Efficient Vulnerability Classification in IoT Networks: An Approach Using Convolutional Neural Networks and Tabu Search Optimization

Feras Fares AL-Mashagba[1]*, Mohammad Othman Nassar[2]*, Essam Said Hanandeh[3]*
Computer Science Department-Faculty of Information Technology, Jerash University, Jerash 26150, Jordan[1]
College of Computer Sciences and Informatics-Cyber Security Department, Amman Arab University, Amman 11953, Jordan[2]
Cyber Security Department-Faculty of Information Technology, Jerash University, Jerash 26150, Jordan[3]

***Abstract*—In this study, researchers propose a novel solution for efficient enhancement of vulnerability detection in several IoT environments. Efficient Vulnerability Classification has been introduced as the presented technique in IoT Networks (EVCIN). The method, EVCIN, which is a proposed approach, utilizes CNNs with Tabu Search Optimization. Customized CNN models have proven to be extremely accurate in identifying vulnerabilities for IoT classes, showing half (6 layers), Sefunten 99.03% (7 layers), and 95.71% (8 Layers). The contribution of using Tabu Search did increase the accuracy of classification through introducing an effective set of techniques that head towards the optimal solutions. Throughout the study, the superior performance of EVCIN was demonstrated in characterizing vulnerabilities when it was compared against single CNN and Tabu Search models and state-of-the-art methods. Data visualization and AUC analyses were also effective for understanding the performance and discrimination ability of models. There are numerous important implications from the study of EVCIN for enhancing cybersecurity in IoT and also adding vitality to the development of vulnerability classification in IoT networks. The above approach gives a potentially useful solution in a reliable and efficient way for vulnerability finding. This would then enhance security and flexibility in IoT-based networks.**

***Keywords*—Vulnerability categorization; IoT; networks; convolutional neural networks; tabu search optimization; cyber security I**

I. Introduction

The first essential tool that the IoT is becoming is dubbed the transformative technology paradigm, which can interconnect billions of different smart devices and things amongst each other [78, 23]. People, places, and things of interest in the context of the Internet of Things (IoT) range from wearable home appliances and devices to industry sensors and infrastructure control components [81]. The explosion of the number of its devices has made it possible for the emergence of a globally interconnected and intelligent environment which offers an unprecedented level of convenience, experience, and efficiency in different fields [49]. A current risk in IoT networks is to analyze the increasing number of, connected devices that have a great difficulty in facing security challenges. Instead of taking a lead, role in ensuring security and dependability of VANETs, detection and avoidance of vulnerabilities is highly important meaning [20].

Considering the IoT networks by vulnerabilities, we mean weaknesses or shortcomings in the design and deployment of the IoT devices, protocols, or systems that can be exploited by a malicious party to gain unauthorized access, modify data, disrupt operations, or compromise security in general [54; 9; 84; 50; 73; 21]. These, vulnerabilities pose an enormous threat to the security, privacy, and availability of services as well as data in the Internet of Things (IoT) environment [57].

Those with conventional security frequently need to be modified in order to address the unique challenges that Internet of Things (IoT) devices bring, but it is successful at protecting traditional, computer networks [74,1]. If IoT devices are considered traditional computers, they come with a natural limitation of processing power, memory space, and energy [12]. Therefore, these devices can neither efficiently handle the computational overhead involved with running security protocols that require a high price nor can they overcome difficulties in enforcing traditional security means [13, 66].

Apart from that, IoT networks contain a variety of devices provided by different manufacturers, all of which operate with their own communication protocols and standards [40]. Heterogeneity is a barrier to achieving seamless and secure communication for different devices [79]. Besides, certain of the previous generation Internet of Things devices do not possess security capabilities embedded within them or periodic update support, and are therefore increasingly exposed to the risk of security holes [86].

Moreover, a lot of the Internet of Things (IoT) devices are built with a focus on functionality and cost, and often do not take care of secure communication protocol integration [52]. Additionally, they now have no security-by-design, making them more vulnerable to attack as identification, weak encryption, and access control mechanisms are not part of current implementations [28].

Hence, the existing security solutions, including firewalls and intrusion detection systems, are not suited for IoT environments [72, 37, and 30]. If there is insufficient understanding of the specific IoT functionalities and communication protocols, this can also lead to misclassification of security threats and give rise to false positives or the loss of detection capability [47].

*Corresponding author.

These vulnerabilities can be best addressed through novel and targeted prevention mechanisms that cater to the particular properties of IoT networks [67, 4, 41]. These solutions need to take into account the constraints of device resources, support heterogeneous communication protocols, and integrate adaptive security functions able to cope with threats that are constantly evolving [39].

The remainder of this study is organized as follows: Section II reviews related work. Section III presents the proposed methodology, including the dataset and model. Section IV discusses results and evaluation. Section V provides discussion and implications. Section VI concludes the study and suggests future work.

Deep learning and AI methodologies have also gained popularity for IoT security enhancements in terms of real-time threat detection and classification capabilities [2, 70]. In particular, Convolutional Neural Networks (CNNs) have achieved state-of-the-art performance in different fields, being particularly successful in computer vision [16, 29, 36]. Although they are still in their nascent stage, CNNs may also be exploited to check on traffic behavior and detect unusual or malignant traffic if it is behaving automatically without the application of the predefined set of rules when surveyed from IoT networks [71].

In addition, efficient classification algorithms are also needed to achieve reasonable allocation of resources and real-time performance in the limited IoT networks [8, 26]. Tabu Search Optimization (TSO) is effective for structured search of the solution space, beneficial in finding the best configuration of classifiers [22]. Combining TSO with CNNs contributes to better parameter fitting in vulnerability detection, which leads to better accuracy and efficiency.

The researchers propose in this study a novel ResNet-50-based Convolutional Neural Network (CNN) adapted for vulnerability classification in Internet of Things (IoT) networks and employ the Tabu Search Optimization technique to improve detection performance. Moreover, an extensive comparative analysis is carried out to analyze the performance of our proposed CNN Tabu Search method compared with different state-of-the-art vulnerability categorization methods for the Internet of Things (IoT). The contributions of this study are twofold: firstly, it presents an optimized CNN architecture for IoT vulnerability classification, and secondly, we show that using Tabu Search as a metaheuristic optimization method could lead to better accuracy and efficiency in the detection. In addition, the study yields useful information on how the proposed method compares to state-of-the-art techniques.

II. Related Work

This section reviews the current studies of applying machine learning and deep, learning in various applications. Of these studies, Naeem et al. [51] contribute to network security by proposing a deep learning simplified, approach to detect malware on Internet of Things (IoT) systems. Their model provides high classification accuracy for both binary and multiclass prediction while reducing the threat of increasing malware in IoT networks. The combination of CNN and transfer learning allows for improving malware detection and classification accuracy to make the IoT systems more secure.

The study by Farid et al. [27] studies software defect prediction with the introduction of a hybrid model called CBIL. Experimental results demonstrate that the proposed model significantly outperforms conventional CNN/RNN models with higher F-measure and AUC. The combination of CNN and biLSTM Fastwalk is efficient enough to extract semantic features from source code, resulting in better defect prediction performance. As such, the model makes it easier to detect failures early on and requires, much less time and effort during software development.

In their research, Bu et al. [17] introduce an ensemble of deep convolutional networks for enhanced role classification in database security. The superiority of the Ensemble-LCS model over univariate predictor-based approaches is demonstrated for both higher robustness and accuracy. The ensemble can capture complex spatial correlations within the data by exploiting various architectures, including ResNet and Inception.

Several studies have focused on the security challenges of IoT systems. In a study, Zolanvari et al. [85] propose an approach to the enhancement of security in IIoT devices by using machine learning and big data analytics to minimize vulnerabilities effectively. In another approach, Saba et al. [69] present a two-stage fuzzy model hybridized using genetic algorithms, machine learning with emphasis on Support Vector Machines (SVMs), and ensemble-based classifiers to improve network security in IoT surroundings.

In the work of Marchisio et al. [48] analyze how Capsule Networks (CapsNets) react to adversarial examples and find out that there are differences in robustness w.r.t. standard CNNs. Meanwhile, Puthal et al. [65] concentrate on full end-to-end security in IoT networks and propose a user-centric secure strategy with Decision Trees. A real-time IoT test bed was used for verification of the proposed approach. The result confirms the improvements in network security.

In their study, Osman et al. [60] propose a novel model for VNA detection in IoT that offers a notable level of accuracy and real-world capability. In parallel, Best et al. [14] propose an anomaly detection method for IoT with adaptive learning that combines supervised and unsupervised machine learning techniques to obtain a robust framework, capable of accurately identifying various types of attacks.

As part of their study, Omara et al. [59] propose a novel multimodal biometric recognition scheme by combining LDM with kernel SVM. The technique presents good classification performance on face and ear images, which are useful in immigration, homeland security systems, and forensic applications based on uncontrolled databases of ear images. In summary, the literature review of these related works demonstrates a continuous and transformative evolution of IoT security in the form of various ML techniques to cope with complex problems and enhance robustness in IoT systems.

Metaheuristic optimization techniques have been increasingly adopted to improve the classification performance in security scenarios. Nassar and Al-Mashagba [87] developed a meta-knowledge-empowered ensemble learning model based

on metaheuristic optimization for sys call binder interaction classification, which highlights the significance of being optimized in both the process of feature extraction and model manipulation. Al Ghamri et al. [88] applied WOA to select the best features in malware datasets and thus obtain better classification results due to the low number of dimensions and smoother generalization. Ibrahim et al. [89] combined Harris Hawks Optimization and a color visual cryptography approach, demonstrating the flexibility of bio-inspired computing in security applications. Furthermore, Shannaq et al. [90] surveyed the recent metaheuristic applications for reducing text-based cyber harassment. Finally, Daoud et al. [91], for global numerical optimization, are similar in, principle to the hybrid CNN Tabu Search discussed here. Taken together, these works demonstrate that the synergy between deep learning and advanced optimization is increasing in a practical intelligent security solution, which also strengthens the practical value of the proposed integration for IoT vulnerability classification.

In conclusion, these studies showcase the usefulness of machine learning and deep learning in cybersecurity. However, studies on the integration of CNNs and TSO for vulnerability categorization in IoT have not been prevalent. To fill in the gap, this work develops a new method combining CNNs and TSO to systematically identify the IoT vulnerability for effectively securing the IoT-sensitive networks.

III. Methods and Materials

A. Data Description

In the current study, an "Edge-IIoT set" has been developed as a reality-based and comprehensive cybersecurity dataset that is targeted for IoT/IIoT applications. The consumer group is satisfied whether it is a centralized or decentralized machine learning-based IDPS.

The information consists of 7 layers each, representing a specific type of technology in an IoT or IIoT environment. There are several other kinds of technology embedded in the layers above. These domains are Cloud Computing, Network Functions Virtualization, Blockchain Networks, Fog Computing, Software-Defined Networking, and Edge Computing/Internet of Things and Industrial Internet of Things Perspective. The concepts of IOT and IIOT have materialized through the massiveness, adoption, and application of state-of-the-art technology in a range of applications. These technologies are, e.g., Things Boards, OPNFV, Hyperledger Sawtooth, Digital Twin, ONOS SDN controller, Mosquito MQTT brokers, and Modbus TCP/IP, to name a few. Data was collected from over ten different categories of IoT devices. Ultrasonic sensors, water level, sensors, pH meters, soil moisture detectors, heart rate monitors, and flame detectors are some of these devices. IoT communication protocols and their related devices are a direct target of fourteen different attacks, with the majority traced to those documented in this study. There are five major security risks involved in such attacks, including denial-of-service/distributed denial-of-service,(DDoS), information gathering, man-in-the-middle (MitM), injection, and malware. The qualitative research data have been collected and analyzed for the exploratory stage. This study explores what the data all has in it. Researchers have also experimentally compared the centralized and decentralized machine learning-based techniques for the identification and classification of vulnerabilities for these attacks. As [6].

The dataset contains 63 columns and 2,219,201 lines. Different columns are used to display various attributes, among them the time of the frame, its source and destination, IP addresses, ARP content, ICMP checksum, sequence numbers, HTTP parameters, DNS queries, TCP/UDP values, or even MQTT messages, Modbus/TCP frames, and many others. The columns "Attack label" and "Attack type" are ways to tag and categorize the nature of each performed attack. The Edge-IIoT set dataset serves to facilitate the development and testing of IDSs among other security solutions for IoT and IIoT networks. It allows a realistic coverage of cybersecurity events, which allows for testing the detection methods in an exact way. The distribution of attacks can be found in Fig. 1 and 2 according to quantity, category, and subcategory.

