# Screening Cyberattacks and Fraud via Heterogeneous Layering

ABDULRAHMAN ALAHMADI
Department of Computer Science and Information
Taibah University, Saudi Arabia

***Abstract*—On the Internet of Things (IoT) age, intelligent equipment is employed to give effective and dependable utilization of applications. IoT devices may recognize and provide extensive information while also intelligently processing that data. Data systems, systems for control, plus sensing are growing increasingly vital in contemporary manufacturing processes. The amount of internet of things gadgets and methods used is growing, that has culminated in a rise in assaults. Such assaults have the potential to interrupt international activities and cause major financial losses. Multiple methods, including Machine learning (ML) in addition to Deep Learning (DL), are being utilized for identifying cyberattack. In this investigation, researchers offer an ensemble staking approach that is strong strategy in ML for detecting assaults via the Internet of Things having excellent accuracy. Tests were carried out using three distinct information: credit card data, NSL-KDD, and UNSW. Single fundamental classifications were beaten by the suggested layered ensembles classification. The results show that the cyberattack detection model in this research possessed a $95.15\%$ accuracy percentage, while the credit card fraud detection model achieved a $93.50\%$ accuracy percentage.**

***Keywords*—Fraud; Internet of Things (IoT); Deep Learning (DL); ensemble; stacking; cyberattack; Machine Learning (ML)**

## I. Introduction

Information has grown into an indispensible component of our daily life. Depending on gadgets, especially the World Wide Web, is growing increasingly vital as tech and the Internet become increasingly integrated into all aspects of our daily lives, which has raised interest in Network-based methods, particularly the Internet of Things (IoT). The Internet of Things (IoT) enables devices that are connected to share information and engage for a particular reason without no requiring human involvement [33]. These machines have several characteristics and advantages that permit between machines connections, allowing a broad spectrum of applications and developments to emerge [22]. The Web and the Internet of Everything has grown into an increasingly popular subject over the past ten years due to its capacity to simplify people's life simpler, provide greater satisfaction to clients and organizations, and promote independence in their jobs. Notwithstanding these benefits, the Internet of Things has various limits and impediments which might inhibit its ability to attain its maximum potential. As stated by the authors of [10] many IoT applications fail to adequately consider user confidentiality or security, resulting in an acute issue. In connected devices, there are two sorts of attacks: passive and active. Passive assaults do not hinder by means of records and are employed to gather classified data while being noticed. Active assaults are directed at systems and perform unlawful activities which jeopardize the computer's privacy and security. As IoT nodes and gadgets are expected to facilitate most financial transactions, fraudulent assaults have emerged as one of the predominant issues. The proliferation of e-commerce dealings and the advancement of IoT applications have exacerbated the problem of financial fraud. As reported in [15] $87\%$ of businesses and vendors currently accept electronic payments, a figure that is poised to increase further with the proliferation of mobile wallets and the enhanced payment capabilities of IoT devices. Consequently, these systems are increasingly susceptible to fraudulent attacks. Electronic payment fraud can manifest in various manners, but the most prevalent is the unauthorized acquisition of certification numbers or credit card details. This type of fraud can occur physically by physically stealing the card and employing it for deceitful transactions or virtually by gaining access to card or payment information electronically and executing fraudulent transactions. In the realm of IoT, virtual credit card fraud is particularly widespread, as it doesn't necessitate the physical presence of the card. Perpetrators are consistently exploring novel methods to obtain critical data, including verification codes, card numbers, and expiration dates, for the purpose of executing fraudulent transactions, necessitating the creation of Systems and conceptual frameworks capable of identifying and thwarting such fraudulent activities. The issue of cyber and fraudulent attacks can result in incalculable harm. Anticipated statistics indicate that over 22 billion Internet of Things (IoT) devices are projected to be connected to the web in the coming years [28]. This underscores the need to identify approaches and create models to provide secure and reliable IoT services to both consumers and enterprises. Consequently, numerous ML and DL models have been introduced for the purpose of identifying fraudulent and malicious attacks. As contrasted with the known starting point models, several of these algorithms use collective learning, whereby combines multiple classifiers together to offer greater overall accuracy.

An examination of obtainable solutions revealed primary constraints, namely the absence of validation for the suggested remedies and the uncertainty associated with the application of new data to generalization.

Thus, the contribution of this article introduces an innovative stacked ensemble model that employs multiple ML models to effectively identify various cyberattacks and fraudulent attacks. In our stacked ensemble strategy, we tested numerous ML algorithms, utilizing both the most effective and least effective models to assess the performance enhancement achieved by incorporating baseline models into our stacked ensemble approach. Our approach amalgamates the strengths and capabilities of different algorithms into a single, resilient model. This ensures the optimal combination of models to

address the issue and enhance generalization when making detections. To validate our ensemble algorithm, three datasets were employed. The experimental outcomes for the Credit Card Fraud Detection, NSL-KDD, and UNSW datasets reveal that the proposed stacked ensemble classifier elevates generalization and surpasses comparable endeavors in existing literature.

This paper is structured as follows: Section II delves into related research. Section III elaborates on the stacking methodology. Section IV showcases the experimental results. Finally, Section V concludes the paper, accompanied by a discussion of future directions.

## II. Related Works

### A. IoT Strata

When designing an Internet of Things (IoT) structure, establishing a framework for various hardware functionalities facilitates the establishment of connections and the provisioning of IoT services across diverse domains. The IoT architecture essentially comprises three primary tiers: insight, request and network [4], [13].

*1) Sensory or bodily stratum:* The senses strata are formed by an actual strata and a medium-access controlling stratum in the framework of the IoT [3]. The physical stratum is largely concerned about physical factors, detectors, and devices that send and receive information via different kinds of communication like as RFID, Zigbee, or Wirelessly. Equipment that is physical communicates with systems at the medium-access control level [36].

