TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 01/21 pp929–947
DOI: 10.26599/TST.2023.9010033
Volume 29, Number 4, August 2024

Enhanced IDS with Deep Learning for IoT-Based Smart Cities Security

Chaimae Hazman*, Azidine Guezzaz*, Said Benkirane, and Mourade Azrour

Abstract: Cyberattacks against highly integrated Internet of Things (IoT) servers, apps, and telecoms infrastructure are rapidly increasing when issues produced by IoT networks go unnoticed for an extended period. IoT interface attacks must be evaluated in real-time for effective safety and security measures. This study implements a smart intrusion detection system (IDS) designed for IoT threats, and interoperability with IoT connectivity standards is offered by the identity solution. An IDS is a common type of network security technology that has recently received increasing interest in the research community. The system has already piqued the curiosity of scientific and industrial communities to identify intrusions. Several IDSs based on machine learning (ML) and deep learning (DL) have been proposed. This study introduces IDS-SIoDL, a novel IDS for IoT-based smart cities that integrates long shortterm memory (LSTM) and feature engineering. This model is tested using tensor processing unit (TPU) on the enhanced BoT-IoT, Edge-IIoT, and NSL-KDD datasets. Compared with current IDSs, the obtained results provide good assessment features, such as accuracy, recall, and precision, with approximately 0.9990 recording time and calculating times of approximately 600 and 6 ms for training and classification, respectively.

Key words: IoT security; intrusion detection; ML; DL; LSTM; TPU

1 Introduction

Internet connections have recently expanded at a rapid rate[1–9]. More than 60 billion Internet-connected devices[10–16] are expected to be accessible by 2023. Internet of Things (IoT) equipment, such as linked sensors, lighting, and meters, is used in smart cities to gather and analyze data due to the complexity of the networks and the variety of devices in the IoT environment[17–20]. Cities then use these data to enhance facilities, public utilities, and services[21–31].

For developing technology infrastructure, smart city initiatives nowadays prioritize environment[32]. Many smart city initiatives currently prioritize the environment for developing technology infrastructure[32]. Numerous studies have focused on problems associated with the early phases of smart urban programs, particularly for teenagers in underdeveloped nations[32, 33]. Many highly potential innovations, such as spreadsheets, data warehouses, highly sophisticated platforms, file sharing, big data, and social mining, are integrated into smart city services[34]. All these smart city methods have been used in a diverse range of settings, including smart houses[35], electric buildings[36], smart towns[37], smart governance[38], green buildings[39], smart factories[40], smart agriculture[41], and smart healthcare applications,

• Chaimae Hazman, Azidine Guezzaz, and Said Benkirane are with Higher School of Technology Essaouira, Cadi Ayyad University, Marrakesh 81000, Morocco. E-mail: {a.guzzaz, chaimaa.hazman, sabenkirane}@gmail.com.
• Mourade Azrour is with Faculty of Sciences and Technologies, Moulay Ismail University, Errachidia 52000, Morocco. E-mail: azrour.mourade@gmail.com.
* To whom correspondence should be addressed.
Manuscript received: 2023-02-20 ; revised: 2023-03-26; accepted: 2023-04-14

which are becoming increasingly important[42–44]. Smart security monitoring is essential in smart cities to improve service delivery and preserve resources for individuals[45]. Several academic researchers have handled IoT security with increasing attention, which has emerged as a key topic[46]. Therefore, communication systems are always vulnerable to attacks over the web. Since then, a variety of intrusion detection systems (IDSs) have been established and enhanced to fulfill system security requirements. Therefore, a component might be crucial to a business. If the IoT node information is hacked, then business regions and economic difficulties might suffer considerably previous IDSs which have shown total incompetence in determining different assaults, particularly negligible exploits and lowering false alarm rate. Consequently, an emerging trend of useful, robust, and expensive IDS networks to maintain reliable Internet protection is observed.

Cybersecurity risks can be efficiently fought in a single system using firewalls and IDSs. The two main categories of potential IDSs developed using various machine learning (ML) and deep learning (DL) methods are misuse and anomaly detection techniques. Monitoring systems mainly depend on the fingerprints of security risks and harmful activities to enable classification and multilayer detection. By contrast, IDSs cannot detect specific attacks in the absence of a signature. Consequently, these systems are highly capable of detecting recognized hazardous activity and its variants. Meanwhile, anomaly detection-based IDS approaches depend on user activity to discover future threats[28]. Thus, several anomaly detection methods might produce false positives. Anomaly and abuse detection are two considerations in the application of ML methods[28]. Classical ML algorithms are unsuitable for use on usage on huge quantities of data, due to the lack of annotated trained data and the high emphasis on recovered characteristics obtained by users. DL, a revolutionary technology in ML, employs artificial neural networks and outperforms conventional approaches.

The main areas of the current research include network instrusion detection system (NIDS), network traffic intrusions, and alerting system administrators. This research examines a subset of inboard network traffic from outside the network infrastructure. Therefore, the real interconnected efficiency remains unaffected. First, obtained packets are examined via host- or network-based sensors. Thus, features are extracted using feature engineering. The acquired features are then used to run classification algorithms to identify the intrusion or abnormality. Moreover, creating cutting-edge artificial intelligences (AIs), such as ML and DL, are essential to improve IDSs. This system is a dependable method for safeguarding IoT environments from several attacks, such as service scanning, keylogging denial of service (DoS), and distributed DoS (DDoS). However, intrusion detection is still a subject of research. Various ensemble learning, ML, and DL techniques have been coupled to improve IDSs. Several problems, including real-time detection, class imbalance, quality enhancement, high dimensionality, vast volume, and time performance, remain unaddressed despite these efforts.

The current research mainly aims to improve and enhance the effectiveness of classifiers to address different intrusion detection issues.

