses HCNN (Hybrid Convolutional Neural Networks) for identifying IoT attacks in a city. After completion of pre-processing stages, FS (Feature Selection) using EHOA (Entropy-Hummingbird Optimization Algorithm) is used. Subsequently, classifications that use optimizations are carried out for IoT attack detections and classification results evaluated. KH-AES (Krill Herd-Advanced Encryption Standard) algorithm in data exchanges for security. The NSL-KDD dataset is utilised in this research to implement IDS. The data was classified based on six types of attacks: U2R, DoS, R2L, Probing, normal, and unknown. The weights in HCNN layers have significant impacts on classification outcomes. The proposed scheme is compared with popular approaches in terms of FS, classifications and security of data shares where it was found that proposed approach yields commendable outcomes.

**Liang Zhou et al. (2025) [32]** examined, the rapid development of smart cities and the integration of IoT devices have significantly increased security vulnerabilities, especially within consumer electronics, exposing them to complex cyber-attacks. Develop a robust security model to enhance threat detection and protection of these devices in smart city environments. They proposed a novel approach utilizing the Harris Hawks Optimizer (HHO) for feature selection and the Mountain Gazelle Optimizer (MGO) for hyperparameter tuning within an XGBoost-based framework for network traffic analysis. The dual optimization technique is designed to balance computational efficiency with high accuracy, ensuring scalability across diverse smart city applications. Experimental evaluations on a labeled dataset indicate that our model outperforms conventional machine learning approaches, achieving 91.13% accuracy, 95.48% precision, and 91.13% recall, thereby reducing false positives while

maintaining high detection rates. The potential of their model was an effective and scalable solution for enhancing cybersecurity in interconnected urban systems, paving the way for further exploration of hybrid optimization strategies and broader datasets to support real-time smart city applications.

**Kavitha Ramaswami Jothi et al. (2024) [33]** explained, living circumstances and construction techniques have generally improved, occupants of these spaces frequently feel unsatisfied with the sense of security they provide, which leads to looking for and eventually enacting ever-more-effective safety precautions. The continuous uncertainty that contemporary individuals experience, particularly regarding their protection in places like cities, prompted the field of computing to design smart devices that attempt to reduce threats and ultimately strengthen people's sense of protection. Intelligent apps were developed to provide protection and make a residence a smart and safe home. The proliferation of technology for smart homes necessitated the implementation of rigorous safety precautions to protect users' personal information and avoid illegal access. The importance of establishing cyber security has been recognized by academic and business institutions all around the globe. Providing reliable computation for the Internet of Things (IoT) is also crucial. A new method for enhancing safety in smart home environments' sustainability using IoT devices is presented in this paper, combining the Whale Optimization Algorithm (WOA) with Deep Convolutional Neural Networks (DCNNs). WOA-DCNN hybridization seeks to enhance safety measures by efficiently identifying and averting possible attacks in real time. They showed how effective the proposed approach is in defending smart home systems from a range of safety risks via in-depth testing and analysis. By providing a potential path for protecting smart home surroundings in a world that is growing more linked, this research advances the state of the art in IoT security.

**Wangjun Zhangtate et al. (2024) [34]** expressed, the Internet of Things technology is widely used in all aspects of power. A deep analysis method proposed for the message data of power Internet of Things terminal. The message data of power Internet of Things terminal is collected without disturbance through data mirroring, the hierarchical relationship of protocol tree is constructed, and the collected message data of power Internet of Things terminal is analyzed layer by layer according to the hierarchical relationship of protocol tree. Protocol reverse engineering is used to process the analyzed data, obtain the communication protocol of the electric IoT terminal, and extract the meaning of the operation instruction generated in the communication process. The meaning of the operation instruction included the behavioral meaning of the device instruction and payload data. At the same time, the model takes into account the undisturbed acquisition, real-time analysis and deep analysis of message parsing, effectively, the global IoT management, and has portability, which can realize the scalability, and consistency of the capacity expansion of electric IoT terminal equipment, provides strong technical support for the automatic registration of electric IoT terminal equipment and the rapid online service, and improves the work efficiency of electric IoT terminal equipment.

**Amjed A. Ahmed et al. (2024) [35]** explained, during the years 2018-2024, considerable advancements have been achieved in the use of deep learning for side channel attacks. The security of cryptographic algorithm implementations is put at risk by this. The aim was to conceptually keep an eye out for specific types of information loss, like power usage, on a chip that is doing encryption. Next, one trains a model to identify the encryption key by using expertise of the underpinning encryption algorithm. The encryption key is then recovered by applying the model to traces that were obtained from a victim chip. Deep learning has been used in many different fields in the past several years. Convolutional neural networks and recurrent neural networks, for instance, have demonstrated efficacy in text generation and object detection in images, respectively. They presented a review on deep learning models for encryption techniques against side channel attacks with a comparison table. Also, we have detailed the necessity of hybrid deep learning models for enhancing encryption techniques against these side channel attacks.