*2) Networking stratum:* IoT devices depend on the communication layer for knowledge and information communication and transit via various transfer methods. Both clouds and server assets are used for preserving and analyzing data inside the networks layer as well as within the internet level and the following level [38].

*3) Application or web layer:* People utilize amenities via online and mobile apps at the last tier of IoT systems. The IoT has become prevalent in the present, modern world due to current developments and uses for intelligent devices. Because of the IoTs and its broad range of applications, different areas such as homes, businesses, transportation, medical care, higher learning, farming, industry, trade, and supply of energy have begun to embrace smarter technology [13].

### B. Categorization of Attacks

There are two primary categories of IoT security threats: cyberattacks and physical assaults. In a cyberattack, hackers influence the scheme to either pilfer, erase, modify, or obliterate data from IoT device users. Conversely, a physical assault results in physical harm to IoT devices [16]. In the subsequent sections, we discuss multiple types of cyberattacks that occur within the IoT's three principal layers [18], [24]. Fig. 1 illustrates some ordinary IoT attack in different layers:

1. DoS assault: Denial of Connectivity disruptions, known as DoS disruptions,, disrupts system amenities by generating numerous superfluous needs. DoS assaults are widespread in IoT applications, particularly affecting low-end IoT devices that are more susceptible to such attacks [8].
2. Blocking assaults: Blocking assaults, which are a subclass of DoS assaults, interrupt the path of communication. Inbound signals interfere with wireless data transfer, increasing congestion in networks and harming users [19], [34].
3. Networks injection: Thieves be able to use this method to establish a gadget that masquerades as an IoT data transmitter and sends data in the manner that it had been a member of the IoT network [7].
4. Humanity to between breaches: In this kind of situation, criminals try to get into the network's communications through a link directly to a third gadget [19]. Because IoT network elements are each tied to the portal for interactions, if the server is targeted, every device that send and obtains data might be hacked [34].
5. Harmful entry assaults: A hacker may insert scripts that are malicious into a program, allowing them to be accessed by all users. Malicious material can be saved in files, user discussions, or any other type of storage system. These attacks cause financial losses, higher power usage, and network connectivity degradation [45].
6. Information tampering: To obtain complete control, a perpetrator must physically get accessibility to an IoT gadget, which may involve causing harm or a substitute of the nodes on the gadget itself. Intruders alter customer details in order to compromise their privacy, focusing on smart gadgets that record data on location, health state, billing, and other critical factors [37].
7. Phishing and Sibyl assaults: Phishing and Sybil assaults in IoT systems users without their knowledge and acquire unauthorized access to the systems. It is critical to remember that TCP/IP fails to offer adequate safety, leaving IoT gadgets especially susceptible to fraud attempts [42], [20].
8. Knowledge leakage: gadgets with internet access hold delicate and proprietary data. If this information becomes available, it could be misused. Realizing the shortcomings of an application raises the chance of data leaking [27].
9. Hazardous material: If a hacker discovers a weakness in a program, such as an SQL injection and bogus information insertion, he or she may post malware. Infected code is illegally introduced into computers or online scripts, resulting in unintended consequences, privacy violations, or computer operating system harm [2].
10. Rebuilding the model: By hacking systems that are embedded, hackers can get confidential data. Cybercriminals exploit this strategy to discover data that software developers have mistakenly left behind, such as encoded passwords and flaws, they then may utilize for additional assaults on computer chips [27].

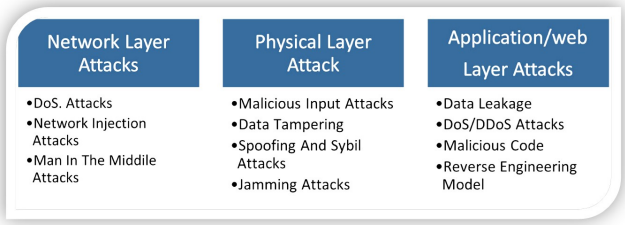


Fig. 1. Categorization of cyber assaults determined by the strata of the IoT.

### C. Identification of Cyberattacks in IoT Networks

In this segment, we explore a range of ML and DL approaches as prospective remedies for identifying cyber intrusions within IoT systems. Tables I and II furnish a summary of the ML and profound learning strategies practical in the realm of IoT for the purpose of spotting cyber assaults, correspondingly. Anthi et al. [6] used controlled learning to create a three-tier interruption discovery system, or IDS, for intelligent homes. The system finds hateful packets of data by collaborating among the three strata in the suggested IDS framework. Al Zubi et al. developed a mental ML-assisted identification of attacks system (CML-ADF) to protect health care data [5]. As contrasted to other methods in use, they used extreme machines learning (EML) as the system for detection to improve precision, assault forecasting, and performance. A technique for detecting cyber vulnerabilities in IoT-based elegant metropolis applications was proposed in an additional study [30]. A separate investigation proposed an attack detection structure for systems that offer suggestions through the development of a deterministic portrayal of invisible variables for showing multi-model facts [27]. When the suggested structure was compared with existing models, it was found to be more capable of detecting anomalies in recommendations. A single study presented a linear categorization iterative method for accurately categorizing cyberattacks from numerous sources at a minimal cost. The researchers of [41] used a step-wise individually regular classify on a multi-source collection of real-world information concerning cybersecurity to identify infections and their sources. Cristiani et al. proposed the Fuzzy Intrusion Detection System for IoT Networks (FROST), which was intended at avoiding and discovering various types of cyberattacks, but it had a high mistake probability and needed modification [12]. Rathore et al., on the other hand, provided an innovative identification approach built upon the ELF-Based Fuzz C-Means (ESFCM) method that utilized the cloud computer concept. This technique can detect attacks at the system's edge while also addressing distribution, scaling, and latency issues. Jahromi et al. developed a two-tier ensembles assault identification and blame arrangement for industrial monitoring systems in a separate study. Deep visual intelligence is used in the first tier to discover regulatory imbalances, while deep neural networks (DNNs) are used in the subsequent stage to assign observable attempts. Singh et al. developed a Multi-Classifier internet alerting system (MCIDS) using a DL technique which identifies high-accuracy monitoring, assessment, DoS, fuzzers, overall, flaws, and port codes invasions. Battista et al. tackled the problem of data manipulation via wireless networks, which endangered physical and virtual systems. They used a new approach to secure their control system by encoding its results matrix structures to generate a hidden structure, using Fibonacci p-sequences and key-based mathematics sequential. Diro et al. proposed utilizing a DL engine to detect subconscious patterns in information that comes with the goal to avoid assaults in the world of IoT in a different investigation. They claim that this model is better than traditional artificial intelligence models at identifying attacks. Moussa et al. discovered cyber attacks in the automobile sector amid communication of information among the cloud or end-user devices. They used an altered form of a stacked autoencoder for precisely recognizing these specified incursions. Soe et al. developed a lightweight security discovery system (IDS) based on the logistic model of the tree (LMT), the random forest (RF) classifiers, J48, and a Hoe ding trees (VFDT) in a different paper. They pioneered a creative method that was called correlated-set thresholding on the ratio of gain (CST-GR), which was used uniquely in this study. Finally, Al-Haija et al. developed the IoT-base Security Detection and Class System Using a intricacy Neural Network (IoT-IDCS-CNN), an automated learning-based detecting and categorization method. The technique is divided into three subsystems: the design of features, learning features, and data classification.