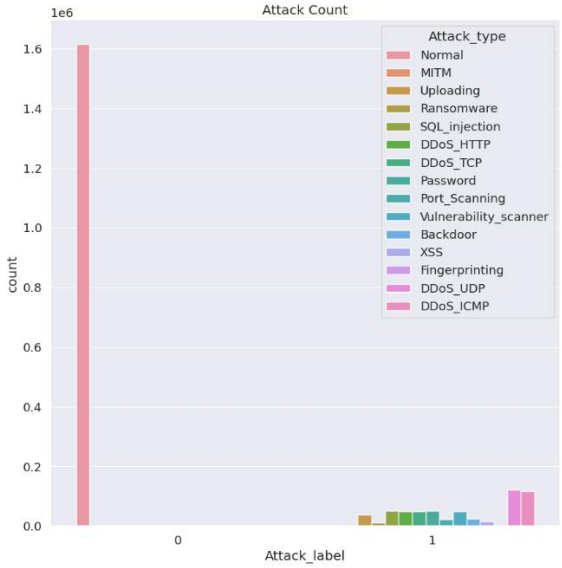

Fig. 1. Illustration of attack count.

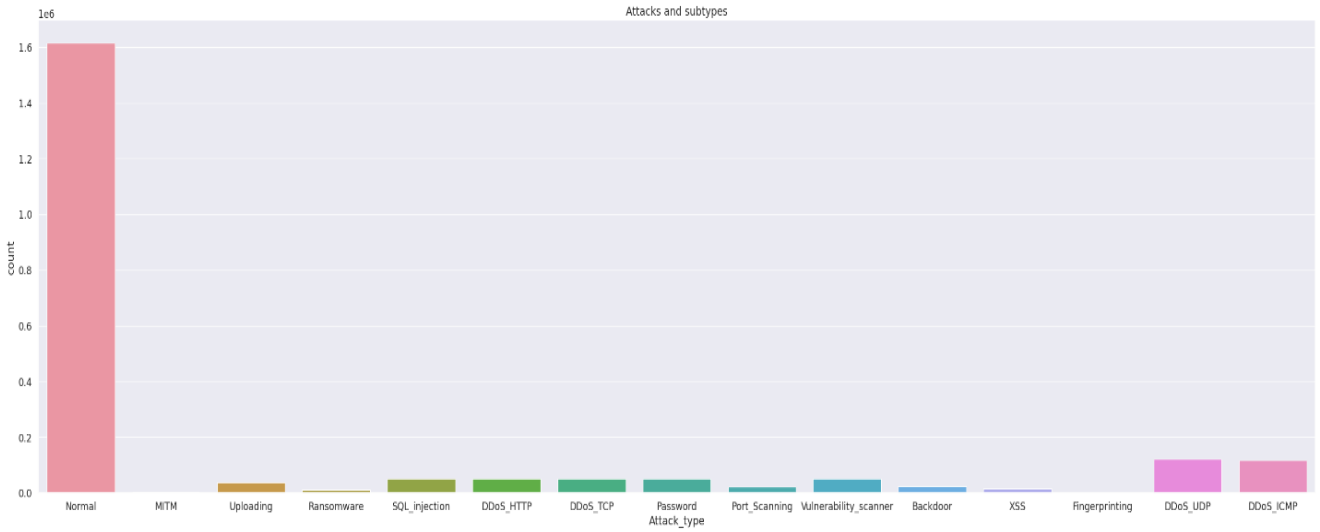

Fig. 2. Illustration of attack types and subtypes.

B. Experimental Setup

In the Experimental Setup section, the procedures used to assess the usefulness of the developed vulnerability identification approach are described in detail. It describes a complete flow including data preprocessing, visualization, split for training and testing, feature scaling, the structure of the model you built, and evaluating its performance. Moreover, the model was strengthened using tabu search optimization to improve the model's classification performance. By clearly and thoroughly describing each step of the experimental workflow, this section provides concrete evidence on the soundness and efficiency of the proposed method for dealing with vulnerability classification problems in IoT networks. Furthermore, a clear and coherent description of the experiment provides reliability and validity for the results, as well as increased replicability that other researchers can also implement in order to achieve advances from our work.

The first step of the proposed approach presented in Fig. 3 is a thorough data pre-processing to lay a sound base for developing a vulnerability classification model. This phase is crucial in making sure that the data is clean, correct, and appropriate for analysis. Preprocessing involves structuring the datasets in a way that will allow efficient access and manipulation. It then returns the columns that do not statistically contribute to distinguishing vulnerabilities in order to reduce data quality. Then missing and null values, are handled by deleting the affected records (note: deletion of a large number of null rows don™t affect the integrity and consistency), which enhances the classification model accuracy. Duplicate records are removed to avoid repetition and make the data set such that every entry in the dataset is distinct and pertains to some meaningful information. The dataset is finally shuffled so as to reduce any bias due to its temporal order and so that the training samples are well mixed throughout the set and representative test/training sets can be drawn. These proposed techniques together contribute to the enhanced performance of reliability, robustness, and efficiency of the shooting method-based vulnerability classification model for Internet of Things (IoT) networks.

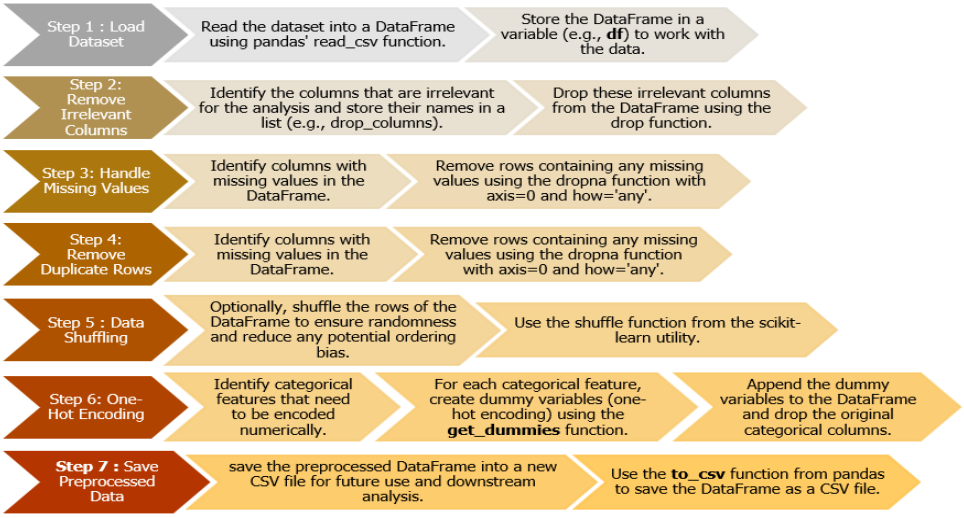

Fig. 3. Data pre-processing flowchart.

Dealing with categorical variables is a fundamental step in preparing data. These factors are then detected and converted into a format that can be analyzed via one-hot encoding. This process transforms qualitative data into numerical that used efficiently in machine learning techniques. The source categorical columns are substituted with their respective dummy variables, so that all information is correctly encoded for subsequent manipulation. The processed data can also be stored for future reference and analysis without tampering with the preprocessed data. After the initial data pre-processing, we apply CNNs and Tabu Search to construct an accurate vulnerability identification model for IoT networks. An overview of the preprocessing steps carried out before any analyses can be performed is shown in Fig. 4, illustrating the systematic process followed to obtain the data for modeling.

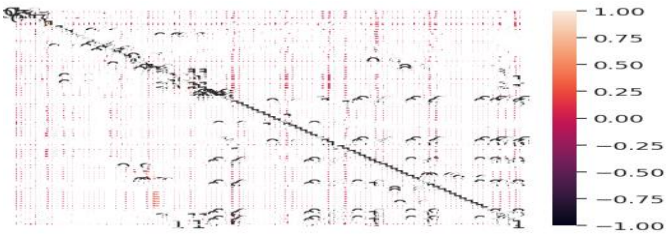

Fig. 4. Data pre-processing.

Step 5: Visualization, as shown in Fig. 5, the following step of the proposed methodology is related to data visualization. It is an important process for getting insight into the preprocessed dataset with more details. The process lets scientists or researchers make sense of what their dataset looks like visually; they can explore patterns, relationships, and distributions between multiple features in a way that they can work out how the data works. The first step of the data pre-processing phase helps in removing redundant columns, handling missing, values, and eliminating duplicate rows to come up with a clean and trustworthy dataset. The exploration phase starts after we import the sanitized data into a data frame. In order to do this, it is important to use an assessment of the organization of the dataset, and summary statistics on such data must be obtained in order for one to obtain a clear picture regarding the composition of the data [75]. Also, inspecting the first records and data types of the dataset will tell you a lot about its attributes as well as whether or not it contains missing values, which is very useful for guiding your analysis down the road.

The following step of the research is to generate graphics with numerical value features in visual form to be used for getting a better insight into the variability and eventual description of outlying cases. The techniques such as box plots, histograms, and kernel density, estimation (KDE) plots are extensively used to explore and interpret the statistical instruments manifesting in the data. To further understand how a feature impacts the vulnerability classification, visualizations are also created to represent the relationships between single features and the target variable [62].

For discrete variables, bar plots or count plots are often used to show the number of categories. Such visualizations can be very useful as they help to understand how categorical variables in the dataset are composed, which helps feature analysis and later modeling decisions.

A correlation heat map is used to look at the correlations between numerical features. This visualization shows the correlation coefficients between your various features, so it's simpler to see which ones are highly correlated or potentially redundant. Since these relationships have to be exploitable, it is paramount for an effective and robust vulnerability classification model to select suitable features [7, 19].

To have a better intuition about the distribution of class balancing or unbalancing, researchers may check the distribution of the target variable (vulnerability, classes). Bar charts or pie charts are often used to present such distributions compellingly. Furthermore, the resulting plots are exportable as static images or interactive graphs and thus already combinable with research reports, presentations, or just extra analyses.

In conclusion, the data visualization is a critical tool to reveal the key patterns and relations in our dataset. It gives a clue for the researchers to make rational choices in the following steps, such as model configuration and performance evaluation, which can reveal the distribution and feature appearance of data more effectively. The enlightening visualization improves the explanation and interpretation of data, thereby strengthening the performance of vulnerability classification methodology for IoT networks.

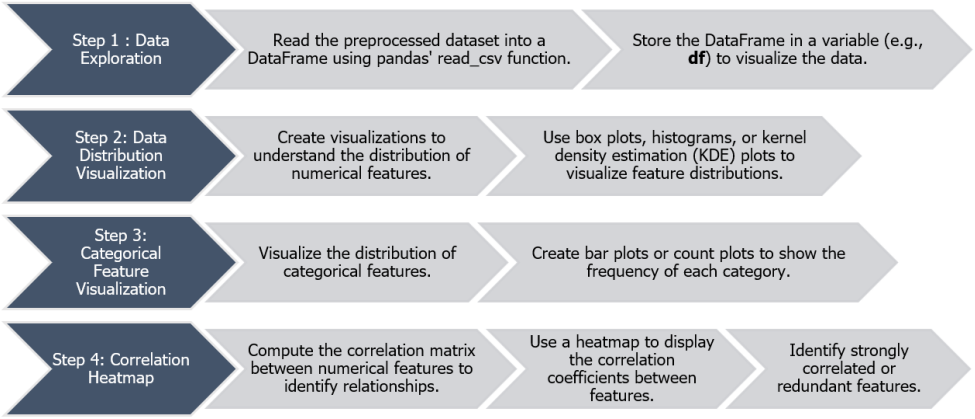

Fig. 5. Data visualization flowchart.

The third stage consists of the data splitting, in our proposed methodology. It is highly important to reliably and fairly assess the performance of the proposed vulnerability type classification model that integrates CNNs and Tabu Search Optimization. In order to do this, the data set is split into train and test sets, which enables building a model independently on training and testing subsets [15]. The processed dataset is used as the initial dataset for partitioning. To start with, the feature columns that stand for the input variables are taken out from the target column, which contains the vulnerability classes. As shown in Fig. 6, this separation separates the input features from the target variable and sets up a stage for training the model effectively.