**Tinshu Sasi et al. (2024) [36]** The Internet of Things (IoT) has set the way for the continuing digitalization of society in various manners during the past decade. IoT is a vast network of intelligent devices exchanging data online. The security component of IoT is crucial given its rapid expansion as a new technology paradigm since it may entail safety-critical procedures and the online storage of sensitive data. Unfortunately, security is the primary challenge when adopting Internet of Things (IoT) technologies. As a result, manufacturers' and academics' top priority now is improving the security of IoT devices. A substantial body of literature on the subject encompasses several issues and potential remedies. However, most existing research fails to offer a comprehensive perspective on attacks inside the IoT. Hence, this survey aims to establish a structure to guide researchers by categorizing attacks in the taxonomy according to various factors such as attack domains, attack threat type, attack executions, software surfaces, IoT protocols, attacks based on device property, attacks based on adversary location and attacks based on information damage level. This is followed by a comprehensive analysis of the countermeasures offered in academic literature. In this discourse, the countermeasures proposed for the most significant security attacks in the IoT are investigated. Following this, a comprehensive classification system for the various domains of security research in the IoT and Industrial Internet of Things (IIoT) is developed, accompanied by their respective remedies. In conclusion, the study has revealed several open research areas pertinent to the subject matter.

**M. Arul Selvan (2024) [37]** expressed, the ever-evolving landscape of cyber threats necessitates robust and adaptable intrusion detection systems (IDS) capable of identifying both known and emerging attacks. Traditional IDS models often struggle with detecting novel threats, leading to significant security vulnerabilities. This paper

proposes an optimized intrusion detection model using Support Vector Machine (SVM) algorithms tailored to detect known and innovative cyberattacks with high accuracy and efficiency. The model integrates feature selection and dimensionality reduction techniques to enhance detection performance while reducing computational overhead. By leveraging advanced optimization techniques such as Grid Search and Particle Swarm Optimization (PSO), the proposed SVM-based IDS achieves superior classification results.

**Chinnappa Annamalai et al. (2023) [38]** investigated the Internet of Things (IoT) is a kind of advanced information technology that has grabbed the attention of society. Stimulators and sensors were generally known as smart devices in this ecosystem. In parallel, IoT security provides new challenges. Internet connection and the possibility of communication with smart gadgets cause gadgets to indulge in human life. Thus, safety is essential in devising IoT. IoT contains three notable features: intelligent processing, overall perception, and reliable transmission. Due to the IoT span, the security of transmitting data becomes a crucial factor for system security. Designed a slime mold optimization with ElGamal Encryption with a Hybrid Deep-Learning-Based Classification (SMOEGE-HDL) model in an IoT environment. The proposed SMOEGE-HDL model mainly encompasses two major processes, namely data encryption and data classification. At the initial stage, the SMOEGE technique is applied to encrypt the data in an IoT environment. For optimal key generation in the EGE technique, the SMO algorithm has been utilized. Next, in the later stage, the HDL model is utilized to carry out the classification process. To boost the classification performance of the HDL model, the Nadam optimizer was utilized. The experimental validation of the SMOEGE-HDL approach is performed, and the outcomes are inspected under distinct aspects. The proposed approach offers the following scores: 98.50% for specificity, 98.75% for precision, 98.30% for recall, 98.50% for accuracy, and 98.25% for F1-score. This comparative demonstrated the enhanced performance of the SMOEGE-HDL technique compared to existing techniques.

**Yasmeen Alslman et al. (2022) [39]** examined**,** medical image encryption has gained special attention due to the nature and sensitivity of medical data and the lack of effective image encryption using innovative encryption techniques. Several encryption schemes have been recommended and developed to improve medical image encryption. Most of these studies rely on conventional encryption techniques. However, such improvements have come with increased computational complexity and slower processing for encryption and decryption processes. Alternatively, the engagement of intelligent models such as deep learning along with encryption schemes exhibited more effective outcomes, especially when used with digital images. This paper aims to reduce and change the transferred data between interested parties and overcome the problem of building negative conclusions from encrypted medical images. To do so, the target was to transfer from the domain of encrypting an image to encrypting features of an image, which are extracted as float number values. Therefore, we propose a deep learning-based image encryption scheme using the autoencoder (AE) technique and the advanced encryption standard (AES). Specifically, the proposed encryption scheme is supposed to encrypt the digest of the medical image prepared by the encoder from the autoencoder model on the encryption side. On the decryption side, the analogous decoder from the auto-decoder is used after decrypting the carried data. The autoencoder was used to enhance the quality of corrupted medical images with different types of noise. In addition, we investigated the scores of structure similarity (SSIM) and mean square error (MSE) for the proposed model by applying four different types of noise: salt and pepper, speckle, Poisson, and Gaussian. It has been noticed that for all types of noise added, the decoder reduced this noise in the resulting images. Finally, the performance evaluation demonstrated that our proposed system improved the encryption/decryption overhead by 50–75% over other existing models.