### D. Detection of Fraudulent Activities in IoT Systems

Mishra et al. [23] proposed a k-fold linear regression method for identifying and preventing criminal activity in IoT environments. The k-fold approach is used to generate numerous subdivisions of money movements prior applying your logistic regression method. The authors offer an approach for detecting abnormalities in IoT financial conditions in [38]. The method detects illegal behaviours such as Remote-to-Local (R2L) assaults by identifying unusual and deceptive acts using a two-tier package that employs the K-Nearest Neighbour and Nave Bayes classifiers. A subsequent study [26] proposes an alternate method for detecting fraud in IoT systems by employing neural network technology and predictive algorithms to process large amounts of statistical info and detect activities that are fraudulent. The researchers of [11] used a Node2Vec technique to learn and encode finance networking graph attributes in a low-dimensional scalar. This allowed the suggested approach to produce precise projections and categorise portions of data from huge databases efficiently and precisely using neural networks. The development of a deep convolution neural network model that recognizes criminal behavior is divided into several phases [44]: pre-model use (data preprocessing), designs implementation (using the convolutional neural network), and post-model being applied (obtaining the results). According to mastercard behavior, another investigation [29] proposed an unattended independent translation method that was taught to construct a simpler representation of the input training samples with decreased dimensions. The work in [43] offered an innovative technique that combines Hunt's and Luhin's methods using choice trees. Card numbers are verified utilizing Luhn's approach, and the correct invoicing relocation is confirmed using the location verification requirement to determine if it matches the package's destination. If the addresses used for payment and shipping corresponds, the order is deemed likely to be authentic. Assistance Vector Machines, simple neural

TABLE I. A STUDY OF ARTIFICIAL INTELLIGENCE ALGORITHMS FOR DETECTING CYBERATTACKS

| Ref. | Method | Evaluation Metric | Dataset | Application | Limitation |
|---|---|---|---|---|---|
| [27] | Partially Oversaw ML. | Area under the curve | MovieLens, BookCrossing, LastFM | Recommender Systems (Sequential Attack) | The suggested approach's effectiveness is not demonstrated. |
| [6] | Various Oversaw ML | F- measure, precision, and recall | Network activity data | Intrusion Detection system for smart homes | Absolute precision cannot be evaluated. |
| [5] | Cognitive ML | Reliability of forecast ratio, transmission expenses, latency, and effectiveness | Information from a trusted device | Cyberattack detection in Healthcare | Evaluation method is not clear |
| [30] | Artificial Neural Network | Accuracy, recall, precision, and F1 score | UNSW NB15 | Cyberattack detection for smart cities | A small sample was utilised to test the approach used. |
| [41] | ML | Accuracy | MSRWCS | Cyberattack detection for Multisource Applications | There is insufficient verification statistics. |
| [12] | ML (Fuzzy Clustering) | Classification rate | UNSW-NB15 | Cyberattacks on IoT Networks | There is insufficient verification statistics. |
| [31] | Partially - Oversaw Algorithm | Accuracy, PPV, sensitivity | NSL-KDD | Using Integrated Protection for Identifying Threats in IoT Networks | There will be no experiments on actual data. |

TABLE II. A STUDY OF NEURAL NETWORK ALGORITHMS FOR DETECTING CYBERATTACKS

| Ref. | Method | Evaluation Metric | Dataset | Application | Limitation |
|---|---|---|---|---|---|
| [17] | Shallow Neuronal Networks and Two-Level Selection Tree-Based Deep Participation Training | Accuracy, recall, precision, and F score | SWaT and Mississippi state University Gas Pipeline Data | Identification and causation of cyberattacks in gas pipelines and water purification facilities | High computational cost |
| [39] | Convolution Neural Networks (CNN) | Accuracy and false positives | UNSW-NB15 | Multi-Classifier instruction Detection System (MCIDS) | There is not any assessment information displayed. |
| [9] | Fibonancci p-series and Key-Based Numeric Sequence | Accuracy, precision, recall, F1 measure | NSL-KDD | Tampered data detection in water distribution system | There is little data regarding the low-depth model. |
| [14] | DL Model | Accuracy, precision, recall, F1 score, and F2 score | NSL-KDD | Attack detection in social IoT | The information is restricted to a particular area. |
| [25] | Systemic Neural Network with Autoencoder as Feature extractor | Accuracy | NSL-KDD | Hacking monitoring in vehicle IoT cloud fog computing | There is insufficient verification data. |
| [40] | Correlated Set Thresholding on Gain Ratio (CST-GR) | Accuracy and processing time | BoT-IoT | Lightweight instruction detection in IoT systems | Mainly detects three types of assaults |
| [1] | Convolution Neural Networks (CNNs) | K-fold cross-validation, TP, TN, FP, and FN | NSL-KDD | In the IoT ecosystem, message recognition and categorization | There were no outcomes of tests in applications in reality. |