The approach in this research is based on the long short term memory (LSTM) model. The methodologies for feature engineering improve the data quality to save time. Quality measures and hyperparameter optimization are utilized to determine the best settings for the proposed approach. Afterward, the LSTM classifier is trained using the newly created dataset.

The newly proposed IDS for IoT-based smart environments, namely IDS-SIoDL, employs DL to improve the detection rate and produce reliable decisions. The suggested framework typically incorporates an ideal deep-based intrusion detection strategy that utilizes LSTM and a variety of methods for feature selection. Results from experiments conducted on the NSL-KDD, BoT-IoT, and Edge-IIoT datasets demonstrate the effectiveness of the proposed method considering accuracy, precision, F1-score, recall, ROC, and AUC. Two important contributions are verified in this research.

First, AE, information gain (IG), and genetic algorithm (GA) are used to improve data integrity. Second, a classification model based on an LSTM model is developed to create an efficient IDS. The proposed model comprises three primary parts, as shown in Fig. 1: data preprocessing component, classifier model element, and prediction component.

The rest of this article is arranged as follows. Section 2 provides an introduction to smart cities and methods for detecting intrusions as well as citations to pertinent IDS research, including ML and DL, to safeguard IoT

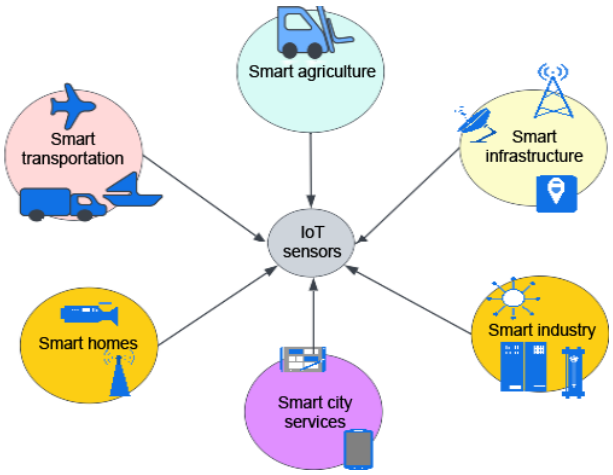


Fig. 1 Smart city components.

settings. This section also presents a critical evaluation of numerous systems. Section 3 comprehensively describes the innovative structure. Section 4 contains the obtained outcomes and relates them to initial approaches. Section 5 describes the results and discussion. Section 6 concludes with a summary and suggestions for additional research.

2 Overview and Related Work

2.1 Overview

2.1.1 Smart city components

Figure 1 depicts the elements of a smart city. Smart city applications generally include four phases: information gathering, transmission/reception, archiving, and analysis. Information collection is case-specific and has served as a crucial motivator for sensing systems in various disciplines. The adjoint component is the distribution of information, which entails sending information from the apparatus for information collection to the clouds for storing and processing. In addition to a wide range of regional networks capable of transferring information on a regional or international scope, several smart cities project Wi-Fi connections across the city, and 4G and 5G services are already being set up. The final level is storage space, in which a variety of functional techniques are used to maintain and organize information for data analysis. Data analysis is the process of dividing and gaining insights using the gathered information to facilitate selections. Simple analysis, including fundamental decisions and intelligence collection, might also be effective in certain situations. Considering the added responsibilities involved, in addition to ML and DL, cloud scalability allows for not only dispersed parameter estimation and computing but also real-time assessment with analysis methods[46].

Smart farming: Smart farming is the use of different sensors in trees and farms to monitor multiple aspects that aid in decision making or the prevention of illnesses and pests[47]. Smart farming is a component of the precision agricultural concept; therefore, this type of farming comprises the placement of sensing into trees to provide specific observations, allowing again for the deployment of tailored healthcare strategies. Agriculture will generally be required for agricultural security[48] and is thus a critical component of something similar to the struggle for sustainable farming. The primary uses of AI in IoT for farming include farm measurement diagnosis as well as information on farm health and decision-making process.

Services for smart cities: Waste management is a purpose and scope of innovation, and has formed a portion of the previously discussed smart city plans, from grates in Barcelona to possessing garbage cans fitted with sensors and linked to virtualization, which not only reassures the relevant agencies of the requirements to clear them but also incorporates AI to determine the most efficient way to maintain low costs[49]. Sensing may also be employed to measure environmental factors in a city to estimate pollution problems[50] and direct residents to the nearest free parking space to reduce gasoline expenses[51].

Smart health: Smart health strives to make healthcare affordable to many individuals through healthcare[52], and enhances assessment aid to clinicians with the use of artificial intelligence[53]. The widespread availability of smartphones and health monitoring devices[54] capable of capturing actual information regarding population lives (electrocardiograph, temperature, body oxygen saturation, and other biosensors), obtaining regular activities, and identifying abnormal movements using motion detectors has become crucial in leveraging cloud infrastructure for accessing the above information to improve medical choices. Therefore, the entire expenses and load on health systems are reduced.

Smart industry: In addition to cyber complex hardware that integrates workforces and hardware, the incorporation of IoT in factories and production mechanisms has resulted in numerous potential

advantages for the marketplace, including quick and highly effective advancement, minimization of mass production schemes, improving quality, and enhancing production plant accident prevention. Moreover, smart industries present several difficulties for IoT usage; functioning with a diverse collection of equipment and automated systems encounters a range of difficulties, requiring the flexible, connected, and rapid arrangement of cyber physical systems to incorporate when used in IoT devices for the smart industry[55]. AI must have collaborated with IoT to accelerate the development and implementation of Industry 4.0 services. With sensing integration in devices and other manufacturing methods, data from such resources introduce the possibility for AI approaches to be used to boost mechanization and execute effective intelligence activities. In addition, academics[55, 56] propose concepts for incorporating data into IoT for smart industry prescriptive analytics.