Table 1 Comparative studies of IoT Security Models

| Author(s) & Year | Model | Application Domain | Techniques Used | Performance Results | Encryption Focus | AI/ML Integration | Strengths | Limitations |
|---|---|---|---|---|---|---|---|---|
| Akshaya, V., et al. (2023) [31] | HCNN + EHOA + KH-AES | IoT Attack Detection in Smart Cities | Hybrid CNN, Entropy-Hummingbird Optimization for Feature Selection, KH-AES for secure data exchange | Improved attack detection accuracy across six attack types (NSL-KDD dataset) | Yes (KH-AES used for secure data exchange) | Hybrid CNN with optimized feature selection (EHOA) | High accuracy in multi-class attack detection; secure data sharing via KH-AES | Requires further validation across real-time or diverse IoT datasets |
| Liang Zhou et al. (2025) [32] | HHO-MGO with XGBoost | Smart Cities | HHO for feature selection, MGO for hyperparameter tuning | 91.13% Accuracy, 95.48% Precision | Yes (Network traffic analysis) | XGBoost with metaheuristic tuning | High detection accuracy with efficient optimization | Needs broader dataset validation |
| Kavitha Ramaswami Jothi et al. (2024) [33] | WOA-DCNN Hybrid | Smart Homes | Whale Optimization, Deep CNN | Real-time attack detection demonstrated | Yes (Smart home data security) | DCNN with Whale Optimization | Real-time detection and lightweight for IoT | Potential overfitting in home-specific contexts |
| Wangjun Zhangtate et al. (2024) [34] | Protocol Reverse Engineering for Power IoT | Power IoT | Data mirroring, protocol tree parsing | Real-time analysis, high scalability | Partial (Protocol security) | Protocol analysis, no ML | Non-intrusive, scalable protocol analysis | Limited to power IoT domain |
| Amjed A. Ahmed et al. (2024) [35] | DL Models for Side Channel Attacks | Encryption Vulnerabilities | CNNs, RNNs for encryption key recovery | Comparative review of DL models | Yes (Cryptographic side-channel attacks) | Deep Learning (CNN, RNN) | Detailed insight into DL vulnerability | Focused on attack modeling, not prevention |
| Tinshu Sasi et al. (2024) [36] | IoT Attack Taxonomy and Survey | General IoT Security | Survey-based Taxonomy | Comprehensive classification system | No (Focus on classification of attacks) | No direct ML model | Comprehensive overview of attack types | No experimental validation provided |
| M. Arul Selvan (2024) [37] | Optimized SVM with Grid Search & PSO | Intrusion Detection | SVM, Grid Search, PSO | High detection accuracy & efficiency | No (Focus on intrusion detection) | SVM with optimization techniques | Effective classification with low overhead | Depends heavily on feature selection quality |
| Chinnappa Annamalai et al. | SMOEGE-HDL Model | IoT Data Encryption | Slime Mold Optimization, ElGamal, Hybrid DL | 98.5% Accuracy, 98.75% Precision | Yes (IoT data encryption with ElGamal) | Hybrid Deep Learning with Nadam | High precision and multi-layered security | High complexity in integratio |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| (2023) [38] | | | | | | | | n and training |
| Yasmeen Alslman et al. (2022) [39] | AE + AES for Medical Image Encryption | Medical Image Security | Autoencoder, AES, SSIM/MSE analysis | 50–75% reduction in overhead, improved SSIM/MSE | Yes (Medical image feature encryption) | Autoencoder-based DL integration | Efficient encryption with reduced processing load | Specific to medical imaging domain |

## III. METHODOLOGY

This study aims for the identification of cybersecurity attacks in IoT systems using a deep learning-optimization hybrid methodology. The system is designed to scan network traffic and detect unusual patterns that signal potential cyberattacks. The model accomplishes high recall and precision in labelling network traffic as malicious or benign through the integration of Hybrid Convolutional Neural Networks (HCNN), Random Forest classifiers, and optimized feature selection techniques. This unification provides real-time threat detection with reduced false positives, providing a scalable and proactive solution that is well-suited for protecting various IoT applications. This study strengthens IoT security by identifying cyber threats via a hybrid model that integrates HCNN, Random Forest, and enhanced feature selection. It examines network traffic to discover anomalies in real-time with high accuracy and low false positives to guarantee efficient and scalable threat detection.

### A. Implementation tool

Python was utilized for the study because of its extensive library ecosystem, which can be used for optimization, machine learning, and data science. Core libraries such as Pandas and NumPy were utilized for handling data efficiently—Pandas handled data cleaning and categorical encoding, whereas NumPy enabled fast numerical operation and transformation that were vital for training models. Scikit-learn was utilized to play a central part in preprocessing (label encoding and normalization), clustering via K-Means to enhance feature clarity, and model performance evaluation using measures such as accuracy and F1-score. In deep learning, TensorFlow/Keras was employed in developing the Hybrid Convolutional Neural Network (HCNN), taking advantage of Keras's ease of constructing layers, utilization of regularization strategies, and hyperparameter tuning.