TABLE III. PROPORTIONAL PSYCHOANALYSIS OF FRAUD FINDING APPLICATIONS

| Ref. | Method | Evaluation Metric | Dataset | Application | Limitation | Metric value |
|---|---|---|---|---|---|---|
| [23] | k-Fold Computing and Statistical Regression | Accuracy, recall mean, and recall score | 2015 European Data | Fraud prediction in IoT smart societal environments | High computational cost | (%97.0), (%61.90), (%96.11) |
| [26] | Two-Tier Dimension Reduction and Classification Model | Detection rate and false alarm rate | NSL-KDD dataset | Anomaly detection in financial IoT environments | Prone to missing information | (%84.86), (%4.86) |
| [11] | ML and Artificial Neural Networks Model | F-measure | Real transaction data in IoT environment in Korea | Fraud detection in financial IoT environments | Not enough validation metrics | (%74.75) |
| [44] | Node2vec | Precision, recall, F1-score, and F2-score | Fraud samples obtained from a large Chinese provider | Fraud detection in telecommunications | Data are limited to a single region | (%75), (%65), (%70), (%68) |
| [29] | CNN | Accuracy | Real-time credit card fraud data | Fraud detection in credit cards | Not enough validation metrics | (%96.9) |
| [43] | Self-Organized Map Fraud detection in credit cards | NA | Single credit card data | Fraud detection in credit cards | No performance evaluation | |
| [35], [32] | Decision Tree Model | NA | Single credit card data | Fraud detection in credit cards | No performance evaluation | |
| [21] | Clustering | Recall, precision, and FPR | Purchases submitted in actual life on a website that sells electronic goods | Fraud detection in e-commerce | Falsely classifies cancelled orders | (%26.4), (%35.3), (%0.1) |

nets, Behavioral Genetics Planning, and Parametric Neural Research were among the data mining techniques used in [35], [32]. In [21], a method was developed that used clustering agglomeration to arrange orders that were bogus from a similar category. Table III contains a comprehensive overview of identification of fraud systems. Tables of comparisons for cybercrime and fraudulent identification application, it is evident that the primary constraints lie in the absence or sole reliance on a single validation metric and the use of a singular dataset. This diminishes the reliability of these applications since it remains unclear how well the models execute by the test data. Moreover, the utilization of a solitary dataset does not authenticate the model's performance adequately, given the dynamic and diverse nature of cyberattack and fraud data. It is conceivable that a model may perform effectively on one dataset but falter when applied to another dataset containing different or more extensive features. Additionally, most research in the literature involves optimizing a single model for superior test performance. We identified this as an area of opportunity where we could harness multiple high-performance models to construct a more robust model or employ a stacked generalization algorithm to enhance the performance of multiple weaker models. The diagram of the stacking technique in Fig. 2 it consist of the base models and the meta-learner. The base models are individual machine learning models that fit and make predictions on the training data. The second layer of the stacking ensemble model is the meta-learner. The meta-learner takes input from the base models' output and learns how to make new predictions based on the predictions of the base models.

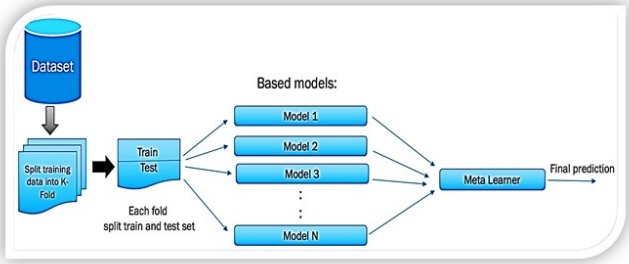


Fig. 2. Diagram of the stacking technique.

## III. Methodology

In this investigation, researchers offer a collective anchoring approach for detecting assaults via the Internet of Things having excellent accuracy. Tests were carried out using three distinct information: credit card data, NSL-KDD, and UNSW. Single fundamental classifications were beaten by the suggested layered ensembles classification.

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage. For example, write "15 Gb/cm$^2$ (100 Gb/in$^2$)." An exception is when English units are used as identifiers in trade, such as "$3^{1/2}$-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength $H$ is A/m. However, if you wish to use units of T, either refer to magnetic flux density $B$ or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m$^2$."

K-Nearest Neighbours (KNNs), Decision Trees (DTs), Gaussian Naive Bayes (GB), support vector machines (SVMs), AdaBoost (AB), Gradient Boosting (GB), Random Forest (RF), Extra Trees (ET), Multi-Layer Perceptron (MLP), and a technique called classification were evaluated as essential models. Researchers used various methods of ML to evaluate our basic models on an invoice theft dataset and two separate cyberattack populations. We documented the success of any model to each dataset and evaluated how achievement increased when building ensemble approaches were used, encompassing the pair of best-performing along with worst-performing approaches. In addition, researchers tested multiple meta-learners to see whether they impacted efficiency and opted for the most excellent-acting meta-learner for every data. We recorded the outcomes of multiple ML methods, including MLP Classifier, XGBoost, and gradient booster, and chose the most efficient and correct models as the master learner in every case study. The mathematical complexity of our stacking strategy is completely determined by the basic framework with the greatest amount of computing time (i.e., Tmax). The stacked model's mathematical expense is given by the equation O(Tmax + t), where t is the extra linear time caused by the meta-learner. As a result, the whole stacking approach has good adaptability for large datasets.