2.1.2 IoT in smart cities

The IoT is at the foundation of smart city projects; it is the embedded system that has allowed widespread automation, promoting the concept of intelligent cities. The IoT refers to the universal interconnection of devices to that same Internet. This interconnection enables cloud send with information and possibly obtain orders for performing tasks. IoT entails information gathering, including performing data analytics processes that obtain data to assist in policy and decision-making.

2.1.3 Security issues in IoT-based smart cities

The IoT serves to automate every aspect of people's daily lives. This technique for smart cities comprises the multiplication of sensing devices throughout each area of a city's gear system. Given the large service range, the development and implementation of IoT devices in smart urban areas present enormous obstacles that must be addressed. This subsection addresses the problems encountered by IoT network architects while deploying applications for smart cities. Figure 2 depicts the numerous problems encountered by smart city IoT system implementation, including privacy and security, smart sensors, and big data analytics[56].

Smart sensors: In smart cities, smart sensors are the major parts that collect information. Various devices that use multiple sensor methods, measuring instruments, data structures, and network protocols have been developed by several companies. Smart city

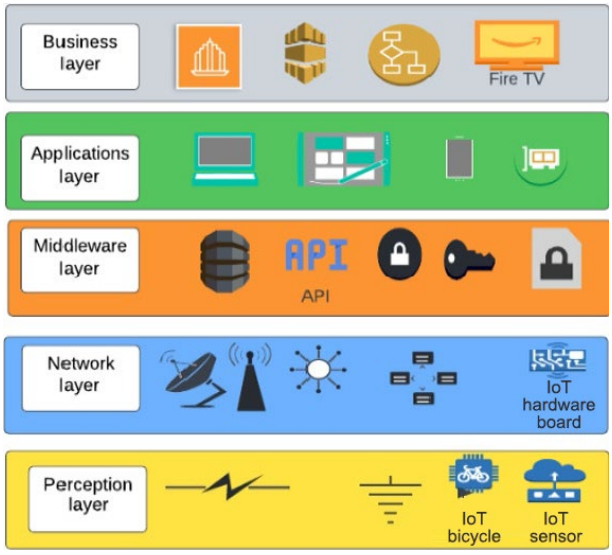


Fig. 2 IoT architecture.

adoption will require these gadgets to exchange information, coordinate work, and aggregate information to make deductions.

Data analytics: New data analytic techniques should be created to maximize the advantage of massive data, and continually enhance the solutions required by smart cities. With the variety of characteristics observed in smart cities, such algorithms must be adaptive to different kinds of information, and superior information merging approaches must be created to integrate information profoundly and draw conclusions to identify patterns. DL can use such substantial amounts of information to produce improved outcomes for a diverse set of solutions, thereby gaining increasing interest from researchers in this field[54].

Privacy and security: The cybersecurity of IoT devices is a major issue due to the increased number of apps and consumers in IoT nodes. The combination of IoT infrastructure with smart settings increases the effectiveness of smart items. Moreover, the consequences of known IoT vulnerabilities are extremely hazardous in crucial smart buildings used in industries such as safety and manufacturing. Software and services will now be jeopardized in IoT-based smart objects that lack adequate security controls. Confidentiality, integrity, and availability are three critical protection principles of services and applications in intelligent environments powered by IoT; consequently, increasing attention from researchers on data security in IoT systems is required to solve these issues[57]. Researchers investigate IoT

security issues from various perspectives; thus, these issues are regarded as the protection risk posed by IoT networks[58]. The current research concentrates on IDSs for smart cities regardless of any specific protocol.

2.1.4 Intrusion detection systems

IDSs are often grouped into three types. One type of IDS is signature IDS (SIDS), which may collect Internet traffic and match them to a database of known threats[59, 60]. SIDS has a low percentage of false accept rate (FAR) but has high detection probability when detecting malicious activity (DMA). SIDSs have been increasingly effective throughout numerous cases, due to the requirement to continuously maintain the database current with new threats and limit the growth of vulnerabilities. Furthermore, anomaly IDS (AIDS) has a high potential for resolving this problem. AIDS can infer usual trends and classify any variance or departure as an incursion[61]. Host-based intrusion detection system (HIDS) is a combination of SIDS and AIDS[61–64]. HIDS provides massive DMA in identified assaults while lowering the FAR in unidentified intrusions. From an implementation perspective, alternative classifications of IDS, including HIDS and NIDS, are discovered in the current research. Inner breaches can be detected by hosting IDS only within the host, whereas NIDS gathers and evaluates data passing via the networks[65–78]. Network infrastructure and protected communication are inaccessible to NIDS[59].

ML is a subclass of AI that has reduced the need for interaction between people in various industries. The methodologies of ML are divided into two major phases: training and testing. During the training stage, the method learns distinct patterns based on the data to produce a learning algorithm. The model can be employed to identify unknown cases during the testing phase. Two types of ML are available: supervised and unsupervised learning. Supervised classifiers use prelabeled inputs to construct the model.

2.2 Related work

This part comprises a summary of IoT technology techniques as well as citations to several recent related IDS works that incorporate ML and DL algorithms to improve IoT security. IoT environments are rapidly spreading because of the proliferation of linked items and varied networking equipment outfitted with diverse sensors, actuators, and CPUs. Devices can immediately share data via the Internet without user intervention. IDS are widely used in traditional industrial automation as well as modern industrial IoT. The industrial IoT is a large and complicated system. Each error or irregularity in a network element could rapidly cause substantial harm to the entire network. Therefore, rapidly and reliably recognizing cyberattacks are critical for a rapid and successful network response. An IDS is essential for network data protection because it helps the system to detect network breaches rapidly.