Security was incorporated with PyCryptodome, which utilized the Krill Herd-Optimized AES (KH-AES) algorithm to secure IoT data in transit. SciPy's ARFF module facilitated loading and processing of KDDTrain+ and KDDTest+ datasets within Python itself. A modified Enhanced Harris Hawks Optimization Algorithm (EHOA) was also utilized for feature selection, enhancing the accuracy of the model by eliminating irrelevant features and improving intrusion detection performance. This dual framework provided both powerful analytical potential and effective cybersecurity integration within the IoT ecosystem.

### B. Model Evaluation

The performance of the hybrid HCNN + Transformer model was tested with various key metrics and tools. A confusion matrix gave a detailed overview of true positives, true negatives, false positives, and false negatives and how well the model differentiated normal from anomalous traffic. The classification report gave an overview of important metrics—precision, recall, F1-score, and accuracy—for both classes, assisting in measuring the effectiveness of the model as a classifier. Particularly, accuracy maintained a low false positive ratio by counting correctly classified attacks among all forecast ones, recall minimized false negatives by detecting true attacks, and the F1-score weighted both to assess comprehensively. Matplotlib was also utilized for the visual observation of performance trends, i.e., training loss and accuracy graphs across epochs, and for offering meaningful insight into learning patterns of the model and possible spots for improvement.

### C. Dataset Source and Computing Environment

The dataset for this study was obtained from Kaggle and represented IoT network traffic used to determine typical and unusual behaviour. Pre-processing was an important step in readying the data for training and testing of models. Class weighting methods were used during training to avoid bias toward the majority class to solve the problem of class imbalance. Categorical variables like protocol types and services were encoded into numerical representations via label encoding, while normalization through MinMaxScaler provided equal feature scaling for quicker convergence and better model precision. Google Colab, a cloud computing Python environment, hosted the project with seamless integration of needed libraries, datasets, and GPU. Colab's capability of GPU acceleration greatly improved the training time of advanced models such as HCNN and Random Forest, and its interactive nature allowed real-time visualization, debugging, and collaborative work.

### D. Model Combination

This study introduced a hybrid architecture that combined HCNN (Hybrid Convolutional Neural Network) and Calibrated Random Forest Classifier to achieve improved anomaly detection in IoT networks. HCNN successfully extracted spatial and temporal attributes from network traffic, and Random Forest, learned from features which were selected via the Enhanced Harris Hawks Optimization Algorithm (EHOA), used strong classification and calibrated probability estimations through CalibratedClassifierCV.

This combination methodology combined predictions of both models, balancing deep feature extraction with structured decision-making to enhance detection accuracy and scalability. The prior research has also employed machine learning techniques like CNNs, coupled with optimization algorithms like EHOA and K-Means clustering, to enrich feature selection and pre-processing of data. Major metrics for measurement—precision, recall, and F1-score—were accompanied by hyperparameter tuning and cross-validation to perform reliable and steady threat detection at the expense of few false negatives and false positives.

**E. Proposed Model**

In this study, innovative hybrid machine learning methods and optimization techniques were utilized to improve the detection of malicious behaviour in IoT networks. The foundation of the approach was a Hybrid Model based on Hierarchical Convolutional Neural Networks (HCNN) and a Calibrated Random Forest (RF) classifier that exploited the capabilities of both deep learning and conventional ensemble approaches. The HCNN module picked up spatial patterns in network traffic, while Random Forest classifier with multiple decision trees offered strong, structured classification. Feature selection used the Enhanced Harris Hawks Optimization Algorithm (EHOA) so that the model could concentrate on the most descriptive attributes by eliminating redundant or meaningless features based on entropy-based ranking. This optimization lowered the data dimensionality, reduced computational overhead, and improved model convergence. The process flow comprised four phases: data pre-processing, feature optimization and selection, model training and hybridization, and evaluation. Data preprocessing comprised the treatment of categorical variables, normalization of numerical values, and application of K-Means clustering (KMC) to cluster similar patterns, remove noise, and provide structural depth to the feature set. The last model was tested on the basis of important performance indicators like accuracy, precision, recall, and F1-score and proved effective in detecting abnormal network activity in real time.

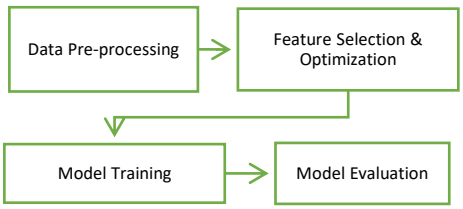


Fig 6 Flow Chart of Methodology

The dataset used in the present study was the NSL-KDD, a well-known benchmark dataset for intrusion detection, obtained from Kaggle. Exactly, the KDDTrain+.arff and KDDTest+.arff datasets were utilized for training and testing. At the preprocessing stage, categorical features were converted into numerical form using label encoding, and MinMaxScaler was used for numerical values normalization to improve model efficiency. The application of K-Means clustering assisted in revealing hidden structure in the data, and cluster labels produced by it were added as additional features, increasing the model's capacity to distinguish between attack and normal traffic. Feature selection using EHOA again cleaned up the dataset, discovering important predictors for successful classification. The preprocessed data was then restructured to satisfy the input needs of both the HCNN and Random Forest models, resulting in interoperability and seamless integration into the hybrid framework. Not only did this well-structured and systematic process enhance model training effectiveness but also enhanced classification performance, producing an efficient and precise solution for real-time IoT intrusion detection.