### A. Data Processing

We utilized alike processes to prepare all datasets. Initially, we visually inspected and examined each dataset to ascertain the quantity of characteristics, records, missing values, and categorical features. We then conducted an analysis of feature correlations to eliminate redundant features from the datasets. Categorical features were encoded, and normalization was applied to standardize the features on a common scale. For the fraud dataset, we partitioned the data into training and testing sets using a $75-25\%$ split, whereas the cyberattack datasets were already divided. Additionally, the fraud detection dataset exhibited a significant class imbalance, with the fraud class having far fewer instances than the non-fraud class. As a consequence, under sampling was used to balance the class distribution. We used a ten-fold cross-validation technique when creating the test set. The basic model' forecasts was subsequently utilized for developing the final model using the training information.

## IV. Experimental Results

### A. Datasets

Researchers used a total of three data sets for learning the models we built. The NSL-KDD and UNSW-NB15 datasets were used to train an ensemble model for identifying intrusions. The combined model with identifying fraud, in the opposite end of the spectrum, were solely generated with one database due to the lack of alternative datasets with a significant amount of data for conditioning a sophisticated

model. We examine all the databases used in the current investigation in detail follows.

*1) NSL-KDD:* The dataset provided by the NSL-KDD is made up of data that depict online activity as seen by a rudimentary intrusion detection network. These data show patterns of traffic observed by legal intrusion detection systems. Every entry in the aforementioned set has 43 properties, 41 of which are connected to the entered traffic information, while the two additional ones are tags. The first label shows when the traffic is normal or reflective of an assault, and the second label reflects the magnitude of the communication input. The NSL-KDD dataset is a revised variant that replaces the original KDD'99 dataset, which included a large number of duplicates. For the benefit of users, the dataset's creators painstakingly separated into separate sets for training and testing. The set for training has 125,973 documentation, whereas the test set has 11,272 records. This dataset was gathered in 1999 in the course of the Information Discovery as well as ML contest to acquire genuine web traffic statistics. In addition, the NSL-KDD the test and training sets contain a large number of documents, which enables thorough testing requiring the expense of selection at random. This guarantees that the examination reports for multiple research initiatives stay consistent and easily comparative.

*2) UNSW-NB15:* The UNSW-NB15 collection contains unprocessed packets from the network created by the IXIA PerfectStorm tool in the Cyber Range Lab, located at the College of New South Wales Capital. It is intended to combine actual current network operations with current artificial assault behaviours. The data set was created by capturing 100 GB of raw web traffic with tcpdump. Ffuzzers, analysis, backdoors, DoS, exploits, broad assaults, observation, shellcode, and grubs are among the nine types of attacks covered. There are a total of 2,540,044 variables in the collection. For the training set, a subset of 175,341 records was selected, while another subset of 82,332 records was designated as the testing set. These subsets consist of records representing normal network activity and various attack types.

*3) Database for detecting credit card theft:* The information in this dataset concentrates on financial card purchases made in September 2013 by European cardholders. During a two-day time frame, 492 of the 284,807 transactions that took place was fake. Additional preparation measures were required to even out the category distributions in this data set due to the extreme class imbalance, with forged payments encompassing just 0.172 percent of total trades. The findings were obtained as part of a large data mining and prevention of fraud investigation partnership between the Worldline and the Machine Translation Group at Université Libre de Bruxelles (ULB). Due to concerns over privacy, the info was subjected to a PCA evaluation but only the numbers of principle components were retained, with a couple of two columns: "Amount" and "Time." The "Time" column indicates the time elapsed since the first transaction, while the "Amount" column specifies the transaction amount, which is relevant for cost-sensitive analysis. Due to data sensitivity, the actual attributes and transaction data were inaccessible.

### B. Experimental Results

Table IV shows the consequences of detecting fraudulent use of credit cards utilizing community layering. The studies were carried out depending on the degree of efficacy for different artificial intelligence algorithms. We created a variety of starting points and used a 10-fold cross-validation procedure to find the best and worst versions for participation in level 0 of the layered group approach. For each dataset, several supervised learning procedures were chosen as the starting point. Random Forest, XGBoost, MLP, and gradient strengthening classifiers, for example, appeared from among the top-performing models for detecting financial card fraud. In contrast, with the NSL-KDD and UNSW information sets, the best classifiers were Decision Tree, XGBoost, and Random Forest. Furthermore, as shown in Tables IV to VII, we evaluated the amount of training duration for every single modelling and collective stack. The receiver operating characteristic (ROC) curves of the dataset produced by the NSL-KDD are shown in Fig. 3, while the ROC curves for the UNSW and debit card samples are shown in Fig. 4 and 5, correspondingly. Tables IV to VII show that the top-performing predictive algorithms require more training time than the low-performing basic designs. The ROC curve and reliability showed enhancements however the best method for a particular situation is dependent on the conditions. As economy is of the essence, smaller however poorer powerful ML procedures might become favored, whereas performance-driven scenarios may need the deployment of the best-performing machines training methods.

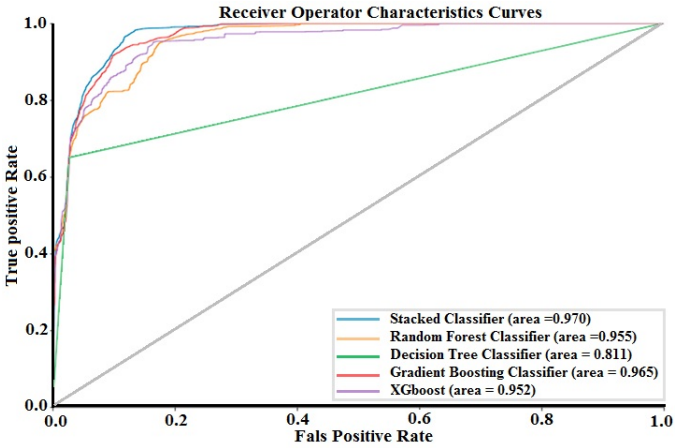


Fig. 3. The NSL-KDD Information's ROC Profile.