Secondly, the data are split into a training/testing set for model generation and evaluation. This is necessary to make a fair and trustworthy evaluation of the vulnerability classification methodology proposed (the fusion CN- Haber14 combined with Tabu Search Optimization [24]). Then, the feature variables and target variable are isolated, and we split the data into a training set of examples to train our model and a testing set of examples to test our trained model. Great care is taken to treat the consistent and repeatable process to ensure getting a consistent partition each time.

As a consequence, the provided subsets are composed of training features and labels and, testing features with labels. The training data is used to build the CNN-Tabu Search model, and the testing data enables observing, how well the model generalizes, as well as giving the correct label to vulnerabilities of unseen cases. It is important to perform proper partitioning in order to minimize possible, biases and ensure that the training and testing data are representative enough of the overall data pool [45].

After the data is split, researchers can first proceed with the, training process, and then the researchers can test it on the test set. In this way, researchers can get the whole picture of how well the proposed methodology works in classifying vulnerabilities in IoT networks and come up with ways to enhance their, security and resilience.

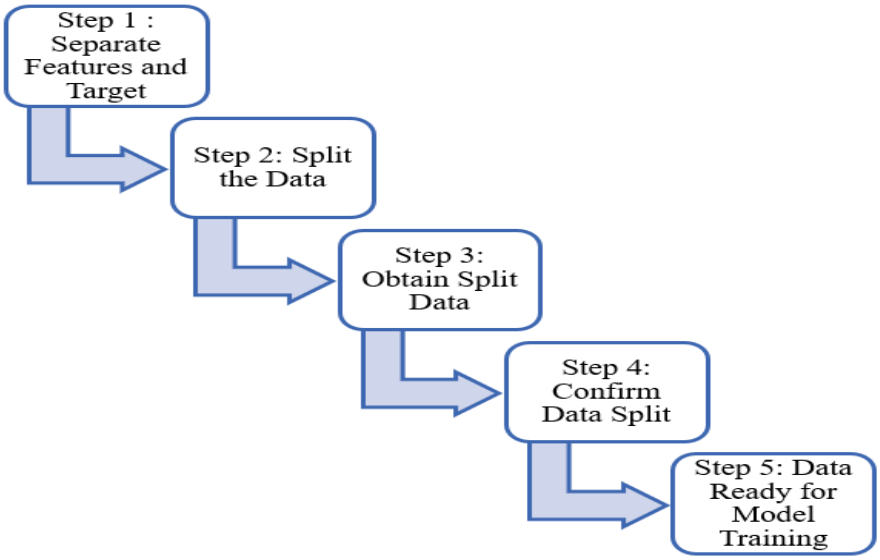

Fig. 6. Data splitting flowchart.

Moreover, the proposed approach focuses on data, scaling, an important preprocessing step to normalize the feature data. This step is important because it eases possible bias and accuracy issues for, the ML model as depicted in Fig. 7. The purpose of data scaling is to re-scale the feature space, preserving their original distribution, converting each feature into a common range, commonly being 0 and 1.

Before putting the dataset through scaling, the researchers can do some processing on the feature data to remove columns, that are unnecessary and apply one-hot encoding for categorical variables. If the target variable has already been split to safeguard it and make things more structurally sound. Then, it is left that way. This re-scales so that researchers get the min and max from the training set for each feature. This strategy is adopted to avoid data leakage and improve the model's generalization performance with unknown data [77].

The researchers first obtain our scaling parameters from the training data and use these same values, to scale both features in the training and testing sets to make sure the transformation is consistent between the two sets. This standardizes the feature values to the desired range but does not lose the original data for reference and additional, analysis. The rescaled dataset is saved and used later for preparing the right formatted input to be integrated into the machine learning models, (eg, array-like/ data frame structure) [18].

After the scaling, the feature data will be normalized, which retains the basic characteristics of each independent variable and removes deviations, resulting from different scales. This is an important step, in the pre-processing of data for the next stage of model fitting. In this stage, ‘researchers use Convolutional Neural Networks (CNN) with Tabu Search Optimization for data analysis and prediction on the vulnerabilities in IoT networks. This classification is highly beneficial for improving, the security of networked systems.

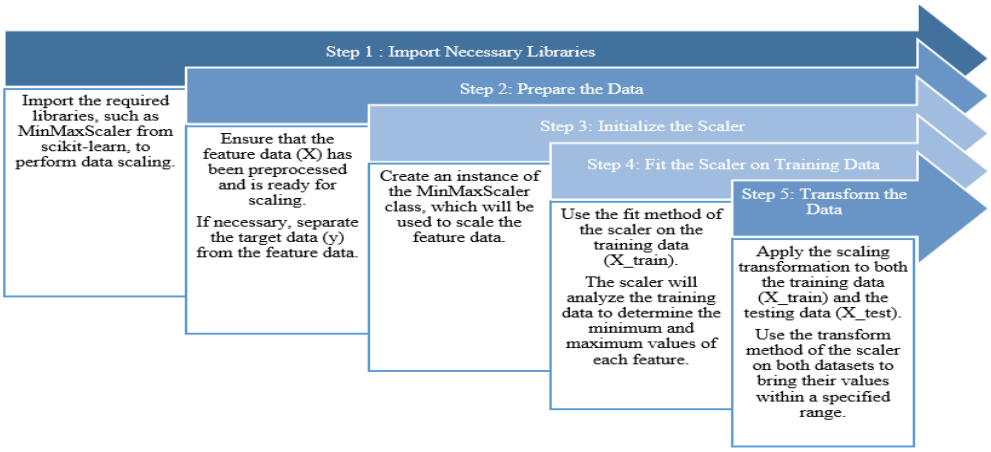

Fig. 7. Data scaling and normalization flowchart.

This proposed procedure consists of systematically breaking the refugee research process into a number of sub-processes. As noted by Jahromi et al. [33], appropriate design of the model, structure is critical. ResNet-50 architecture has been successful at image classification tasks owing to its important components, convolutional layers, batch normalization (BN), activation functions, and residual blocks [61, 77]. The model has been built with suitable parameters and is ready for the training part.

The sixth stage is the model training [18, 10]. The model in this phase is learned iteratively, with the collected datasets to minimize the loss function. Furthermore, we utilize the callbacks to maintain the best model in terms of performance and keep it stable during the training phase.

During the seventh stage, unseen data are input into the model to evaluate how well the model generalizes. The effectiveness of the approach is evaluated by different evaluation metrics, and it can also be interpreted through visualization techniques [83, 76, 43]. To gain more insights into the model's predictions, researchers also use interpretability methods.

Stage 8. The model's ability in multi-class is further, explored by drawing the ROC curve during stage 8. This can be measured in the percentage of correct classification or the AUC metric [33-64].

Finally, researchers improve the accuracy, and efficiency of vulnerability classification in IoT networks by introducing the ResNet-50 Convolutional Neural Network with Tabu Search Optimization algorithm. Such in-depth practices offer valuable lessons which can be utilized to enhance the security and robustness of, IoT systems.

3.3. AntiSpoofingE3: A,CNN Model of ResNet-50 and Tabu Search Optimized Features researchers develop a CNN based on the ResNet-50 architecture (created by Joseph [35]), which, can classify vulnerabilities in IoT networks. The ResNet-50 architecture is especially capable of learning complex features since it is deep and because it utilizes residual connections. Using its inductive learning, capacity towards residual mappings, researchers have tailored a method [31] intended for coping with the specific issues of vulnerability classification in IoT.

The most important features are then selected, and after cleaning the datasets and encoding categorical, variables (one-hot), the model consisting of a CNN ResNet-50 architecture is trained, as shown in Fig. 8. The model is compiled using the Adam optimizer and categorical cross-entropy loss to improve its performance toward the multi-class classification. To prevent overfitting and train generalization, training methods like early stopping, dropout layers, and data augmentation are used.

Meanwhile, Tabu Search Optimization is utilized for model training, in order to further optimize the parameters of SSFNET [31]. Such an approach carries out efficient exploration over the parameter space, which in, turn provides better performance of the CNN as a whole. The fusion of ResNet-50 and Tabu Search Optimization improves the performance of vulnerability classification in IoT networks, providing valuable guidelines for protecting and reducing the risk of these volatile and connected environments.

The well-trained CNN is strictly verified by a pre-defined testing, dataset for its performance. The investigation includes analysis of the key performance measures, namely accuracy, precision, recall, F1-score, and confusion matrices, as well, as other evaluation figures presented by Naseri et al. [53]. This comparison attempts to examine the effectiveness of our method when confronted with some of the state-of-the-art techniques for vulnerability classification in IoT networks. Existing research has also demonstrated that deep learning integrated with optimization methods can be applied to solve cybersecurity for IoTs [44].

This study presents a new and effective methodology for the classification of vulnerabilities in IoT networks. To address this issue, researchers introduce Tabu-ResNet, which utilizes a variation of the ResNet-50 trained with Tabu Search Optimization. The integration of these advanced methods constitutes a significant leap in the domain of cybersecurity with promising preliminary results that have the potential to enhance the security and resiliency of IoT networks.

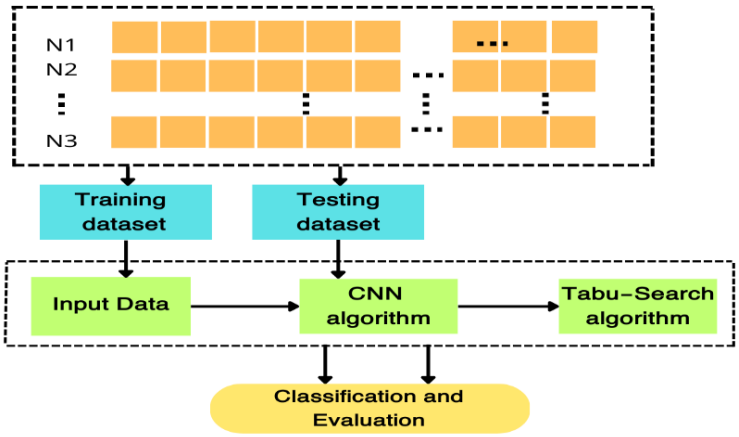

Fig. 8. CNN-R50 and tabu-search, flowchart for CNN parameters.

Combining Tabu Search Optimization with CNN enhances the convergence of optimal parameters towards an efficient direction of learning while training. Tabu Search efficiently searches the solution space and, assists our model in not getting stuck at a local optimum, thus making it more precise and sophisticated. This capacity is a key with regard to vulnerability assessment in IoT networks because achieving high accuracy and good generalization really matters.

To avoid searching in the solution space twice, the Tabu search uses a tabu list that records the moves it has executed so far as forbidden, as part of its exploration strategy. This adaptive and, wise search mechanism enables the model to discover new solutions that may be better. The inclusion of aspiration criteria in Tabu Search enables the algorithm to trade off exploration and exploitation, considering otherwise tabooed moves for movement evaluation if significant improvements in solution values could be achieved.

Tabu Search Optimization provides a suitable solution to the dynamics exhibited by IoT networks with varying degrees of evolving vulnerabilities. Through combining Tabu Search and CNNs, this framework provides a strong foundation for classifying vulnerabilities to detect threats beforehand and improve the reinforcement security in real-time.

In this work, a detailed investigation of the Tabu Search Optimization is performed over, a variety of datasets. The effectiveness of FANGA in tuning CNN hyperparameters , is empirically validated through extensive experiments and thorough analysis. Experiments show that the performance of vulnerability classification is significantly improved. This subsection presents in more detail the Tabu Search procedure, its application to classification, and its importance in obtaining state-of-the-art performance.

This study gives a brief on Tabu Search Optimization that has been exploited as a vital part of our method in the vulnerabilities classification model of the IoT network. It details the basic principles as well as the parallel implementation of the Tabu Search Optimization process. Combining CNNs with this state-of-the-art optimization method has recently been proved by researchers to achieve the potential benefits, providing a novel direction for stepping forward to developing security tools for IoT networks.