**F. Hybrid Model**

This study provides a hybrid intrusion detection approach for IoT networks that integrates Hierarchical Convolutional Neural Networks (HCNN) with a Calibrated Random Forest (RF) classifier to improve detection accuracy and performance. HCNN learns the spatial and temporal patterns from network traffic, whereas RF provides organized decision-making through 300 decision trees and calibrated probabilities for accurate classification. For optimal performance, the Enhanced Harris Hawks Optimization Algorithm (EHOA) is employed for feature selection, dimensionality reduction, and concentration of the most important data. Label encoding, normalization, and K-Means Clustering (KMC) are preprocessing steps adopted for enhanced structuring of data. Binary cross-entropy loss and Adam optimizer are utilized to train the model with binary class weights to counteract data imbalance. It is assessed with accuracy, precision, recall, and F1-score, and plotted with confusion matrices and ROC curves. The combination of deep learning, ensemble methods, and optimization provides a powerful, real-time solution for identifying malicious activity in IoT settings.

**G. Evaluation Metrics**

Accuracy is a standard metric that measures the proportion of correctly predicted instances (both positive and negative) out of the total instances. It is useful for providing a general idea of the model's performance. However, in the context of an imbalanced dataset, accuracy alone may not be a sufficient measure, as it can be misleading when the majority class dominates.

$$Accuracy = \frac{True\ positive + True\ Negetive}{TotalNumber\ of\ Instance}$$

In this research, accuracy provides a baseline understanding of the overall correctness of the predictions, but additional metrics were required to account for the class imbalance in the money laundering dataset.

Precision measures the proportion of correctly predicted intrusions (positive cases) out of all cases that the model classified as intrusions. In intrusion detection systems (IDS) for IoT environments, high precision is crucial because it reduces false positives, ensuring that normal network traffic is not mistakenly flagged as an attack.

This is particularly important in cybersecurity applications, as excessive false positives can lead to unnecessary security alerts, wasted computational resources, and increased operational costs. By maintaining a high precision score, the model ensures that security teams can focus their efforts on actual threats, improving the overall efficiency and reliability of the intrusion detection system.

$$Precision = \frac{True\ positive}{True\ Positive + False\ Positives}$$

A high precision value indicates that when the model predicts fraud, it is likely correct. This is crucial for ensuring that false alarms (false positives) are minimized.

Recall, or sensitivity, measures the model's ability to correctly identify actual intrusions (positive cases). In other words, it evaluates how many real cyber-attacks or anomalies are successfully detected by the model. High recall is crucial in intrusion detection systems (IDS) for IoT environments because it minimizes false negatives, ensuring that actual security threats are not overlooked. If recall is low, some malicious activities may go undetected, potentially leading to security breaches, unauthorized access, or network disruptions. By prioritizing high recall, the model enhances cyber defense mechanisms, ensuring that intrusions are detected and mitigated in real-time to safeguard IoT networks from evolving threats.

$$\text{Recall} = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

In intrusion detection systems (IDS) for IoT security, high recall is critical because missing an actual intrusion (a false negative) can have severe consequences, such as leaving networks vulnerable to cyber-attacks, unauthorized access, or data breaches. If an attack goes undetected, it can lead to system compromise, data theft, or even large-scale disruptions in IoT networks. Ensuring high recall allows the model to capture and mitigate potential security threats in real-time, preventing malicious actors from exploiting network vulnerabilities. This is particularly important in critical infrastructure and IoT security, where undetected intrusions can lead to severe financial, operational, and privacy risks.

## IV. RESULTS AND DISCUSSION

This section discussed the performance of a hybrid model consisting of a 1D Convolutional Neural Network with residual connections and a Calibrated Random Forest classifier in identifying money laundering. Employing a weighted ensemble approach optimized using grid search with ROC-AUC scores, the model is assessed using performance metrics such as accuracy, precision, recall, F1-score, and ROC curves. Threshold tuning through the precision-recall curve optimizes the F1-score, whereas methods like class balancing, early stopping, and learning rate optimization enhance stability and minimize false positives and negatives for reliable real-world performance.

### A. Hybrid Deep Learning Approach for Intrusion Detection with Secure Data Processing

This study provides a hybrid deep learning system for network intrusion detection that incorporates K-Means Clustering (KMC) for preprocessing, Enhanced Harris Hawks Optimization Algorithm (EHOA) for feature extraction, and Hybrid Convolutional Neural Network (HCNN) for classification, alongside KH-AES encryption for safe data management. Preprocessing consists of loading network traffic data from KDDTrain+ and KDDTest+ ARFF files, label encoding of categorical features, and Min-Max Scaling of numerical attributes. KMC is employed to manage missing values and eliminate noise by clustering data and smoothing per cluster. EHOA subsequently chooses the most important features based on an entropy-fitness score, simplifying complexity and enhancing performance. The HCNN, which was trained for more than 20 epochs, consists of Conv1D layers with ReLU activation, MaxPooling, Dropout, and Dense layers and has a test accuracy of 73.51%, precision of 63.82%, recall of 88.91%, and F1-score of 74.31%, indicating balanced detection of intrusions with low false positives. For securing the data, KH-AES encryption (AES-128) is employed, which transforms raw traffic into encrypted hexadecimal form, thereby providing confidentiality and data integrity.