## V. Discussion

The results shown in Table IV demonstrate how our layered combined model beat all of the initial models, detecting credit card transaction fraud with a 93.5% reliability. As both of the group models according to two distinct base models were compared, the weak base group model slightly outperformed the powerful base composite model. Tables V to VII illustrate how well each of the stacked set of models for the identification of cyberattack Notably, as opposed to the predictive model developed with the whole NSL-KDD dataset (78.87%), the combination of models learned with 20% of the NSL-KDD information outperformed (81.28%). This disparity could be related to excessive fitting, which occurs

TABLE IV. DETECTING PAYMENT CARD ABUSE VIA GROUP LAYERING

| Model | F1 Score | Sensitivity | Accuracy | Precision | Specificity | Training time |
|---|---|---|---|---|---|---|
| Ensemble Stacking (Poor) | 0.938931 | 0.911111 | 0.934959 | 0.968504 | 0.963964 | 8.42 |
| Further Trees Classifier | 0.906883 | 0.82963 | 0.906504 | 1.000000 | 1.000000 | 8.34 |
| Choice Tree Classifier | 0.898551 | 0.918519 | 0.886179 | 0.879433 | 0.864847 | 0.19 |
| Gaussian NB | 0.916996 | 0.859259 | 0.914634 | 0.983051 | 0.981982 | 0.05 |
| Ensemble stack (Strong) | 0.934866 | 0.903704 | 0.930894 | 0.968254 | 0.963964 | 21.71 |
| Arbitrary Forest Classifier | 0.924901 | 0.866667 | 0.922764 | 0.991525 | 0.990991 | 3.06 |
| MLP Classifier | 0.939394 | 0.918519 | 0.934959 | 0.96124 | 0.954955 | 11.86 |
| XGB | 0.928302 | 0.911111 | 0.922764 | 0.946154 | 0.936937 | 1.37 |
| Gradient boost Classifier | 0.923664 | 0.896296 | 0.918699 | 0.952756 | 0.945946 | 2.1 |

TABLE V. HETEROGENEOUS LAYERING WAS USED TO DETECT CYBERATTACKS ON 20% OF THE NSL_KDD SAMPLE

| Model | F1 Score | Sensitivity | Accuracy | Precision | Specificity | Training time (second) |
|---|---|---|---|---|---|---|
| Ensemble Stack (Poor) | 0.842655 | 0.884194 | 0.812819 | 0.84843 | 0.719406 | 37.95 |
| Arbitrary Forest Classifier | 0.783889 | 0.708138 | 0.778665 | 0.877789 | 0.870968 | 4.5 |
| Further Tree Classifier | 0.718251 | 0.571987 | 0.74562 | 0.965017 | 0.972862 | 14.33 |
| Gaussian NB | 0.676864 | 0.900235 | 0.512752 | 0.542305 | 0.005632 | 0.89 |
| Ensemble Stacking (Strong) | 0.781112 | 0.655859 | 0.791306 | 0.965497 | 0.969215 | 273.48 |
| Choice Tree Classifier | 0.765857 | 0.634375 | 0.779774 | 0.9666092 | 0.970754 | 1.32 |
| Gradient Boost Classifier | 0.756462 | 0.623047 | 0.772233 | 0.962583 | 0.968189 | 12.46 |

TABLE VI. SHOWS THE RESULTS OF ATTACK DETECTION USING BATCH STACK BASED ON THE NSL-KDD DATASET

| Model | F1 Score | Sensitivity | Accuracy | Precision | Specificity | Training time (second) |
|---|---|---|---|---|---|---|
| Ensemble Stack (Poor) | 0.761161 | 0.626432 | 0.776215 | 0.969723 | 0.974153 | 849.76 |
| Arbitrary Forest Classifier | 0.748626 | 0.610224 | 0.766723 | 0.968225 | 0.973535 | 22.14 |
| Further Trees Classifier | 0.695382 | 0.540949 | 0.730216 | 0.973223 | 0.980332 | 67.65 |
| Gaussian NB | 0.070925 | 0.036858 | 0.450319 | 0.936634 | 0.996705 | 0.61 |
| Ensemble Stack (Strong) | 0.772649 | 0.646303 | 0.78349 | 0.960398 | 0.964782 | 1669.04 |
| Choice Tree Classifier | 0.77757 | 0.648874 | 0.78868 | 0.969948 | 0.973432 | 8.71 |
| XGB Classifier | 0.785367 | 0.659939 | 0.794668 | 0.969659 | 0.972711 | 112.53 |
| Arbitrary Forest Classifier | 0.751705 | 0.614198 | 0.769029 | 0.968543 | 0.973638 | 84.79 |

TABLE VII. HACKING DETECTION USING BATCH LAYERING ON THE UNSW SAMPLE

| Model | F1 Score | Sensitivity | Accuracy | Precision | Specificity | Training time (second) |
|---|---|---|---|---|---|---|
| Ensemble Stack (Poor) | 0.96204 | 0.959357 | 0.951536 | 0.964738 | 0.937624 | 565.65 |
| Arbitrary Forest Classifier | 0.962027 | 0.959333 | 0.951521 | 0.964737 | 0.937624 | 69.65 |
| Further Trees Classifier | 0.909339 | 0.995659 | 0.87291 | 0.836791 | 0.65456 | 94.49 |
| Gaussian NB | 0.622117 | 0.470039 | 0.634471 | 0.919672 | 0.926969 | 1.39 |
| Ensemble Stacking (Strong) | 0.961333 | 0.95892 | 0.95062 | 0.963758 | 0.935855 | 690.82 |
| Random Forest Classifier | 0.962202 | 0.959939 | 0.951722 | 0.964476 | 0.937106 | 155.37 |
| XGB Classifier | 0.947926 | 0.952179 | 0.933032 | 0.943711 | 0.898973 | 108.76 |
| Decision Tree Classifier | 0.951049 | 0.949827 | 0.93741 | 0.952274 | 0.915322 | 12.82 |