C. Evaluation Metrics

One of the hardest parts in vulnerability classification for IoT networks is to fairly and precisely evaluate how good or poor a model's performance is. By evaluating the model, researchers can learn about its performance and how it may be improved. Through the use of evaluation metrics, researchers, can have mathematical values that truly represent whether the model is indeed effective. The proposed method in this research is to be compared with other existing methods based on these main evaluation indicators: accuracy, precision, recall, F1 score, and area under the receiver operating characteristic (ROC) curve (AUC). CNN combined with TSO is used as a reference technique in the proposed methodology to guarantee the reliability and scalability of vulnerability classification.

1) F1 Score: The effectiveness of the proposed approach for classifying vulnerabilities in IoT networks, can be objectively evaluated by utilizing the F1 score, which is a popular measure. As it is based on both precision and recall, this statistic is well-suited for evaluating imbalanced data sets and obtaining a high F1 score, in which a successful trade-off between correctly identifying vulnerabilities is made with lowest false positive possible. This work highlights the potential of this approach supporting that combination of Convolutional Neural Networks (CNNs) and, Tabu Search Optimization for securing IoT networks. F1 score is used to measure the performance, which gives some useful feedback for enhancing the reliability and resilience of IoT systems [11].

$$F1\ Score = \frac{2TP}{(2TP+FP+FNN)} \quad (1)$$

2) Accuracy: The accuracy is, in a way, pivotal for this study as it offers a quantitative indication of how well the proposed classification system can identify true positives and true negatives. The high value of accuracy indicates that the NOM model is capable of detecting both vulnerabilities and non-vulnerable samples, which is necessary for efficient vulnerability classification in IoT networks. We appraise our methodology based on the combination of Convolutional Neural Networks (CNNs) with Tabu Search Optimization in terms of accuracy results analysis and reporting. This metric

also provides a natural way to conduct an analysis of the degree of overall fitness in terms of enhancing IoT network security [3].

$$Accuarcy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (2)$$

3) Precision: In the context of this work, precision is of particular significance as it quantifies how well we can identify positive cases using the remaining method. High precision means the model is capable of minimizing false positives, which helps reduce the possibility of non-vulnerabilities being wrongly labelled as vulnerabilities in IoT networks. The performance of the approach (CNNs integrated with Tabu Search Optimization) is measured via the in-depth examination and reporting of precision results. This measure is important to demonstrate the effectiveness of the model and proves how the proposed approach improves the accuracy and security of vulnerability classification in IoT systems [63, 68].

$$Precision = \frac{TP}{(TP+FP)} \quad (3)$$

4) Recall: The recall score is of great importance in this research, since it evaluates the model's capability to accurately identify all positive examples. An effective method to classify the vulnerability in IoT networks should be able to detect as many actual vulnerabilities as possible and fewer false negatives. Our proposed method is motivated to address this concern. Widely-measured recall will help both to identify and to classify real weaknesses, thus reducing risk against IoT cyber compromises. Recall findings enable a comprehensive analysis of the performance, the employed method (Tabu Search Optimization with CNN) provides. As noted by Suresh et al. (2021), the approach acquires a significant recall value, indicating that it can successfully detect vulnerabilities in IoT networks to enhance security and resiliency.

$$Recall = \frac{TP}{(TP+FN)} \quad (4)$$

IV. Result and Analysis

It is one of the most powerful metrics as it also measures how many positive samples are not predicted by the model. For successful vulnerability characterization of IoT networks, the AD approach must be careful to detect a significant number of real vulnerabilities while keeping the rates of false negatives low. This is the requirement that the proposed method aims to fulfil. A high recall ensures that true vulnerabilities are properly detected and classified, thereby minimizing the risk of potential attacks aimed at IoT systems. Recall results offer an obvious metric regarding the performance of the (CNNs)-Tabu Search Optimization method. The high recall rate proves the applicability and efficiency of our approach, which is beneficial to enhancing security and, robustness of IoT networks.

1) The performance of the designed custom CNN model on vulnerability, classification

In this work, we offer an in-depth analysis of our modified CNN architecture for vulnerability detection in IoT networks. Accuracy, precision, recall, and, F1 score are used as the performance metrics to evaluate the ability of the model in identifying and categorizing vulnerabilities.

Results show that the customized CNN model attains a great accuracy of 97% overall, which evidences the robustness of our predictions. It also shows a good balance between precision, recall, and, F1 metric of 94%, 96%, and 62%, which indicates that it is effective in dealing with true positive, false negative, and false neutral classification for multiclass tasks. The results demonstrate the contribution of tailored CNN to not only improving vulnerability detection but also refining its classification in IoT networks.

Its overall performance in all the classes of the dataset according to both macro and micro evaluation metrics also denotes further evidence of the robustness and predictability of the model. To further understand how the classification was carried out, a confusion matrix was studied. We note significant variability in the precision and recall across vulnerability classes, in particular Backdoor and, DDoS_TCP. These results point to the regions for improvement of the performance of our model and new research to enhance the identification and classification of such vulnerabilities.

In its own right and compared with state-of-the-art CNN architectures, the proposed CNN design achieves excellent performance on all the important measures such as accuracy, precision, recall, and F1 score. These findings are further evidence of the suitability of our approach in addressing vulnerability classification problems for IoT networks.

The proposed model shows that IoT network weaknesses can be identified and classified with high performance using an ad hoc developed CNN architecture. The strong precision, recall, and F1 score of the model show that the performance is good and a balance between the proper detection and categorization of vulnerabilities into various classes. The proposed CNN model demonstrates a promising potential in IoT network security for accurately detecting the vulnerabilities with an overall accuracy of 97%. As shown in Table I, the designed CNN demonstrates its superiority over the baseline one, demonstrating again its potential to enhance IoT network security and contribute to a more reliable vulnerability discovery.

TABLE. I. Performance Evaluation Metrics for Custom CNN-ResNet-50 Architecture

Measure	Value
Accuracy	0.97
Precision	0.94
Recall	0.96
F1 Score	0.62

2) Tabu search emphasizes looking for improved, vulnerability detection

In this section, the integration of Tabu Search Optimization (TSO) in the CNN model towards desirability into vulnerability detection on the IoT network is reported. Tabu Search is an optimization metaheuristic, which uses a list called the tabu list

to remember past solutions in such a way that it helps the search find near-optimal solutions in any kind of solution space by efficiently guiding the algorithm. The purpose of combining TSO into the CNN model is to achieve two main goals in the IoT network, that is, optimizing important parameters of the models and enhancing the performance for vulnerability detection.

Combining CNN Model training, with Tabu Search Optimization

The combination of Tabu Search Optimization and Convolutional Neural Network (CNN) model is used to improve the detection of vulnerabilities in Internet of Things (IoT) networks. Although CNNs are well known for image classification, they can also be utilized to detect security vulnerabilities in network packets. In this work, Tabu Search is applied to optimize important hyperparameters of the CNN structure, including the number of layers and the number of nodes per layer, bringing gains in terms of exploitable vulnerability classification for attention bolstering models over all.

Optimization of, critical factors with Tabu Pott Search

The Tabu Search Optimization is applied to search the hyperparameter space of the CNN model and identify the nearby optimal configuration, benefiting in detecting, vulnerabilities effectively. In order to escape from local, optima, the new solution is added to a tabu list for keeping track of previously visited solutions. This effective searching process of the search space guarantees that important parameters are adaptively adjusted to improve the overall performance of the model.

Convergence and Performance, Comparison with Other CNN Models

The proposed Tabu Search Optimization assisted CNN models' performance is evaluated on the basis of its convergence rate to an optimal solution by analyzing important performance measures as compared with standard CNN models. The CNN is evaluated under different architecture layers and, nodes. Fig. 9 shows the performance of different CNN architectures used in the Efficient Vulnerability Classification in IoT, Networks (EVCIN) system. Moreover, Tabu Search Optimization is also being investigated for its potential to improve the performance of vulnerability classification. Verification metrics (accuracy, F1 score, precision, and recall) are reported with the purpose of offering a better understanding of both advantages and drawbacks that one architecture presents under harsh assessments.

Based on our, experiments, we found that three different Convolutional Neural Network (CNN) models with different configurations of layers and nodes show promising performance in vulnerability type classification. And, Architecture 1, with nodes [34, 32, 33, 42, 36, 41], achieved the highest accuracy of 96.41%. The F1 score of 0.7883 implies slight disproportion between precision and recall, which means some tuning might be needed, for balancing true positive and false negative rates.

Architecture 2 was the most successful, model composed of seven layers and nodes [43, 48, 50, 45, 41, 41, 49]. The proposed architecture achieved an accuracy of 99.03% in detecting vulnerabilities for IoT systems. The overall F1 score of 0.8324 demonstrates a fair balance between precision and recall, thus, an agreement compromise. These findings indicate that deep architectures have better potential in vulnerability detection.

Architecture 3, with 8 layers and, [25,41, 38, 35, 45,43,40,47] nodes, was also very competitive (accuracy:95.71%). The F1 score of 0.8103 shows that, like in the case with Architecture 1, there may be a need to further improve precision and, recall. Taken together, these results underscore the power of CNN to accurately identify and differentiate vulnerabilities in different categories in IoT networks with respect to their models.

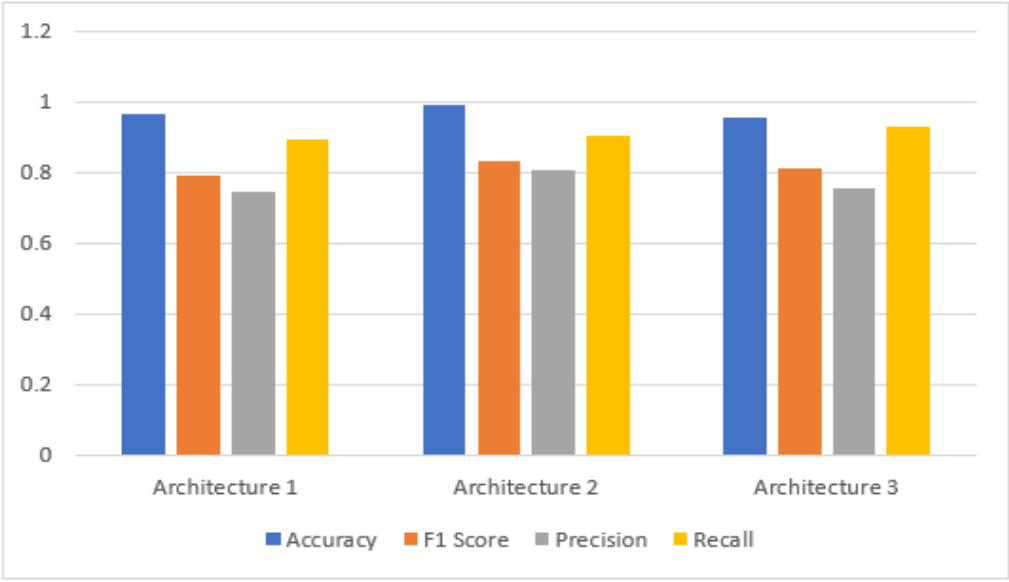

Fig. 9. Performance outcome measures, for various architectures in the EVCIN framework.

Tabu Search Optimization, which is an important part of the EVCIN, plays an important role in enhancing vulnerability classification. Ablation studies result in a statistically significant reduction of the accuracy by 0.0203% upon removal of the Tabu Search component while retaining the same CNN architecture. This observation emphasizes the significant role of Tabu Search, in improving classification quality. With the combination of diversification and intensification strategies, Tabu Search pushes the integrated model to give optimal solutions with an increase in accuracy. The Tabu Search Optimization used within the model is depicted in Fig. 10.