Table 2 HCNN performance metrics

| Metric | Score |
|---|---|
| Accuracy | 0.7351 |
| Precision | 0.6382 |
| Recall | 0.8891 |
| F1-Score | 0.7431 |

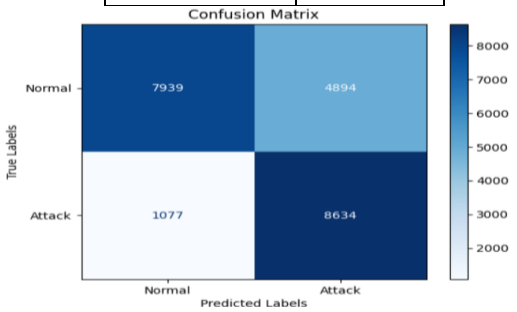


Fig. 7 Confusion Matrix of the previous study

The confusion matrix indicates the model accurately classified 8,634 attacks and 7,939 normal cases but also created 4,894 false positives and 1,077 false negatives. This demonstrates its good attack detection feature but suggests there is a need to minimize false alarms to limit unnecessary alerts.

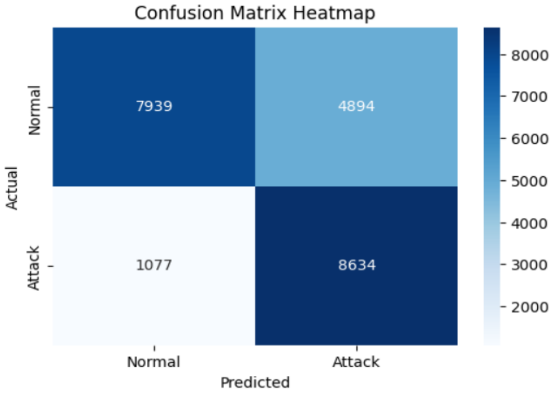


Fig. 8 Confusion Matrix Heatmap

The heatmap of confusion matrix shows that the model accurately classified 7,939 instances of normal cases and 8,634 instances of attacks. It also classified 4,894 instances of normal traffic as attacks and 1,077 instances of attacks as normal. Although the high true positive value indicates robust detection of attacks, the significant rate of false positives suggests a necessity for further fine-tuning in order to suppress false alarms.

Table 3 Classification Report

| Class | | Precision | Recall | F1-Score | Support |
|---|---|---|---|---|---|
| Normal | | 0.880546 | 0.618639 | 0.726715 | 12,833 |
| Attack | | 0.638232 | 0.889095 | 0.743061 | 9,711 |
| Accuracy | | 0.735140 | 0.735140 | 0.735140 | 22,544 |
| Macro Avg | | 0.759389 | 0.753867 | 0.734888 | 22,544 |
| Weighted Avg | | 0.776167 | 0.735140 | 0.733756 | 22,544 |

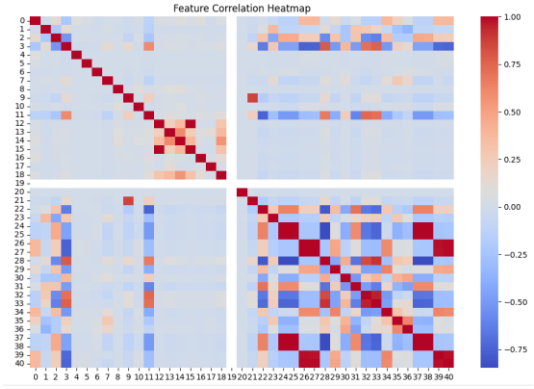


Fig. 9 Feature Correlation Heatmap

The Feature Correlation Heatmap visualizes the relationships between different features in the dataset. The colour scale ranges from red (strong positive correlation) to blue (strong negative correlation), with lighter shades indicating weaker correlations. Features with high positive or negative correlations provide insights into dependencies within the data, which can be used for feature selection or dimensionality reduction. This analysis helps identify redundant features and optimize the dataset for improved model performance. The model's performance in detecting frauds is measured by major metrics apart from accuracy with a focus on precision, recall, and F1-score considering class imbalance. Precision keeps false positives to a minimum by quantifying the accuracy of detected fraud cases, while recall measures the model's fraction of actually fraudulent cases detected, avoiding false negatives. The F1-score strikes a balance between the two for a more comprehensive assessment. Moreover, ROC-AUC and PR-AUC values are computed to measure the model's discriminatory power, particularly for imbalanced datasets. A confusion matrix also visually represents classification results, specifying true and false positives and negatives for further insight.