In 2018, Zhou and Paffenroth[29] proposed a technique for choosing a significant feature based on the random forest algorithm. The suggested model was analyzed using NSL-KDD to yield 0.9933 accuracy. In 2019, authors in Ref. [13] created an intrusion detection model based on ensemble learning of support vector machine (SVM) with logarithm marginal density ratios transformation (LMDRT) transformation as a viable strategy for improving information quality; the CICIDS2017 information shows that accuracy is 0.9364, DMA is 0.9756, and FAR is 0.2028. In the same year, Wang et al.[19] proposed an adversarial multiagent reinforcement learning model for IDSs centered on reinforcement learning, which always has space for development and efficiency, considering efficiency and precision. However, Chen et al.[16] produced an NIDS based on a CNN-based data gathering and surveillance management system in 2020 to safeguard Industry 4.0 against cybersecurity incidents and other attacks on developing automated frameworks and computer hacking on SCADA systems and solutions. In 2021, Yuan et al.[18] introduced the DeepFed approach for identifying and offsetting cyber threats to scatter IoT technology. However, the aforementioned methodologies are inadequate for dealing with current worldwide, massive, and complex multivariate data. A lengthy learning program is typically necessary when working with IoT data. Consequently, precision should increase. In 2021, Ge et al.[21] described in their study an IDS technique for IoT systems that rely on feedforward neural networks employing levels and three thick layers. This technique is referred to as feedforward networks, which apply a classification model to track regular and varied attack types, which are shown in Tables 1 and 2. Afterward, they employed BoT-IoT for multiclass identification to distinguish regular and particular semi-harmful intrusions, achieving 0.9979 accuracy. Ullah and Mahmoud[22] suggested a convolutional neural network-based DL IDS model with a low detection rate

Table 1 Attack types in the BoT-IoT dataset.

Attack	Number of occurrences
DoS-TCP	615 799
DoS-UDP	1 032 974
HTTP	1484
OS fingerprinting	17 913
Service scan	73 167
Data theft	7
Keylogging	74
DoS-TCP	977 382
DoS-UDP	948 253
HTTP	987

Table 2 Attack types in the Edge-IIoT dataset.

Attack	Number of occurrences
Backdoor attack	24 862
DDoS-HTTP attack	229 022
DDoS-ICMP	2 914 354
DDoS-TCP	2 020 120
DDoS-UDP	3 201 626
Fingerprinting	1002
MITM	1229
Password	1 053 385
Portscanning	22 564
Ransomware	10 926
SQL-injection	51 203
Uploading	37 634
Vulnerability-scanner	145 869
XSS attack	15 915

of roughly 0.997 for binary and multicast classifications. Al-Kasassbeh et al.[23] proved that the LightGBM method obtained a perfect accuracy of 1, demonstrating it's superiority over DL approaches. Additionally, Guezzaz et al.[24] proposed an NIDS model based on DT and then compared their model to those that utilized identical datasets for enhanced data quality using the NSL-KDD and CICIDS2017 datasets. The model achieved 0.9942 and 0.9880 overall precision on the NSL-KDD and CICIDS2017 datasets, respectively.

Guezzaz et al.[25] developed an IDS that collects data packets using a multilayer perceptron (MLP) classifier. Moreover, Ashraf et al.[62] proposed IoTBoT-IDS, a unique empirical learning-based botnet detection system that defends IoT-based smart networks from botnet assaults. IoTBoT-IDS models the typical behavior of IoT networks using empirical learning-based approaches, such as the beta mixture model (BMM) and a correntropy model. An aberrant occurrence is defined as any divergence from typical behavior. Three benchmark datasets created from genuine IoT networks were used to test IoTBoT-IDS. The assessment findings reveal that IoTBoT-IDS efficiently identifies different forms of botnets with an overall detection rate of 0.992. In 2022, Mohy-Eddine et al.[28] proposed an efficient IDS model using ensemble learning to secure Edge-IIoT computing. Reference [26] exhibited IoT IDS employing RF, LR, NB, DT, ET, and GB techniques. The GA was used for feature engineering, and RF was employed to calculate the GA fitness function. The model was tested using the UNSW-NB15 dataset, and achieved an average accuracy of 0.8761 and a region under the AUC of 0.98. Guezzaz et al.[27] devloped an anomaly detection system for edge-based IoT security using ML approaches. This framework detected overuse and irregularities by employing *k*-nearest neighbor (KNN) and principal component analysis (PCA) approaches. The KNN predictor is used to increase detection performance and the decision-making process, while the PCA serves to enhance feature engineering and learning. The proposed methodology offers several benefits over other current structures, according to the aforementioned information. This method obtains 0.99 efficiency, 0.98 precision, and 0.027 FAR on the NSL-KDD dataset, and yields 0.98 accuracy, 0.97 precision, and 0.029 FAR on the BoT-IoT dataset. They attempted to compare their model with others using similar datasets. Their model obtained 0.9942 and 0.9880 accuracy on the NSL-KDD and CICIDS2017 datasets, respectively. Moreover, Ref. [63] proposed an IDS model against various cyberattacks on smart city apps based on DL and shallow ML models using a current IoT dataset, and introduced an aggressive learning approach, which can markedly increase governance once confronted with aggressive assaults. The simulation findings show that the inclusion of opposing values decreases detection accuracy by more than 0.70. However, the proposed model can provide detection accuracy of more than 0.99 and resist all forms of assaults, including aggressive ones. Furthermore, Gaber et al.[64] presented an intrusion detection approach to identify injection assaults in smart cities. Different categories of feature selection methods[79], recursive feature deletion, and static

removal were used in this technique, and SVM, RF, and DT were among the ML classifiers that have been investigated. The test was used to evaluate the effectiveness of the suggested feature selection approach. The evaluation results on the published dataset AWID showed that the DT model can identify injection attacks with 0.99 accuracy using only eight characteristics obtained by the specified feature selection technique. Furthermore, Hazman et al.[80] suggested an IDS-SIoEL, a novel IDS for IoT-based smart settings based on ensemble learning. The framework generally provided an optimal anomaly detection model that employed AdaBoost and incorporated many feature selection algorithms, including Boruta, mutual information, and correlation, proposed an effective anomaly detection system based on IoT security. The model was evaluated using the updated NSL-KDD, BoT-IoT, and IoT-23 datasets.