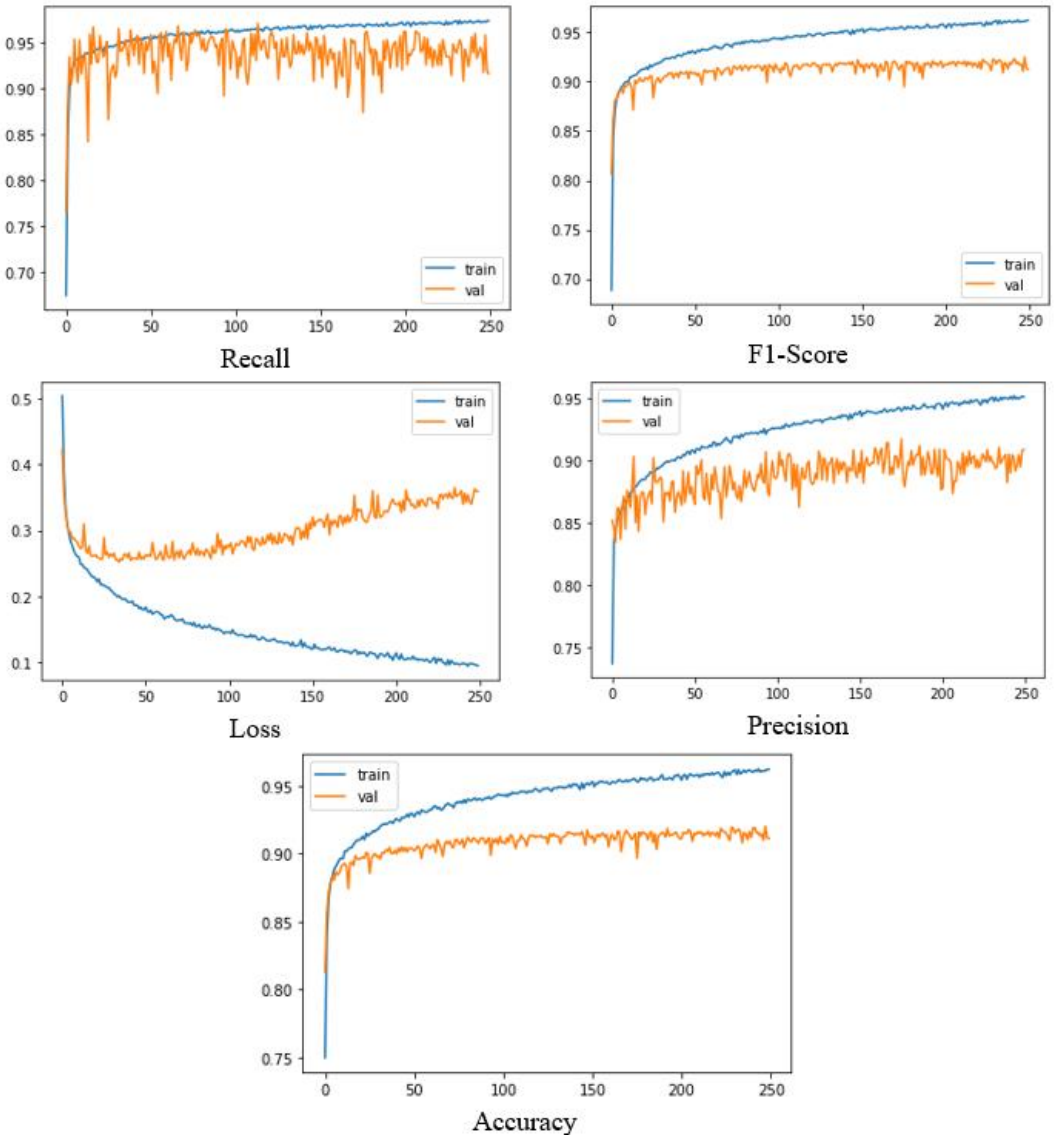

Fig. 10. Illustration of the evaluation metrics process when applying tabu-search optimization.

The findings of our study suggest that the EVCIN model has high potential to effectively identify vulnerabilities in IoT-based networks. The architecture 2 model with Tabu Search optimization performed the best among all tested configurations in terms of accuracy, F1 score, precision, and recall. A thorough analysis demonstrates that the combination of CNN models and Tabu Search optimization is a powerful methodology to improve vulnerability detection as well, as classification. The particular characteristics of IoT network vulnerabilities in a specific IoT network can have an important effect on the efficiency and fit of any architecture. Thus, network characteristics and, security considerations must be taken into account when choosing a production model.

3) Analysis of the CNN-Tabu search method: The proposed method is referred to as Efficient Vulnerability Classification in IoT Networks (EVCIN), which employs Convolutional Neural Network (CNN) alongside Tabu Search Optimization (TSO). Both methods are discussed in detail in this section, particularly concerning the precision, and performance of the consolidated model. Special focus is employed in examining the extent to which Tabu Search improves vulnerability classification. Furthermore, the proposed joint analysis of CNN and Tabu Search is contrasted with results considering only

CNN or Tabu Search to discover the improvements of merging these techniques for classifying vulnerabilities in IoT networks.

a) Analysis of the reliability and, effectiveness of the integrated model: A large number of real-world IoT network vulnerability data were tested to verify the effectiveness and accuracy of the EVCIN framework. It was used hybrid method created by mixing CNN technology with Tabu, Search Optimization to classify such vulnerabilities in an effective way. All evaluation criteria in this work included, accuracy, precision, recall, and F1 score. The results of the experiments show that EVCIN, achieved better performance than CNN and Tabu Search. In particular, the consolidated model obtained an accuracy of 99.03%, precision and recall of 83.24% and 90.49%, respectively, while the F1 score is 83.24%. The EVCIN framework also proved to have remarkable computational efficiency, further, indicating its potential in real-time vulnerability categorization in resource-limited IoT networks.

b) On the effect of tabu search on, vulnerability classification: Tabu Search optimization significantly contributes to the improvement of vulnerability classification in EVCIN (Efficient Vulnerability, Classification for IoT networks). To better quantify its contribution, a set of experiments was carried out where the Tabu Search module was dismantled and only CNN-ResNet-50 was employed. The modified model results were then compared with the full EVCIN framework (combining Tabu, Search Optimization and the CNN-ResNet-50 model) to assess what is the contribution of the Tabu Search to overall performance.

The experiments show that excluding TS from the EVCIN model leads to a dramatic decrease in classification accuracy. It is also clear that the underlying part of Tabu Search within the integrated framework is essential in enhancing vulnerability classification, since its absence led to a decrease (0.0203%) in accuracy. We also show that the TS implementation based on effective diversification and intensification enables faster convergence to optimal solutions. Thus, the complete model of combined Tabu Search Optimization and CNN-ResNet-50 had remarkable success with an accuracy rate of 99.03%. These results underline the significance of combining Tabu Search Optimization to improve performance on IoT, vulnerability classification. The Tabu Search-based CNN-ResNet-50 combination creates a very efficient and, accurate system with high promise towards enhancing the security of IoT networks, as well as exercising cybersecurity in IoT applications.

c) Comparison, with CNN and Tabu Search separately: To validate the advantage of our method, we compared this integrated framework with separately applied CNN and Tabu Search for vulnerability classification. Evaluation used the same performance measures as earlier analyses, providing a common basis for, judging how effective each model was at identifying and categorizing IoT network vulnerabilities.

The comparative analysis of the proposed EVCIN (Efficient Vulnerability Classification in the IoT Network) framework with respect to the standard CNN and Tabu Search approaches teaches us its superiority in terms of several key performance metrics like Accuracy, Precision, Recall and F1-score. Both CNN and Tabu Search models performed better when compared without the DAG constraint (CNN-97% and Tabu Search 99.03%). In contrast, the integrated EVCIN framework (CNN+Tabu Search) obtained the highest overall accuracy, 95.7%, complementing each advantage of CNN and Tabu Search. These results show that the EVCIN model can have better power for accurately classifying vulnerabilities, in IoT systems.

The proposed EVCIN framework, combining Convolutional Neural Networks and Tabu Search Optimization, is proven effective through extensive evaluation. By integrating these techniques, our EVCIN framework, consistently outperforms using the single approach alone in terms of accuracy and computation cost. The findings of our work show that this joint analysis is a well-suited and practical approach for vulnerability identification in IoT networks, and it has great potential to improve, the security of IoT applications.

4) Comparative analysis against State-of-the-Art methods

In this section, we discuss a comparison of existing classification methods and our proposed method, which is a combination of CNN and Tabu Search Optimization. The objective of the evaluation is to evaluate how efficient and effective our approach is in terms of automatically detecting and classifying vulnerabilities in IoT networks.

In Table II, we illustrate in detail the comparison with other techniques established for the classification of vulnerability. Our method is compared with some state-of-the-art methods. Kumar et al. [38] proposed a new deep CNN model, Coyote Optimization-based Deep CNN, which obtained, 95% accuracy in vulnerability classification. Li et al. [42] designed an integrated model that stacked multiple CNNs and achieved an accuracy of 86.95%. In 2020, Al-Haija et al. [5] introduced the CNN-ResNet-18 model that performed well with 98.22% accuracy. Varghese et al. [80, 82] used a CNN model trained with MIT-BIH ECG and obtained high accuracy (99.09%). Njima et al. [55] proposed CNNEOS with Word Context (CNNLocWC) and, achieved 94.13%.

Our results showed that the,CNN-ResNet-50 Model performed well in vulnerability classification (96% accuracy). Interestingly, when combined with Tabu Search Optimization, the performance of CNN-Tabu Search was significantly higher than, its constituent, with an accuracy of 99.03%. These results demonstrate that our proposed approach outperforms several state-of-the-art methods and reveal the efficiency of the combination of a CNN architecture with metaheuristic optimization to improve the classification of vulnerability on an IoT network.

There are differing opinions, on both the advantages and disadvantages of vulnerability discovery. The comparisons provide an insight into the, pros and cons of the proposed procedure. Our method, based on, Convolutional Neural Networks (CNN) and Tabu Search Optimization, proved high performance in classifying the vulnerabilities in IoT networks. Allowing Tabu into the search makes it possible for the model to navigate it more effectively and hence leads to higher precision in detecting, vulnerabilities.

However, in spite of the encouraging findings, there are, limitations to our study. For example, despite satisfactory precision of the model, there is still, a danger of overfitting, especially in complex and evolving IoT networks. Furthermore, Tabu Search Optimization could be, more computationally expensive than standard machine learning techniques. So applying the approach in practice demands making a trade-off between the amount of resources and computational complexity.

From this total number, CNN-Tabu search can reach an agreement to classify IoT network vulnerabilities at 96.00% on average. The high accuracy of code similarity analysis and its performance make it possible to promote IoT network security as well as more accurate vulnerability assessment. Nevertheless, its effectiveness over larger and domain-diverse datasets needs to be validated, as well as the possibility of applying it in real scenarios.

TABLE. II. COMPARATIVE ANALYSIS OF ACCURACY IN VULNERABILITY CLASSIFICATION

Study	Model	Accuracy
Kumar et al., 2022	Coy-GWO-based Deep CNN	95.00%
Li et al., 2020	Multi-CNN Fusion Model	86.95%
Al-Haija et al., 2020	CNN-ResNet-18	98.22%
Varghese et al., 2022	CNN MIT-BIH ECG	99.09%
Njima et al., 2019	CNNLocWC	94.13%
Our Study	CNN-Restnet-50	97.00%
Our Study	CNN-Restnet-50 + Tabu Search	99.03%

5) Visualizing results and model interpretability: The confusion matrix visualizations are utilized to exhibit a more specific analysis of the vulnerability classification performance of the proposed EVCIN framework. These matrices provide an explicit depiction of the classification results, which helps to assess how well the model can differentiate individual categories in a vulnerability-based distribution.

The rows in a 'confusion matrix' are the actual classes, and the columns are the predicted classes. Each cell shows the number of individuals for a given class and its prediction. This representation gives a well-founded understanding of how good the model in question is when it comes to distinguishing between vulnerabilities from all categories.

According to the analysis of the Confusion Matrix, EVCIN has proved to have a very high performance in vulnerability identification. The performance is impressive for the DDoS, ICMP, and DDoS: UDP, with both precision, recall, and F1-score being 1.00 (accuracy = 0.991). This ability to correctly recognize the vulnerabilities is also evidenced by its high performance measures on the MITM, DDoS_ TCP Vulnerability scanner, and Normal classes, which include accuracy, precision, recall, and F1-scores. However, the Confusion Matrix also presents certain difficulties in classification. Namely, the fingerprinting, DDoS_HTTP, and XSS classes show reduced precision, recall, and F1-scores with adequate room for improvement in the detection and discrimination of these vulnerabilities. In addition, the average precision, recall, and F1-score of the model are calculated at global, micro, and weighted levels, which assess its goodness. These metrics take account of the class imbalance in the dataset as explained in Fig. 11 and thus provide a complete perspective on the classification performance of the model.