Table 4 Final Metrics

| Metric | Value |
|---|---|
| Optimal Weights (NN) | 0.1 |
| Optimal Weights (RF) | 0.9 |
| Optimal Threshold | 0.9255 |
| Accuracy | 0.8341 |
| Precision | 0.8529 |
| Recall | 0.743 |
| F1-Score | 0.7942 |
| ROC-AUC | 0.9137 |
| PR-AUC | 0.9089 |

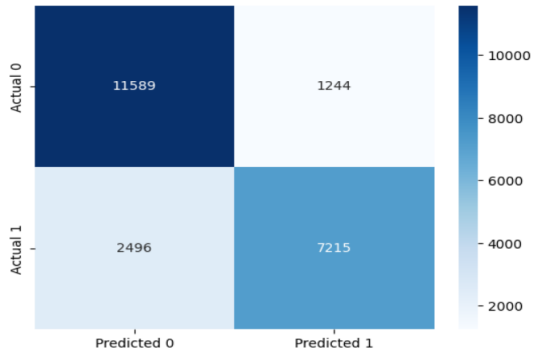


Fig. 10 Confusion Matrix

Figure 10 and Table 4 illustrate the excellent performance of the ensemble model, which involves Neural Network (NN) and Random Forest (RF), in identifying fraudulent cases. The confusion matrix indicates the model accurately identified 11,589 non-fraudulent cases and 7,215 fraud cases, generating 1,244 false positives and 2,496 false negatives. With the best weights of 0.1 (NN) and 0.9 (RF) and thresholding at 0.9255, the model attained an accuracy of 83.41%, precision of 85.29%, recall of 74.3%, and an F1-score of 79.42%, which testifies to a balanced performance. Healthy ROC-AUC (0.9137) and PR-AUC (0.9089) scores also attest to its performance in separating fraudulent and honest transactions, and thus it is a viable method of fraud detection in imbalanced data.

## V. CONCLUSION

This study effectively developed and tested a strong hybrid deep learning model for intrusion detection within IoT settings that integrated the potency of Hierarchical Convolutional Neural Networks (HCNN) and a Calibrated Random Forest (RF) classifier. The system proved powerful by correctly categorizing anomalous and normal network traffic using maximized feature extraction through the Enhanced Harris Hawks Optimization Algorithm (EHOA). Preprocessing by K-Means Clustering, label encoding, and Min-Max scaling helped make the model efficient and generalizable. The last ensemble model obtained 83.41% accuracy, 85.29% precision, 74.3% recall, and an F1-score of 79.42%, as well as ROC-AUC and PR-AUC values higher than 0.91, underlining its capability to differentiate between benign and malicious traffic even for datasets that are imbalanced. The employment of KH-AES encryption also ensured safe handling of the data, making the model not only accurate but also trustworthy and privacy-guaranteeing. These outcomes confirm the efficiency of the model in real-time anomaly detection and also its viability for use in contemporary IoT networks where security, scalability, and low false-positive rates are paramount.

**Conflict of Interest:** The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.



## References

[1] Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & Security*, *148*, 104097**.**

[2] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, *28*(2), 93.

[3] Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. *Blockchain: Research and Applications*, *5*(2), 100178.

[4] Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the trade-offs between wireless security and performance in IoT networks: A case study of web applications in AI-driven home appliances. *Available at SSRN 4927991*.

[5] Mangla, Monika & Ambarkar, Smita & Akhare, Rakhi & Deokar, Sanjivani & Mohanty, Sachi & Satpathy, Suneeta. (2022). A Proposed Framework to Achieve CIA in IoT Networks. 10.1007/978-981-16-8546-0_3.

[6] Almutairi, R., Bergami, G., & Morgan, G. (2024). Advancements and Challenges in IoT Simulators: A Comprehensive Review. *Sensors*, *24*(5), 1511.

[7] Meziane, Hind & Ouerdi, Noura. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. Scientific Reports. 13. 10.1038/s41598-023-46640-9.

[8] Nikfam, F. (2024). Security and Privacy in Artificial Intelligence.

[9] Eswari, B. R., & Saritha, V. (2025). Cyber Hacking Breaches Prediction Using Machine Learning Techniques. *GAMANAM: Global Advances in Multidisciplinary Applications in Next-Gen And Modern Technologies*, *1*(1), 23-31.

[10] Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics*, *12*, 1456491.

[11] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and

solutions. *Journal of Ambient Intelligence and Humanized Computing*, 1-18.

[12] BADI, S. A., Abdulla, A. A., AlAsad, M. A., Al-Qattan, A. A., & Elmedany, W. Enhancing the Lightweight Encryption Algorithm for Secure and Efficient Iot Applications: Addressing Vulnerabilities and Optimizing Performance. *Available at SSRN 5097645*.

[13] Khan, B., & Hashmi, A. (2025). Comparing Crypto and Digital Cash Systems: A Cryptographic Analysis. *Authorea Preprints*.