when a model seeks to account for a huge amount of data points, resulting in decreasing precision and efficiency owing to noise. Whereas, generalization refers to a neural network model's capacity to give reliable outcomes while adjusting to unfamiliar inputs. Filtering on an information set can produce precise and consistent results. As consequence, we infer that modeling on the complete NSL-KDD dataset resulted in over fitting and inadequate results on test data, whereas training on approximately $20\%$ of the dataset resulted in greater generalization and efficient warnings of attacks. When evaluating the outcomes of our packed combination theory for cybercrime discovering the UNSW-NB15 dataset outperformed the NSL-KDD dataset ($81.28\%$). In general, we found that stacking combined models with weakly anchored models performed better compared to those with solid base predictors. This might be ascribed to the meta-learner's increased learning capacity from any weak basis model compared to strong base designs, which are currently extremely accurate. This pattern was consistent throughout all tests, with the exception of Table VI, where each layered model featuring a solid foundation models beat those with weakened foundation models marginally. That trend was also evident in the multilayered composite models' training times. When overlaid forms with poor basis models were put next to alternatives with solid foundation designs, all of them had lower times for training. Researchers found that the top stacking ensembles model's preparing occasion was closely connected to the cumulative readiness occurrence among its bottom versions. Additionally, We discovered found the region beneath the ROC curve (AUROC) for each stacked ensemble model was either higher or equivalent to that of their respective base models, confirming the superior performance of our stacked ensemble classifier.

## VI. CONCLUSION AND FUTURE WORK

The speedy expansion of IoT growth and practice has increased data processing, making applications vulnerable to various cyberattacks. Cybersecurity remains a significant concern in IoT applications. Protecting information as of interruption

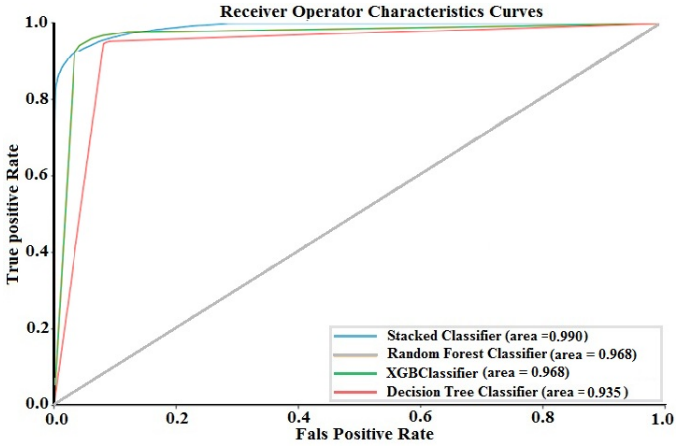


Fig. 4. The ROC curve for the UNSW dataset.

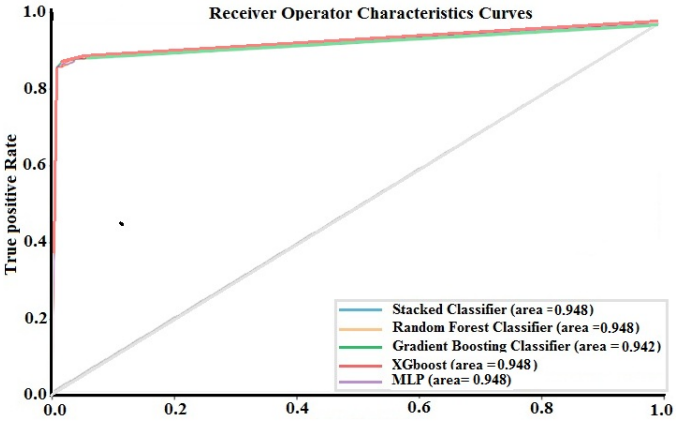


Fig. 5. The ROC curve for the credit card information.

attack and enhancing industry discovery system is crucial. Cyberattacks pose a substantial threat in IoT applications across all industries. We divided principal assaults into three main IoT levels and highlighted cutting-edge technologies to identify and attribution. ML and DL models were highlighted and their strength and confines identified. DL approaches tended to outperform traditional ML models. The NSLKDD and UNSW-NB15 datasets were recognized as valuable for training and testing models. Methods for detecting fraud attacks in IoT systems were also discussed. Our paper presents a unique approach to detect cyberattacks and recognition card fraud in IoT systems. The most accurate cyberattack detection model achieved $95.15\%$ accuracy, while the credit card fraud detection model achieved $93.50\%$ accuracy. These results represent a significant improvement compared to previous studies. The proposed ensembles stacking approach has a lot to offer and we propose it can be improved by experimenting with alternative base model combinations and folding ratios. In the future, we are interested in refining our approach utilizing collaborative learning that is projected to drastically reduce the learning timeframe of building our suggested model. Furthermore, we are able to evaluate additional algorithms and analyze the outcomes to see whether we are able to create higher-performing combined models. Lastly, we can compare the efficacy of various collection techniques. This study's next trajectory is thought to be transferable knowledge.

## REFERENCES

[1] Q. Abu Al-Haija and S. Zein-Sabatto, "An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks," *Electronics*, vol. 9, no. 12, p. 2152, 2020.

[2] M. Aktukmak, Y. Yilmaz, and I. Uysal, "Sequential attack detection in recommender systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3285–3298, 2021.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[4] T. Alam, "A reliable communication framework and its use in internet of things (iot)," *CSEIT1835111— Received*, vol. 10, pp. 450–456, 2018.

[5] A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," *Soft Computing*, vol. 25, no. 18, pp. 12 319–12 332, 2021.

[6] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[7] M. J. Arshad, "Evaluating security threats for each layers of iot system," *International Journal of Recent Contributions from Engineering, Science & IT*, vol. 10, pp. 20–28, 2019.