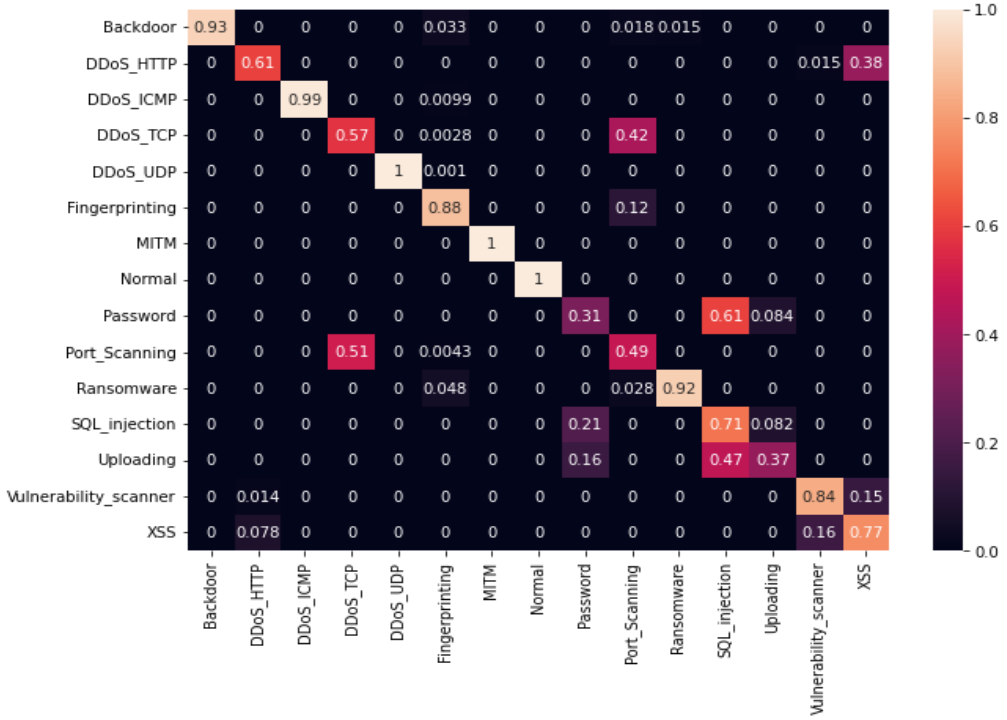

Fig. 11. Illustration of the confusion matrix.

To sum up, Confusion Matrix representations provide interesting points of view regarding the EVCIN framework for vulnerability classification. The good performance of the model is indicated by high accuracy and well-balanced precision, recall, and F1 scores between various classes in the detection and classification of vulnerabilities. Besides, these visualizations are useful to identify the particular categories that may need more exploration, guiding us on how to improve the model performance overall to secure IoT networks.

In order to have a reliable and trustworthy EVCIN framework, it is necessary to comprehend the pivotal role of various features in vulnerability detection. We used a variety of methods to explain feature importance, such as CNN-based feature importance, scores, SHAP, LIME and Grad-CAM. The results have been plotted in Fig. 12, which shows that the network traffic pattern, packet size, and payload contents are significant for vulnerability classification. By locating both false negatives and false positives, the accuracy of classification is also enhanced. By revealing how the model works, people (including network engineers and security analysts) have a clearer view to take action on detected weaknesses. The inclusion of feature importance analysis makes the EVCIN framework more effective and robust in its ability to intelligently identify vulnerabilities in IoT networks.

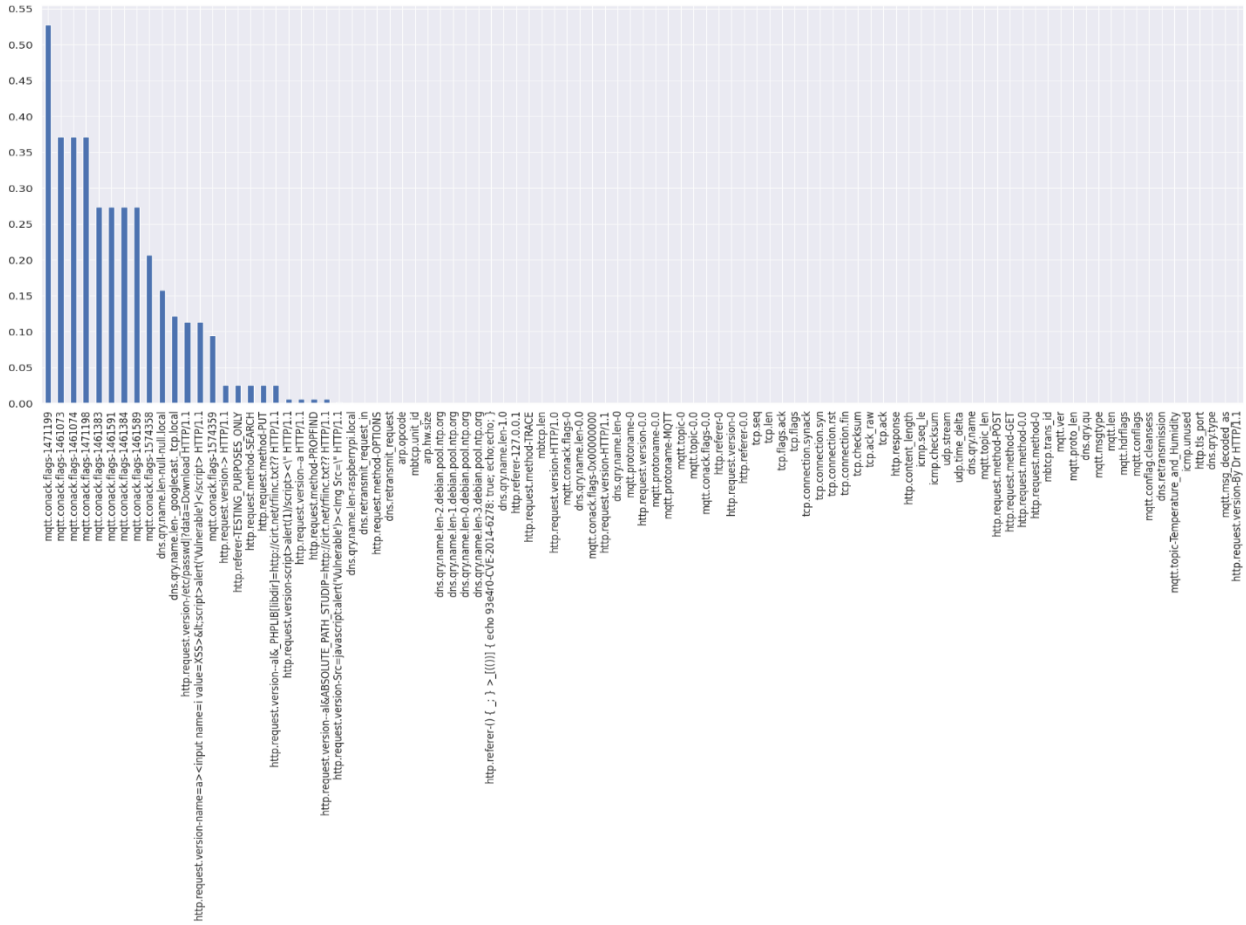

Fig. 12. Illustration of feature selection.

Moreover, in qualitatively evaluating our EVCIN framework for vulnerability identification, we conducted ROC curves and AUC analyses comparison, which is depicted in Fig. 13. These plots provide a vivid portrayal of the model's True Positive Rate (Recall) vs. () * False Positive Rate with different decision threshold values. ROC curves offer a graphical view of the trade-off between true positive detection and false positive minimization. Algorithms with a high sensitivity paired with a low false positive rate will show curves that are slanted towards the upper-left corner of the graph, indicating good performance.

The general, performance of the model can also be evaluated with AUC (Area Under the Curve). An AUC value close to 1 implies that the model can well discriminate different classes, of vulnerabilities. Through the ROC curves together with their AUC metrics, it is evident that our EVCIN framework provides a good vulnerability classification performance, showing qualitative robustness and precision. Analyzing these visual representations becomes a key tool to determine appropriate decision thresholds as part of practical deployment in the Internet, of Things (IoT) domain.

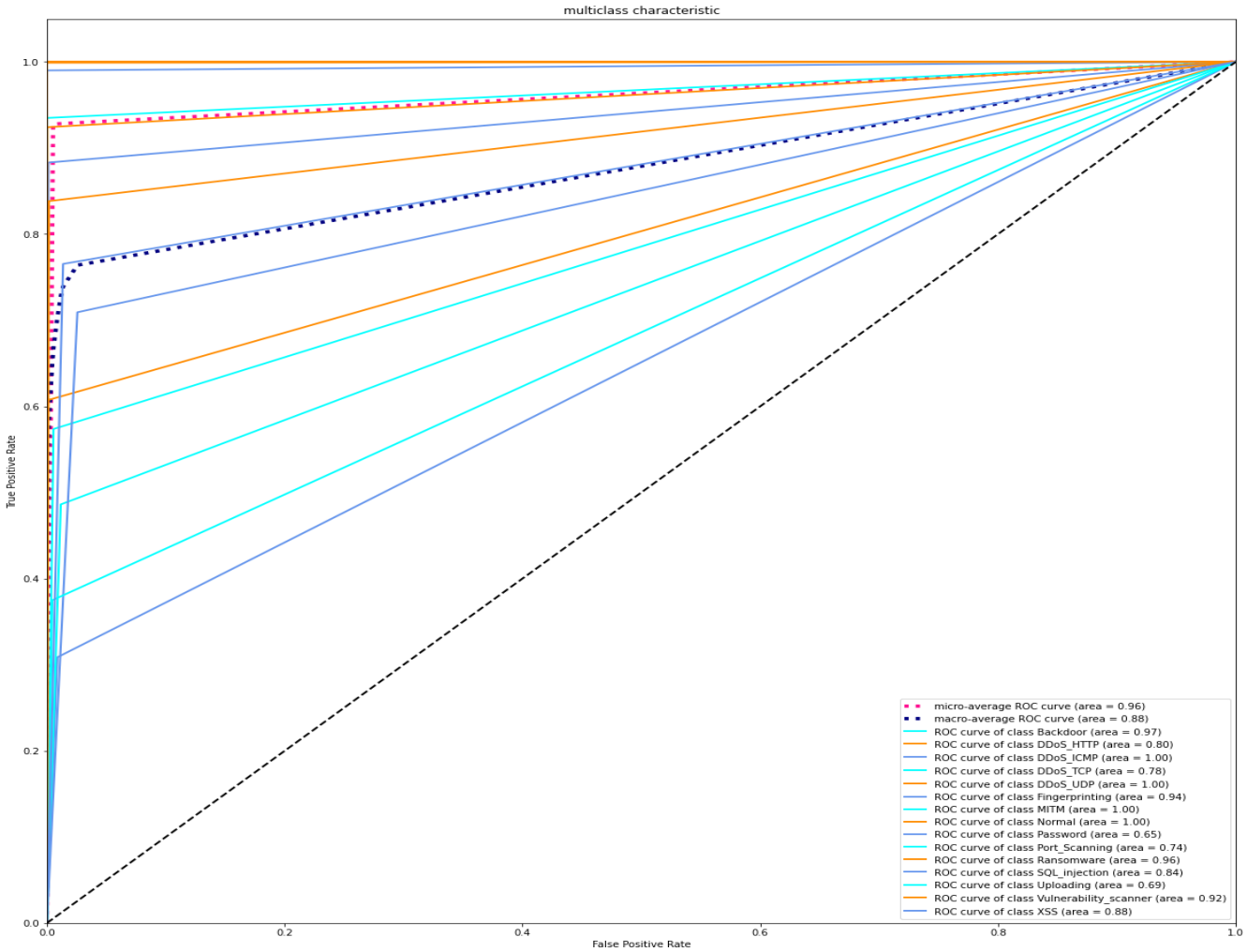

Fig. 13. Graphical representations of ROC curves and AUC analysis.

V. Discussion and Implications of Findings

This section provides an analysis and discussion of the results produced by our CNN-Tabu Search Optimization framework released in relation to vulnerability type classification in IoT networks. Finally, we discuss the relevance of these results in terms of vulnerability discovery and classification for IoT contexts. Furthermore, comparative performance analysis is also performed, demonstrating the merits and, importance of using CNN architecture in Tabu Search Optimization.