In Ref. [28], Mohy-Eddine et al. presented a network intruder detection (NID) model for IoT settings that employed a KNN classifier and feature selection. The NIDS was combined with the KNN algorithm to increase IDS precision and detection rate (DR). Furthermore, PCA, univariate statistical test, and GA were independently used for feature selection to enhance data quality and select the ten best performing features. In the same year, Douiba et al.[81] presented an innovative IDS for IoT-based smart environments that used DL and supervised ML. The framework typically provided an optimal anomaly detection model that combined deep extraction based on the stacked AE and feature selection using IG and GA, which employed MLP, SVM, and KNN for classification. Compared with previous IDSs, the BoT-IoT dataset was used to validate the proposed model metrics. The findings indicated that the proposed approach provided outstanding accuracy, recall, ROC, AUC, and F1-score performance metrics.

3 Proposed Intrusion Detection System

This section explains several techniques to demonstrate the proposed IDS for smart city security. This method introduces and executes a suitable plan that enhances classification performance, reliability, and time consumption. The proposed method aims to assess an enhanced IDS that relies on feature engineering techniques and the LSTM model. Figure 1 depicts the effective predictive approach, which is divided into the following four major sections.

3.1 Effective predictive approach

3.1.1 Data preprocessing

Records have been produced and understood. Consequently, unwanted discrepancies are identified and deleted. The feature and target labels have been specified and prepared. The category variables are then encoded with the CatBoost encoder on the entire dataset to reduce overfitting. The features are then modified and merged.

3.1.2 Data quality part

The feature engineering algorithm (Fig. 3 shows how the algorithm works) is developed to improve quality by first using an AE to extract relevant characteristics, and reduce dimensionality after selecting features based on the quantity of mutual information across each characteristic and the target group. GA is then applied to generate effective training while lowering preparation time and operational costs. As a fitness function, GA determines that the most successful combination of characteristics has the strongest accuracy and smallest false positive rate (FPR).

3.1.3 Classification

The classifier section aims to create a classification model utilizing altered data from the data quality part as input. The classifier procedure will be divided into two parts: model learning and verification. In the first step, half of the information is used to train an LSTM model, which is used in the proposed method, and the rest of the data is utilized to assess the proposed model in the testing phase.

3.1.4 Prediction

The conceptual model can predict a successful assault. This model is studied and validated using metrics of evaluation classifications, such as accuracy, precision, FPR, and false negative rate (FNR). A technique for determining whether incoming traffic is normal or intrusion is introduced. Consequently, this component aims to create two outputs with a yes or no answer to

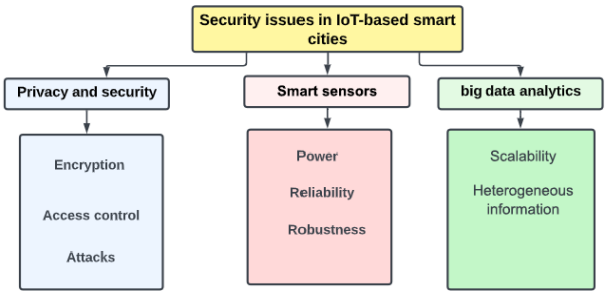


Fig. 3 Security issues in IoT-based smart cities.

confirm the access of classifiers to data. Therefore, numerical values are assigned to both categories, with 0 signifying normal activity and 1 signaling an assault. Notably, the attributes must be pre-determined. Numerous ways are provided to divide the findings into training and testing sets. The *k*-fold approach is presented in this case, and the framework is described in Fig. 4.

3.2 Description of solutions

3.2.1 Autoencoder implementing

A large-scale neural network called AE is frequently used to reduce the number of features because it is more robust than the original dataset considering data organization. In addition to layers with the same number of feature vectors, the AE comprises a low-dimensional hidden unit approximation. AE integrates and trains an encoder and decoder with a backpack. Information is transformed into tiny abstractions, thus reflecting specifics and preserving harsh qualities. The encoder, bottleneck, decoder, and reconstruction loss are all factors to consider and are crucial parts of a generic AE. Information from the input is even further reduced when an encoder is used, minimizing the number of characteristics that must be handled by the model. The bottleneck is the incoming data layer that contains the most compression loss and the fewest attributes. A model can decode the encoded representation and confirm that the output and input are the same using a decoder. The expression "reconstruction loss" refers to the gap between a decoder output and the initial inputs for examining the overall efficiency. Backpropagation is also used for training and reducing rebuilding losses[29]. The AE was used in the current research to reduce dimensionality.

The proposed method offers each incoming value and returns the same results, facilitating training to replicate the input sequence precisely. The AE comprises the following two components: the encoder and the decoder. The encoder trains data evaluation and reduces it to a bottleneck layer-defined intermediate representation. The decoder reproduces the data using the encoder output (the bottleneck layer).

After training the AE, the decoder is employed to reduce data instances to matrices generated by the bottleneck layer.

The encoder should contain two hidden layers: the first with double the amount of inputs and the second containing the same number of inputs as the dataset, followed by the bottleneck layer that contains the same number of entries as the dataset. Batch normalization and leaky ReLU activation are then utilized to guarantee that the model learns effectively.