[8] Z. A. Baig, S. Sanguanpong, S. N. Firdous, T. G. Nguyen, C. So-In, *et al.*, "Averaged dependence estimators for dos attack detection in iot networks," *Future Generation Computer Systems*, vol. 102, pp. 198–209, 2020.

[9] F. Battisti, G. Bernieri, M. Carli, M. Lopardo, and F. Pascucci, "Detecting integrity attacks in iot-based cyber physical systems: a case study on hydra testbed," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 2018, pp. 1–6.

[10] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "Iot elements, layered architectures and security issues: A comprehensive survey," *sensors*, vol. 18, no. 9, p. 2796, 2018.

[11] D. Choi, K. Lee, *et al.*, "An artificial intelligence approach to financial fraud detection under iot environment: A survey and implementation," *Security and Communication Networks*, vol. 2018, 2018.

[12] A. L. Cristiani, D. D. Lieira, R. I. Meneguette, and H. A. Camargo, "A fuzzy intrusion detection system for identifying cyber-attacks on iot networks," in *2020 IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, 2020, pp. 1–6.

[13] J. Davis and J. Cogdell, "Calibration program for the 16-foot antenna," *Elect. Eng. Res. Lab., Univ. Texas, Austin, Tech. Memo. NGL-006-69-3*, 1987.

[14] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.

[15] T. Gates, K. Jacob, *et al.*, *Payments fraud: perception versus reality-a conference summary*. SSRN, 2009.

[16] R. Geetha and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security," *Archives of Computational Methods in Engineering*, vol. 28, pp. 2861–2879, 2021.

[17] A. N. Jahromi, H. Karimipour, A. Dehghantanha, and K.-K. R. Choo, "Toward detection and attribution of cyber-attacks in iot-enabled cyber–physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13 712–13 722, 2021.

[18] A. H. K. Mohammed, H. Jebamikyous, D. Nawara, and R. Kashef, "Iot cyber-attack detection: A comparative analysis," in *International Conference on Data Science, E-learning and Information Systems 2021*, 2021, pp. 117–123.

[19] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing sdn infrastructure of iot–fog networks from mitm attacks," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1156–1164, 2017.

[20] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks," *Computer Networks*, vol. 165, p. 106945, 2019.

[21] S. Marchal and S. Szyller, "Detecting organized ecommerce fraud using scalable categorical clustering," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 215–228.

[22] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont)," *2015 Internet Technologies and Applications (ITA)*, pp. 219–224, 2015.

[23] K. N. Mishra and S. C. Pandey, "Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques," *Wireless Personal Communications*, vol. 119, pp. 1341–1367, 2021.

[24] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

[25] M. M. Moussa and L. Alazzawi, "Cyber attacks detection based on deep learning for cloud-dew computing in automotive iot applications," in *2020 IEEE international conference on smart cloud (SmartCloud)*. IEEE, 2020, pp. 55–61.

[26] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2016.

[27] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in iiot: A comprehensive survey of attacks on iiot and its countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE, 2018, pp. 124–130.

[28] P. Radanliev, D. De Roure, M. van Kleek, and S. Cannady, "Artificial intelligence and cyber risk super-forecasting," *pre-print, https://doi.org/10.13140/RG*, vol. 2, no. 34704.56322, 2020.

[29] S. Ram, S. Gupta, and B. Agarwal, "Devanagri character recognition model using deep convolution neural network," *Journal of Statistics and Management Systems*, vol. 21, no. 4, pp. 593–599, 2018.

[30] M. M. Rashid, J. Kamruzzaman, T. Imam, S. Kaisar, and M. J. Alam, "Cyber attacks detection from smart city applications using artificial neural network," in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. IEEE, 2020, pp. 1–6.

[31] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for iot," *Applied Soft Computing*, vol. 72, pp. 79–89, 2018.

[32] P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision support systems*, vol. 50, no. 2, pp. 491–500, 2011.

[33] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (iot): A security taxonomy for iot," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 163–168.

[34] B. Santhosh Krishna and T. Gnanasekaran, "A systematic study of security issues in internet-of-things (iot)," in *Proc. IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2017, pp. 107–111.

[35] P. Save, P. Tiwarekar, K. N. Jain, and N. Mahyavanshi, "A novel idea for credit card fraud detection using decision tree," *International Journal of Computer Applications*, vol. 161, no. 13, 2017.

[36] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, 2017.

[37] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on iot and iiot devices. in 2020 11th ieee annual ubiquitous computing, electronics & mobile communication conference (uemcon)(pp. 406-413)," 2020.

[38] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging iot paradigm: Visualizing inside functionalities, key features, and open issues," *Journal of Network and Computer Applications*, vol. 143, pp. 111–151, 2019.

[39] S. Singh, S. V. Fernandes, V. Padmanabha, and P. Rubini, "Mcids-multi classifier intrusion detection system for iot cyber attack using deep learning algorithm," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, 2021, pp. 354–360.

[40] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a lightweight detection system for cyber attacks in the iot environment using corresponding features," *Electronics*, vol. 9, no. 1, p. 144, 2020.

[41] S. Taheri, I. Gondal, A. Bagirov, G. Harkness, S. Brown, and C. Chi, "Multi-source cyber-attacks detection using machine learning," in *2019 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2019, pp. 1167–1172.

[42] P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure location of things (slot): Mitigating localization spoofing attacks in the internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199–2206, 2017.

[43] Y. Zhang, F. You, and H. Liu, "Behavior-based credit card fraud detecting model," in *2009 Fifth International Joint conference on INC, IMS and IDC*. IEEE, 2009, pp. 855–858.

[44] H. Zhou, G. Sun, S. Fu, L. Wang, J. Hu, and Y. Gao, "Internet financial fraud detection based on a distributed big data approach with node2vec," *IEEE Access*, vol. 9, pp. 43 378–43 386, 2021.

[45] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based iot: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.