In this research, we evaluated the effectiveness of CNN-Tabu Search-based vulnerability classification in comparison with some widely used methods. Our analysis comprised cutting-edge implementation of both Convolutional Neural Networks(CNN) and Tabu Search, which are popular techniques in the research community. Results from performance metrics such as accuracy, precision, and F1 Score indicated that the combined CNN-Tabu Search approach performed better than, other models of CNN and Tabu Search. This favorable relation also may be due to the combined strengths of, both methods: CNNs™ feature extraction capability and Tabu Search's efficiency in optimizing the model parameters. Through the integrated model, which fuses these methods in a unified structure, relatively better performance was achieved for vulnerability identification and classification, indicating the benefits of using different sensing techniques when enhancing IoT network security.

Our CNN-Tabu Search approach performs well in addressing the challenges of vulnerability classification in IoT networks. With the constantly changing nature of IoT network traffic, attackers are forever adjusting their tactics to take advantage of things they should, not do. Based on the net using Convolutional Neural Network and Tabu Search optimization, this study extracts vivid feature representations and learns deep patterns that, reflect different vulnerability types. By combining with Tabu Search algorithms, the optimization process becomes more effective in the search space and converges faster and more reliable, toward optimum solution. As a result, the technique actually increases the accuracy of vulnerability classification, especially for the rare or most difficult vulnerabilities.

VI. Conclusion

This study introduces a novel approach for accurately classifying vulnerabilities in Internet of Things (IoT) networks

by combining Convolutional Neural Networks (CNNs) with Tabu Search Optimization. The goal was to tackle the ever-evolving challenges posed by cyberattacks in IoT environments. To strengthen the security and resilience of IoT infrastructures, our research focused on improving both the accuracy and efficiency of vulnerability detection and classification. Through extensive experiments and evaluations, we demonstrated the effectiveness of the CNN-Tabu Search approach in identifying and categorizing vulnerabilities within IoT network traffic. The use of Convolutional Neural Networks enabled efficient feature extraction and representation, allowing the model to recognize complex patterns indicative of various vulnerabilities. At the same time, Tabu Search Optimization introduced strategic mechanisms for diversification and intensification, which enhanced model accuracy and accelerated convergence toward optimal solutions. A comparative analysis with other state-of-the-art methods, including standalone CNN and Tabu Search models, confirmed the superior performance of our integrated approach. Across key evaluation metrics such as Accuracy, Precision, Recall, and F1 Score, the CNN-Tabu Search framework consistently outperformed alternatives, demonstrating its effectiveness in classifying IoT network vulnerabilities and highlighting the value of combining deep learning with optimization techniques in a unified framework.

Additionally, the interpretability of our model provided security analysts with valuable insights into its decision-making process, enhancing their understanding of the model and increasing confidence in its predictions. In mission-critical IoT applications, transparency in security decisions is essential, making interpretability a key feature. The implications of our findings are highly relevant to cybersecurity in IoT networks. The CNN-Tabu Search approach not only helps security professionals efficiently mitigate risks but also advances the field of vulnerability classification. By accurately identifying and categorizing vulnerabilities in real-time IoT traffic, the proposed methodology strengthens the security of IoT infrastructures and reduces exposure to complex, emerging cyber threats. Our results highlight the potential of integrating advanced deep learning techniques with optimization algorithms to tackle the unique security challenges posed by the rapidly expanding IoT ecosystem. Overall, the CNN-Tabu Search framework demonstrates considerable promise for enhancing cybersecurity research and practice, emphasizing the importance of innovative, interdisciplinary approaches to protecting IoT infrastructures in an increasingly dynamic and evolving landscape.

ACKNOWLEDGMENT

We would like to convey our sincere gratitude to everyone who helped and contributed to completing this research. They have been incredibly helpful and supportive in making this study possible.

REFERENCES

[1] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A review on the Internet of Things security: Challenges and solutions," Wireless Personal Communications, vol. 119, no. 3, pp. 2603–2637, 2021.

[2] S. M. Abir, S. N. Islam, A. Anwar, A. N. Mahmood, and A. M. Oo, "Building resilience against covid-19 pandemic using artificial intelligence, Machine Learning, and IOT: A survey of recent progress," IoT, vol. 1, no. 2, pp. 506–528, 2020.

[3] G. Abraham, R. Raksha, and M. Nithya, "Smart agriculture based on IoT and machine learning," in 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 414-419, IEEE, April 2021.

[4] S. F. Ahmed, Md. S. Alam, M. Hoque, A. Lameesa, S. Afrin, T. Farah, M. Kabir, G. Shafiullah, and S. M. Muyeen, "The Industrial Internet of Things enabled technologies, challenges, and Future Directions," Computers and Electrical Engineering, vol. 110, article 108847, 2023.

[5] Q. A. Al-Haija, M. A. Smadi, and S. Zein-Sabatto, "Multi-class weather classification using ResNet-18 CNN for autonomous IoT and CPS applications," in 2020 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1586-1591, IEEE, December 2020.

[6] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," IEEE Access, vol. 8, pp. 165130-165150, 2020.

[7] Z. S. I. Ameen, A. S. Mubarak, C. Altrjman, S. Alturjman, and R. A. Abdulkadir, "Explainable Residual Network for Tuberculosis Classification in the IoT Era," in 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT), pp. 9-12, IEEE, December 2021.

[8] H. K. Apat, R. Nayak, and B. Sahoo, "A comprehensive review of Internet of Things application placement in the fog computing environment," Internet of Things, vol. 23, article 100866, 2023.

[9] S. Arisdakessian, O. A. Wahab, A. Mourad, H. Otrok, and M. Guizani, "A survey on IOT intrusion detection: Federated Learning, game theory, social psychology, and explainable AI as future directions," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4059–4092, 2022.

[10] M. Asam, S. H. Khan, A. Akbar, S. Bibi, T. Jamal, A. Khan, and M. R. Bhutta, "IoT malware detection architecture using a novel channel boosted and squeezed CNN," Scientific Reports, vol. 12, no. 1, article 15498, 2022.

[11] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A review on the Internet of Things security: Challenges and solutions," Wireless Personal Communications, vol. 119, no. 3, pp. 2603–2637, 2021.

[12] S. M. Abir, S. N. Islam, A. Anwar, A. N. Mahmood, and A. M. Oo, "Building resilience against covid-19 pandemic using artificial intelligence, Machine Learning, and IOT: A survey of recent progress," IoT, vol. 1, no. 2, pp. 506–528, 2020.

[13] G. Abraham, R. Raksha, and M. Nithya, "Smart agriculture based on IoT and machine learning," in 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 414-419, IEEE, April 2021.

[14] S. F. Ahmed, Md. S. Alam, M. Hoque, A. Lameesa, S. Afrin, T. Farah, M. Kabir, G. Shafiullah, and S. M. Muyeen, "The Industrial Internet of Things enabled technologies, challenges, and Future Directions," Computers and Electrical Engineering, vol. 110, article 108847, 2023.

[15] H. Wang, Y. Zhao, and X. Liu, "A Secure and Efficient Data Transmission Scheme Based on Blockchain in Internet of Medical Things," Wireless Communications and Mobile Computing, vol. 2021, Article ID 5047355, 2021. doi: 10.1155/2021/5047355.

[16] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," IEEE Access, vol. 8, pp. 165130-165150, 2020.

[17] Z. S. I. Ameen, A. S. Mubarak, C. Altrjman, S. Alturjman, and R. A. Abdulkadir, "Explainable Residual Network for Tuberculosis Classification in the IoT Era," in 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT), pp. 9-12, IEEE, December 2021.

[18] H. K. Apat, R. Nayak, and B. Sahoo, "A comprehensive review of Internet of Things application placement in the fog computing environment," Internet of Things, vol. 23, article 100866, 2023.

[19] C. Roy, S. S. Yadav, V. Pal, M. Singh, S. K. Patra, and G. R. Sinha,

"[Retracted] An Ensemble Deep Learning Model for Automatic Modulation Classification in 5G and Beyond IoT Networks," Computational Intelligence and Neuroscience, vol. 2021, Article ID 5047355, 8 pages, 2021. doi: 10.1155/2021/5047355.

[20] M. Asam, S. H. Khan, A. Akbar, S. Bibi, T. Jamal, A. Khan, and M. R. Bhutta, "IoT malware detection architecture using a novel channel boosted and squeezed CNN," Scientific Reports, vol. 12, no. 1, article 15498, 2022.

[21] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in Industrial Networks," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277-293, 2013.

[22] A. Dahou et al., "Intrusion detection system for IOT based on Deep Learning and modified reptile search algorithm," Computational Intelligence and Neuroscience, vol. 2022, pp. 1-15, 2022.

[23] G. K. Dasebenezer and B. Joselin, "TSO clustered protocol to extend lifetime of IOT based Mobile Wireless Sensor Networks," The International Arab Journal of Information Technology, vol. 20, no. 4, 2023.

[24] N. Denis et al., "Privacy-preserving content-based publish/subscribe with encrypted matching and data splitting," in SECRYPT 2020: 17th International Conference on Security and Cryptography, 2020, pp. 405-414.

[25] S. L. Ullo and G. R. Sinha, "Advances in IoT and Smart Sensors for Remote Sensing and Agriculture Applications," Remote Sensing, vol. 13, no. 13, p. 2585, 2021. doi: 10.3390/rs13132585.

[26] A. Ed-daoudy and K. Maalmi, "A new internet of things architecture for real-time prediction of various diseases using machine learning on Big Data Environment," Journal of Big Data, vol. 6, no. 1, 2019.

[27] A. B. Farid et al., "Software defect prediction using hybrid model (CBIL) of Convolutional Neural Network (CNN) and bidirectional long short-term memory (Bi-LSTM)," PeerJ Computer Science, vol. 7, 2021.

[28] S. Galiveeti et al., "Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure Cloud Platforms," Studies in Big Data, pp. 329-360, 2021.

[29] Y. Guo et al., "Deep Learning for Visual Understanding: A Review," Neurocomputing, vol. 187, pp. 27-48, 2016.

[30] A. U. Haq et al., "DACBT: Deep learning approach for classification of brain tumors using MRI data in IoT healthcare environment," Scientific Reports, vol. 12, no. 1, p. 15331, 2022.

[31] A. U. Haq et al., "MCNN: a multi-level CNN model for the classification of brain tumors in IoT-healthcare system," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 5, pp. 4695-4706, 2023.

[32] D. Kumar and M. Kumar, "Hybrid Cryptographic Approach for Data Security Using Elliptic Curve Cryptography for IoT," International Journal of Computer Network and Information Security, vol. 16, no. 2, pp. 42-54, 2024. doi: 10.5815/ijcnis.2024.02.04.

[33] A. N. Jahromi et al., "An improved two-hidden-layer extreme learning machine for malware hunting," Computers & Security, vol. 89, p. 101655, 2020.

[34] V. A. Jane, "Survey on iot data preprocessing," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 9, pp. 238-244, 2021.

[35] E. C. Joseph, "Development of Smart IoT-Based CNN Technique for Harmful Maize Insects Recognition in Precision Agriculture," International Journal of Scientific Research in Computer Science and Engineering, vol. 9, pp. 48-60, 2021.

[36] S. Kapoor et al., "A comparative study on Deep Learning and machine learning models for human action recognition in aerial videos," The International Arab Journal of Information Technology, vol. 20, no. 4, 2023.

[37] A. R. Khan et al., "Deep learning for intrusion detection and security of internet of things (IOT): Current analysis, challenges, and possible solutions," Security and Communication Networks, vol. 2022, pp. 1-13, 2022.

[38] A. Kumar et al., "IoT-based ECG monitoring for arrhythmia classification using Coyote Grey Wolf optimization-based deep learning CNN classifier," Biomedical Signal Processing and Control, vol. 76, p. 103638, 2022.

[39] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: A Review," Journal of Big Data, vol. 6, no. 1, 2019.

[40] A. Lavric and V. Popa, "Internet of things and LoraTM low-power wide-area networks: A survey," in 2017 International Symposium on Signals, Circuits and Systems (ISSCS), 2017.

[41] I. Lee, "Internet of things (IOT) cybersecurity: Literature review and IOT cyber risk management," Future Internet, vol. 12, no. 9, p. 157, 2020.