The decoder should follow an identical architecture but within the inverse. The decoder will contain two hidden layers: the first containing the amount of data in the dataset and the next with double that amount. The output layer has the same number of nodes as the columns in the inputs, thereby outputting integer values that use a linear activation function. This reconstruction is a form of cross regression issue. Thus, the model is fitted using the effective Adam variant of stochastic gradient descent, which reduces the squared error.

3.2.2 Information gain

The decrease in entropy or surprise caused by altering a dataset is calculated as information gain. Equation 1 enhances IG for a set in entropy, specifically characteristics *A* and *C*. Entropy and IG are utilized to choose which characteristics to branch on to develop a superior prediction of the attribute value. This approach also signals when dividing should be discontinued[12].

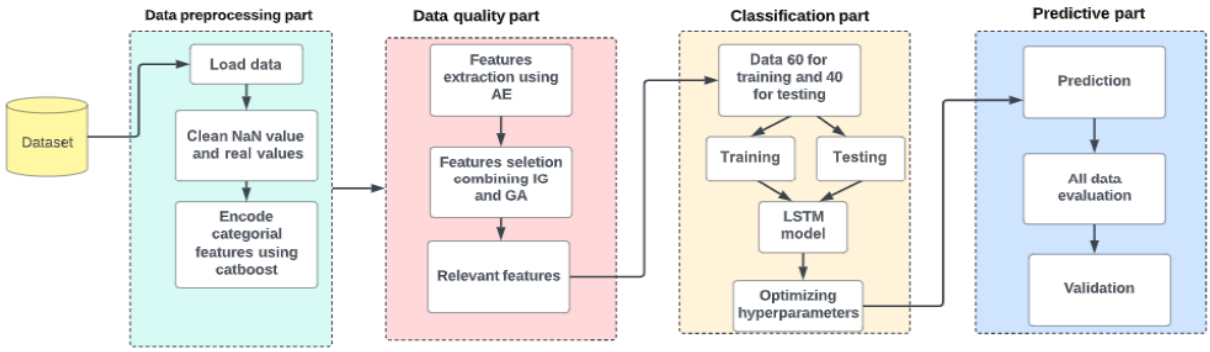


Fig. 4 Flowchart of a generalized system.

$$\mathrm{IG}(A,C) = H(A) - \sum P(C) \times H(C) \quad (1)$$

3.2.3 Genetic algorithms

The decrease in entropy or surprise caused by altering a dataset is calculated as information gain. Equation 1 enhances IG for a set in entropy, specifically characteristics A and C. Entropy and IG are utilized to choose which characteristics to branch on to develop a superior prediction of the attribute value. This approach also signals when dividing should be discontinued[12].

A method shown in Fig. 5 and based on migration is used by GA to choose the best set. The first stage in feature selection is to create research based on selections of potential characteristics[30].

(1) A starting population is created.

(2) The individuals of populations are given a score.

(3) A tournament is used to choose a subgroup for replication.

(4) A genetic material to be transmitted is chosen.

(5) Mutations are used.

(6) The process is repeated through several generations.

3.2.4 LSTM implementing

LSTM is a type of recurrent neural network. The output of the previous stage is used as the input in the current node in the RNN. High competitiveness and Schulte also create LSTM, which tackles the problem of RNN long-term reliance when the RNN may detect terms saved in long-term memory but may offer highly precise forecasts based on the current input. RNN occasionally functions poorly as the separation lengthens. By definition, LSTM may continue to demonstrate data for quite some time. LSTM is used to analyze, forecast, and categorize time series data[31]. Thus, LSTM is utilized in the current research for classification. Each LSTM neuron has a hidden layer output h_i, a memory cell C_i, and three inputs: the input data x_i, the following time step's hidden layer output and cell state, namely h_{t-1} and C_{i1}, respectively. The system comprises N functional neurons, and the input data comprises an M-element matrix. The following equations describe overall network behavior[66]:

$$\begin{aligned} G_i &= \sigma(W_{gx} \times x_t + W_{gh} \times h_{i-1} + a_g), \\ j_i &= \sigma(W_{ix} \times x_t + W_{ih} \times h_{i-1} + a_j), \\ \tilde{c}_i &= \tanh(W_{\tilde{c}x} \times x_t + W_{\tilde{c}h} \times h_{t-1} + a_{\tilde{c}}), \\ C_i &= f_i \circ C_{t-1} + j_i \circ \tilde{c}_i, \\ O_i &= \sigma(W_{ox} \times x_i + W_{oh} \times h_{i-1} + a_o), \\ h_i &= o_i \circ \tanh(C_i) \end{aligned} \quad (2)$$

where W is the matching $N \times M$ weight matrices, and x represents the measurement. N is the source vector structure matrix, h is the N size output vector, C is the N size cell state vector, and O is the M size bias vector. N and M are independent of one another. The consequences of N and M iteration are indicated by the variable subscripts t and $i-1$. Notably, matrix-to-vector and element-wise vector multiplications, commonly known as nonlinear combinations, are denoted[66].

A sequential model is established, and then three layers are added to build the neural network. An embedding layer is the initial layer added to the neural network model. The parameters of the layer are the input dim and vector size as the output dim. In this approach, the size of the input can be estimated from the number of features in each dataset. The vector size remains unknown. However, each feature is represented in 32-dimensional because this condition is larger than the purpose of employing an embedding layer. Finally, this LSTM layer is connected to a total layer containing two neurons, each of which represents a single class only in the binary classification. An error function is employed for category crossing variance to train the model, and its parameters are minimized using the Adam optimizer. Adam is chosen as the model optimizer because it performs better in many instances than other optimizers.