[14] İnce, K., İnce, C., & Hanbay, D. (2025). Random Strip Peeling: A novel lightweight image encryption for IoT devices based on colour planes permutation. *CAAI Transactions on Intelligence Technology*.

[15] Devendiran, R., & Turukmane, A. V. (2024). Dugat-LSTM: Deep learning-based network intrusion detection system using chaotic optimization strategy. *Expert Systems with Applications*, *245*, 123027.

[16] Scientific, L. L. (2025). HYBRID DEEP LEARNING FRAMEWORK FOR INTRUSION DETECTION: INTEGRATING CNN, LSTM, AND ATTENTION MECHANISMS TO ENHANCE CYBERSECURITY. *Journal of Theoretical and Applied Information Technology*, *103*(1).

[17] Lakshmi, J. M., Krishna Prasad, K., & Viswanath, G. (2025). Proactive Security in Multi-Cloud Environments: A Blockchain Integrated Real-Time Anomaly Detection and Mitigation Framework. *Cuestiones de Fisioterapia*, *54*(2), 392-417.

[18] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., ... & Mohamed, Rai, H. M., Shukla, K. K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. *Heliyon*, *10*(19).

[19] Singh, J., Singh, A., Singh, H., & Doyon-Poulin, P. (2025). Implementation and evaluation of a smart machine monitoring system under industry 4.0 concept. *Journal of Industrial Information Integration*, *43*, 100746.

[20] Ahmed, Ejaz & Yaqoob, Ibrar & Gani, Abdullah & Imran, Muhammad & Guizani, Mohsen. (2016). Internet of Things based Smart Environments: State-of-the-art, Taxonomy, and Open Research Challenges. IEEE Wireless Communications. 23. 10.1109/MWC.2016.7721736.

[21] Sharma, H., Manhas, J., & Sharma, V. (2025). DLIIoT: A Deep Learning based Intelligent Attack Detection in IoT Networks using Cooja Simulator. *Journal of Scientific Research*, *17*(1), 177-193.

[22] Khanam, Shapla & Ahmedy, Ismail & Idris, Mohd & Jaward, Mohamed & Sabri, Aznul. (2020). A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3037359.

[23] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, *28*(2), 93.

[24] Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the trade-offs between wireless security and performance in IoT networks: A case study of web applications in AI-driven home appliances. *Available at SSRN 4927991*.

[25] Li, Q., Peng, Z. M., Feng, L., Liu, Z., Duan, C., Mo, W., & Zhou, B. (2024). Scenarionet: Open-source platform for large-scale traffic scenario simulation and modeling. *Advances in neural information processing systems*, *36*.

[26] MacDougall, A., Gellatly, W., & Kleinman, J. Advancing the Art of Cybersecurity Cost Estimating.

[27] Sarker, Iqbal & Furhad, Md & Nowrozy, Raza. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science. 2. 10.1007/s42979-021-00557-0.

[28] Pütz, P., Mitev, R., Miettinen, M., & Sadeghi, A. R. (2023, December). Unleashing iot security: Assessing the effectiveness of best practices in protecting against threats. In *Proceedings of the 39th Annual Computer Security Applications Conference* (pp. 190-204)

[29] Akshaya, V., Mandala, V., Anilkumar, C., VishnuRaja, P., & Aarthi, R. (2023). Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things. *Measurement: Sensors*, *30*, 100917.

[30] Zhou, L., Gaurav, A., Arya, V., Attar, R. W., Bansal, S., & Alhomoud, A. (2025). Smart City Electronics Security Using XGBoost with Metaheuristic Algorithms. *IEEE Consumer Electronics Magazine*.

[31] Jothi, K. R., & Vaithiyanathan, B. (2024). Developing a Hybrid Approach with Whale Optimization and Deep Convolutional Neural Networks for Enhancing Security in Smart Home Environments' Sustainability Through IoT Devices. *Sustainability*, *16*(24), 11040.

[32] Zhang, W., Lu, S., Chen, Y., Wu, J., Pan, C., He, X., ... & Zhu, Y. (2024, March). Power IOT Terminal Message Depth Analysis Model. In *2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 7, pp. 142-145). IEEE.

[33] Ahmed, A. A., Hasan, M. K., Aman, A. H., Safie, N., Islam, S., Ahmed, F. R. A., ... & Rzayeva, L. (2024). Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks. *IEEE Access*.

[34] Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and intelligence*, *2*(6), 455-513.

[35] Selvan, M. A. (2024). SVM-Enhanced Intrusion Detection System for Effective Cyber Attack Identification and Mitigation.

[36] Annamalai, C., Vijayakumaran, C., Ponnusamy, V., & Kim, H. (2023). Optimal ElGamal Encryption with Hybrid Deep-Learning-Based Classification on Secure Internet of Things Environment. *Sensors*, *23*(12), 5596.

[37] Alslman, Y., Alnagi, E., Ahmad, A., AbuHour, Y., Younisse, R., & Abu Al-haija, Q. (2022). Hybrid encryption scheme for medical imaging using autoencoder and advanced encryption standard. *Electronics*, *11*(23), 3967.