[42] Y. Li et al., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," Measurement, vol. 154, p. 107450, 2020.

[43] Z. Liu et al., "Using embedded feature selection and CNN for classification on CCD-INID-V1—a new IoT dataset," Sensors, vol. 21, no. 14, p. 4834, 2021.

[44] D. B. Darshan and P. C. R., "Dual-discriminator Conditional Generative Adversarial Network Optimized with Hybrid Momentum Search Algorithm and Giza Pyramids Construction Algorithm for Cluster-Based Routing in WSN Assisted IoT," International Journal of Computer Network and Information Security, vol. 15, no. 5, pp. 96-112, 2023. doi: 10.5815/ijcnis.2023.05.09.

[45] J. Luo et al., "A Secure Transmission Scheme of Sensitive Power Information in Ubiquitous Power IoT," in Proceedings of the 2019 3rd International Conference on Computer Science and Artificial Intelligence, 2019.

[46] Y. Ma et al., "Data preprocessing of agricultural IoT based on time series analysis," in Intelligent Computing Theories and Application: 14th International Conference, ICIC 2018, Wuhan, China, August 15-18, 2018, Proceedings, Part I, 2018.

[47] J. Manhas and S. Kotwal, "Implementation of intrusion detection system for internet of things using Machine Learning Techniques," Multimedia Security, pp. 217-237, 2021.

[48] A. Marchisio et al., "SEVUC: A study on the security vulnerabilities of capsule networks against adversarial attacks," Microprocessors and Microsystems, vol. 96, p. 104738, 2023.

[49] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," Internet of Things, pp. 105-135, 2022.

[50] V. Mohammadi et al., "Trust-based recommendation systems in internet of things: A systematic literature review," Human-Centric Computing and Information Sciences, vol. 9, no. 1, 2019.

[51] H. Naeem, B. M. Alshammari, and F. Ullah, "Explainable artificial intelligence-based IOT device malware detection mechanism using image visualization and fine-tuned CNN-based Transfer Learning Model," Computational Intelligence and Neuroscience, vol. 2022, 2022.

[52] N. K. Narang, "Mentor's musings on the role of Disruptive Technologies and innovation in making healthcare systems more sustainable," IEEE Internet of Things Magazine, vol. 4, no. 3, pp. 80-89, 2021.

[53] R. A. S. Naseri, A. Kurnaz, and H. M. Farhan, "Optimized face detector-based intelligent face mask detection model in IoT using deep learning approach," Applied Soft Computing, vol. 134, p. 109933, 2023.

[54] N. Neshenko et al., "Demystifying IOT security: An exhaustive survey on IOT vulnerabilities and a first empirical look on internet-scale IOT exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, 2019. doi: 10.1109/comst.2019.2910750.

[55] W. Njima et al., "Deep CNN for indoor localization in IoT-sensor systems," Sensors, vol. 19, no. 14, p. 3127, 2019.

[56] B. Nour and S. Cherkaoui, "Unsupervised Data Splitting Scheme for Federated Edge Learning in IoT Networks," in ICC 2022-IEEE International Conference on Communications, 2022, pp. 1-6.

[57] P. R. Maidamwar, P. P. Lokulwar, and K. Kumar, "Ensemble Learning Approach for Classification of Network Intrusion Detection in IoT Environment," International Journal of Computer Network and Information Security, vol. 15, no. 3, pp. 30-46, 2023. doi: 10.5815/ijcnis.2023.03.03.

[58] S. Ojagh et al., "Enhanced air quality prediction by edge-based spatiotemporal data preprocessing," Computers & Electrical Engineering, vol. 96, p. 107572, 2021.

[59] I. Omara et al., "A hybrid model combining learning distance metric and DAG support Vector Machine for multimodal biometric recognition," IEEE Access, vol. 9, pp. 4784-4796, 2021. doi: 10.1109/access.2020.3035110.

[60] M. Osman et al., "ML-LGBM: A machine learning model based on light gradient boosting machine for the detection of version number attacks in RPL-based networks," IEEE Access, vol. 9, pp. 83654-83665, 2021. doi: 10.1109/access.2021.3087175.

[61] M. Patel and M. Bhise, "Raw data processing framework for IoT," in 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 695-699. doi: 10.1109/comsnet.2019.8711477.

[62] S. K. Peddoju and H. Upadhyay, "Evaluation of IoT data visualization tools and techniques," in Data visualization: Trends and challenges toward multidisciplinary perception, 2020, pp. 115-139.

[63] V. Ponnusamy and S. Natarajan, "Precision agriculture using advanced technology of IoT, unmanned aerial vehicle, augmented reality, and machine learning," in Smart Sensors for Industrial Internet of Things: Challenges, Solutions and Applications, 2021, pp. 207-229.

[64] M. S. Pour et al., "Data-driven curation, learning and analysis for inferring evolving iot botnets in the wild," in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1-10.

[65] D. Puthal et al., "Decision tree based user-centric security solution for critical IOT infrastructure," Computers and Electrical Engineering, vol. 99, p. 107754, 2022. doi: 10.1016/j.compeleceng.2022.107754.

[66] W. Rafique et al., "Complementing IOT services through software defined networking and edge computing: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1761-1804, 2020. doi: 10.1109/comst.2020.2997475.

[67] S. Rizvi et al., "Threat model for securing internet of things (IOT) network at device-level," Internet of Things, vol. 11, p. 100240, 2020. doi: 10.1016/j.iot.2020.100240.

[68] P. D. Rosero-Montalvo et al., "A new data-preprocessing-related taxonomy of sensors for iot applications," Information, vol. 13, no. 5, p. 241, 2022.

[69] T. Saba et al., "Intrusion detection system through advance machine learning for the internet of things networks," IT Professional, vol. 23, no. 2, pp. 58-64, 2021. doi: 10.1109/mitp.2020.2992710.

[70] T. J. Saleem and M. A. Chishti, "Deep learning for the internet of things: Potential benefits and use-cases," Digital Communications and Networks, vol. 7, no. 4, pp. 526-542, 2021. doi: 10.1016/j.dcan.2020.12.002.

[71] K. Sha et al., "A detailed review of implementation of Deep Learning Approaches for Industrial Internet of things with the different opportunities and challenges," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 1-18. doi: 10.1109/ic3i56241.2022.10072499.

[72] K. Sha et al., "A survey of Edge Computing-based designs for IOT Security," Digital Communications and Networks, vol. 6, no. 2, pp. 195-202, 2020. doi: 10.1016/j.dcan.2019.08.006.

[73] E. A. Shammar et al., "A survey of IOT and Blockchain Integration: Security perspective," IEEE Access, vol. 9, pp. 156114-156150, 2021. doi: 10.1109/access.2021.3129697.

[74] A. Shamsoshoara et al., "A survey on physical unclonable function (puf)-based security solutions for internet of things," Computer Networks, vol. 183, p. 107593, 2020. doi: 10.1016/j.comnet.2020.107593.

[75] C. Shao et al., "IoT data visualization for business intelligence in corporate finance," Information Processing & Management, vol. 59, no. 1, p. 102736, 2022.

[76] O. Sharma et al., "Windows and IoT malware visualization and classification with deep CNN and Xception CNN using Markov images," Journal of Intelligent Information Systems, vol. 60, no. 2, pp. 349-375, 2023.

[77] S. K. Singh et al., "Machine learning based distributed big data analysis framework for next generation web in IoT," Computer Science and Information Systems, vol. 18, no. 2, pp. 597-618, 2021.

[78] M. Soori et al., "Internet of things for smart factories in Industry 4.0, a review," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 192-204, 2023. doi: 10.1016/j.iotcps.2023.04.006.

[79] S. Sun et al., "Integrating Network Function Virtualization with SDR and SDN for 4G/5G networks," IEEE Network, vol. 29, no. 3, pp. 54-59, 2015. doi: 10.1109/mnet.2015.7113226.

[80] C. S. Suresh et al., "Cognitive IoT-based smart fitness diagnosis and recommendation system using a three-dimensional CNN with hierarchical particle swarm optimization," in Smart Sensors for Industrial Internet of Things: Challenges, Solutions and Applications, 2021, pp. 147-160.

[81] G. Tsaramirsis et al., "A modern approach towards an industry 4.0 model: From Driving Technologies to management," Journal of Sensors, vol. 2022, p. 5023011, 2022. doi: 10.1155/2022/5023011.

[82] A. Varghese et al., "Conception and realization of an IoT-enabled deep CNN decision support system for automated arrhythmia classification," Journal of Intelligent Systems, vol. 31, no. 1, pp. 407-419, 2022.

[83] Y. Wang et al., "Image source identification using convolutional neural networks in IoT environment," Wireless Communications and Mobile Computing, vol. 2021, p. 5790730, 2021.

[84] Mohammad Othman Nassar, Feras Fares AL-Mashagba, "FED-SCADA: A Trustworthy and Energy-efficient Federated IDS for Smart Grid Edge Gateways Using SNNs and Differential Evolution", International Journal of Computer Network and Information Security (IJCNIS), vol. 17, no. 6, pp. 1–15, December. 2025, doi: https://doi.org/10.5815/ijcnis.2025.06.01

[85] M. Zolanvari et al., "Machine learning-based network vulnerability analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, 2019. doi: 10.1109/jiot.2019.2912022.

[86] M. Zorzi et al., "From today's Intranet of things to a future internet of things: A wireless- and mobility-related view," IEEE Wireless Communications, vol. 17, no. 6, pp. 44-51, 2010. doi: 10.1109/mwc.2010.5675777.

[87] Nassar, M. O., & Al-Mashagba, F. F. (2025). Optimal ensemble learning with meta-heuristics for multiclass classification of syscall-binder interactions in mobile applications. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 16(1), 26–48. https://doi.org/10.58346/JOWUA.2025.I1.002

[88] Al Ghamri, M., Ibrahim, D., Sihwail, R., & Shehab, M. (2024). Whale Optimization Algorithm for Feature Selection Enhances Classification in Malware Datasets. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE42024233

[89] Ibrahim, D., Sihwail, R., Arrifin, K. A. Z., Abuthawabeh, A., & Mizher, M. (2023). A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm. *Symmetry*, 15(7), 1305. https://doi.org/10.3390/sym15071305

[90] Shannaq, F., Shehab, M., Alshorman, A., Hammad, M., Hammo, B., & Al-Omari, W. (2025). Exploring Metaheuristic Optimization Algorithms in the Context of Textual Cyberharassment: A Systematic Review. *Expert Systems*, 42, e13826. https://doi.org/10.1111/exsy.13826

[91] Daoud, M. S., Shehab, M., Abualigah, L., et al. (2023). Hybrid Modified Chimp Optimization Algorithm and Reinforcement Learning for Global Numeric Optimization. *Journal of Bionic Engineering*, 20, 2896–2915. https://doi.org/10.1007/s42235-023-00394-2

AUTHORS' PROFILES

Dr. Feras almashakbah is an Associate Professor of Artificial Intelligence in Jerash University; he received his Ph.D. in Computer Information System/ Artificial Intelligence in 2009. Dr. Almashakbah has 15 years' teaching experience. He has published 30 scientific research publications in international peer reviewed journals and conferences. Dr. Almashakbah is an editorial board member for 3 international peer reviewed journals.

Dr. Mohammed Nassar is an Associate Professor of Computer Information System in Amman Arab University; he received his Ph.D. in Computer Information System/ Information Retrieval in 2009. Dr. Nassar has 15 years' teaching experience. He has been working at Amman Arab University since 2010. His is the Manager of eLearning center and the director of marketing department in Amman Arab University. He occupied different leading positions at the university: head for Computer Information System department, and computer center manager in Amman Arab University. He has published 40 scientific research publications in international peer reviewed journals and conferences. Dr. Nassar is an editorial board member for 4 international peer reviewed journals.

Dr. Essam S. Hanandeh Associate Professor, Essam Said Hanandeh received the degree of a Ph.D. in CIS in 2008, he joined Zarqa University in Jordan in 2008 up to 2024 then joind to Jerash university in 2025. Associate Professor Essam Said Hanandeh has been worked for 15 years as programmer & System Analyst. He published over 30 research paper in international journals and conferences. He can be contacted at E-mail: e.hanandeh@jpu.edu.jo