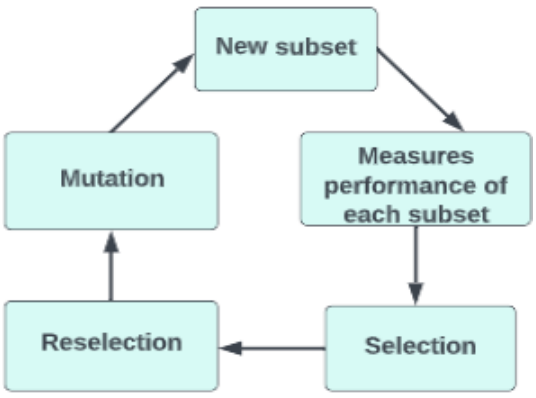


Fig. 5 Genetic algorithms.

4 Experiment

The proposed model is validated using recall, accuracy, and precision. Accuracy is determined by the fraction of correctly identified data to the total amount of samples. Precision is determined by the fraction of successfully predicted items to the overall TP (true positive) and FP (false positive).

The recall factor is calculated by dividing the entire amount of TP-measured data by the actual number of TP and FN measurement techniques (false negative). FPR and FNR are also computed. The FPR is the proportion of normal samples that test positive, whereas the FNR is the proportion of aberrant samples that test negative.

TP: The classifier forecasts an assault as true; thus, it is true.

TN: The classifier forecasts normal as false but is true.

FP: The classifier forecasts an attack, yet it never occurs.

FN: The classifier forecasts normal but is incorrect.

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{3}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \tag{4}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \tag{5}$$

$$\text{FNR} = \frac{\text{FN}}{\text{FN}+\text{FP}} \tag{6}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP}+\text{TN}} \tag{7}$$

IDS evaluation is a significant subject. Moreover, the classifications used are determined in accordance with the most appropriate performance variables in the training and testing datasets. This study uses three datasets; the first dataset has already been prepared and labeled for potential multiclass usage. An offensive flow, a class of attacks, and a subclass are all designated by the label features. In actuality, BoT-IoT has 99.94% more attacks than benign ones (0.01%), and contains 46 attributes, one of which is the target variable[67]. The Edge-IIoT dataset is a developed method for genuine cyber security datasets of IoT systems that may be used by ML-based IDS in two distinct modalities: centralized and federated learning[68]. This dataset has 99.99% more assaults than benign attacks (0.01%). The final dataset[69] is an enhanced version of KDD99, which has grown by first removing unnecessary entries and subsequently duplicating values. Except for the validation sample, the current research employs 20% NSL-KDD considering all characteristics.

The empirical assessment of the technique is executed using a gaggle computer with 13 GB of RAM, 15 GB of TPU V3−8 memory, and a 64-bit operating system. In addition to the Pandas, NumPy, and sklearn modules, the model is created using Jupyter Lab and Python 3.9.7.

5 Result and Discussion

5.1 Binary classification

All characteristics are multiplied by two as a consequence of this process. These characteristics are then inputted into the AE. The AE settings are reduced to a minimum. An AE is employed for the initial detection stage. A “dropout layer” is introduced to the AE input to prevent overfitting. This layer acts as a batch normalization constraint. Auto encoding is interrupted from reproducing the input to generate an output, demonstrating the proper use of the input approach. The dropout layer eliminates a random variety of neurons from the input during learning. AEs have a single hidden level that remains undetected. The total number of brain cells in this buried layer has a considerable influence. The second stage involves the combination of the IG and GA techniques for the feature selection. The first takes the data collected using AE and selects the best features using IG. Mutual information of a couple of variables shows their degree of dependency in a probabilistic sense. This idea of conceptual reliance cannot be mistaken with that of physical causality, even if one frequently implies the others in action. The GA then determines the most effective combination characteristics with the top importance area under the curve and receiver operating characteristic (AUR-ROC) rating, maximum accuracy, precision, recall, and the smallest FPR as a fitness function. The final phase is a model classification performed with the “LSTM” DL model with hyperparameters to obtain the highest accuracy. Figure 6 depicts the proposed model.

5.1.1 Results on BoT-IoT dataset

Following the steps mentioned in Fig. 4, the models are deployed to the BoT-IoT dataset, and the following results are obtained. Table 3 and Figs. 7–9 show positive findings utilizing the BoT-IoT dataset, with the proposed approach being the most successful vulnerability scanning strategy considering accuracy, precision, and recall (approximately 0.9994) and the lowest error rate of around 0.0030. Fitting the model on the TPU takes around 600–616 ms, while detecting assaults over the full dataset takes 8 ms. Figure 10 shows the use of 20 features to train and test the

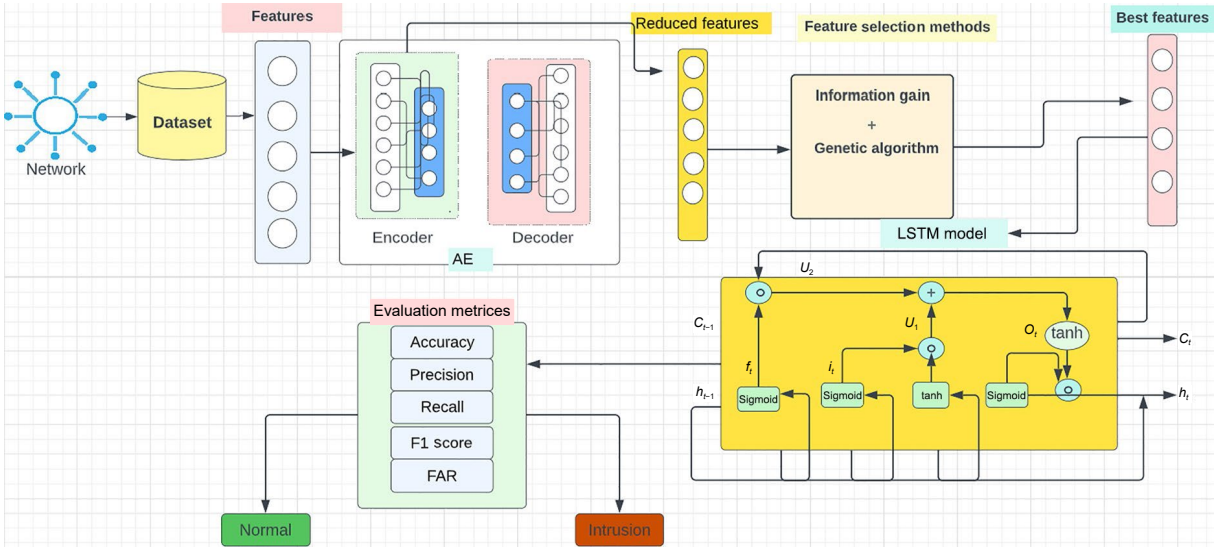


Fig. 6 Scheme of our IDS-SIoDL framework.

Table 3 Results of quality measures applied to the BoT-IoT dataset.

Number of epochs	Loss	Accuracy	val_loss	Recall	Precision	val_accuracy	Training time	Validation time
1	0.0071	0.9991	0.0041	0.9994	0.9994	0.9994	608 ms	10 ms
2	0.0039	0.9991	0.0030	0.9994	0.9994	0.9994	600 ms	8 ms
3	0.0034	0.9992	0.0030	0.9994	0.9994	0.9994	600 ms	8 ms
4	0.0034	0.9994	0.0028	0.9994	0.9994	0.9994	608 ms	8 ms

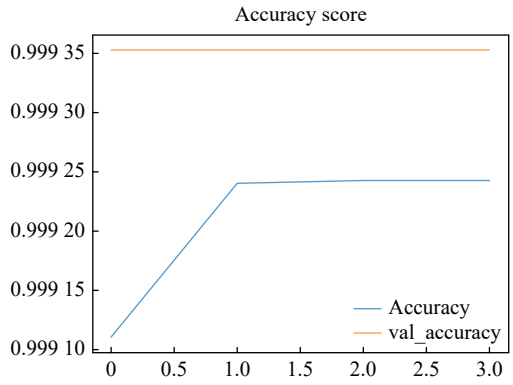


Fig. 7 Training validation accuracy of the developed framework in BoT-IoT over four epochs.

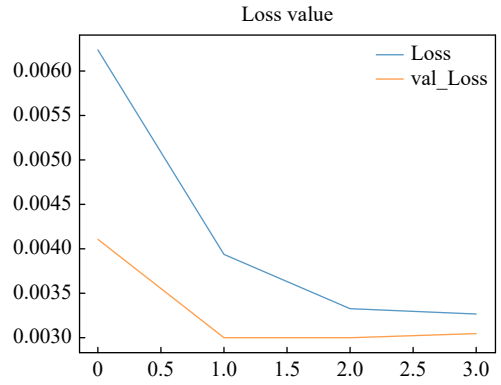


Fig. 8 Training validation loss of the developed framework over four epochs of BoT-IoT.

proposed model and validate their effect on performance

5.1.2 Edge-IIoT dataset

The findings show that the model performs with 1 accuracy, 0 FPR, and 0 FNR for precision and recall. With Edge-IIoT, we evaluated the model, and Table 4 and Figs. 9, 11, and 12 shows improved outcomes. The results attested to the model's efficacy. The findings for accuracy, precision, and recall are all 1. Moreover, the error is with zero, as shown in Fig. 13, therefore we only need 410 ms to fit the model in TPU and 5 ms to identify attacks across all datasets.

5.1.3 Results from the NSL-KDD dataset

NSL-KDD is used to evaluate and validate the quality of the model. The achieved results confirm the effectiveness of the proposed approach. Table 5 contains overall scores for accuracy, precision, and recall, which are around 0.9970, as shown in Figs. 9, 14, and 15. The confusion matrix in Fig. 16 shows that the error is minimum at 0.0184 with 0.0000 1 FNR and 0.0001 7 FPR. Furthermore, fitting the model in TPU takes only 100 ms and detecting assaults in all datasets

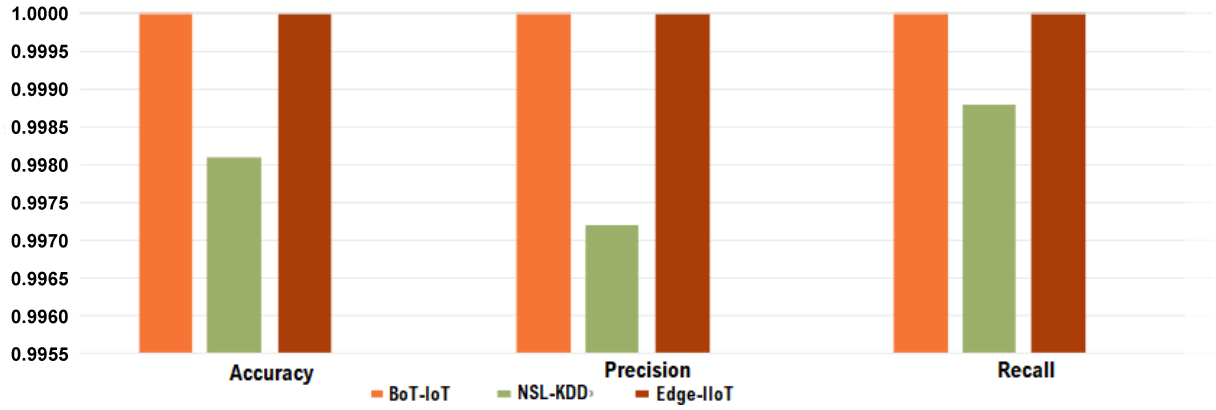


Fig. 9 Performance evaluation of our framework.

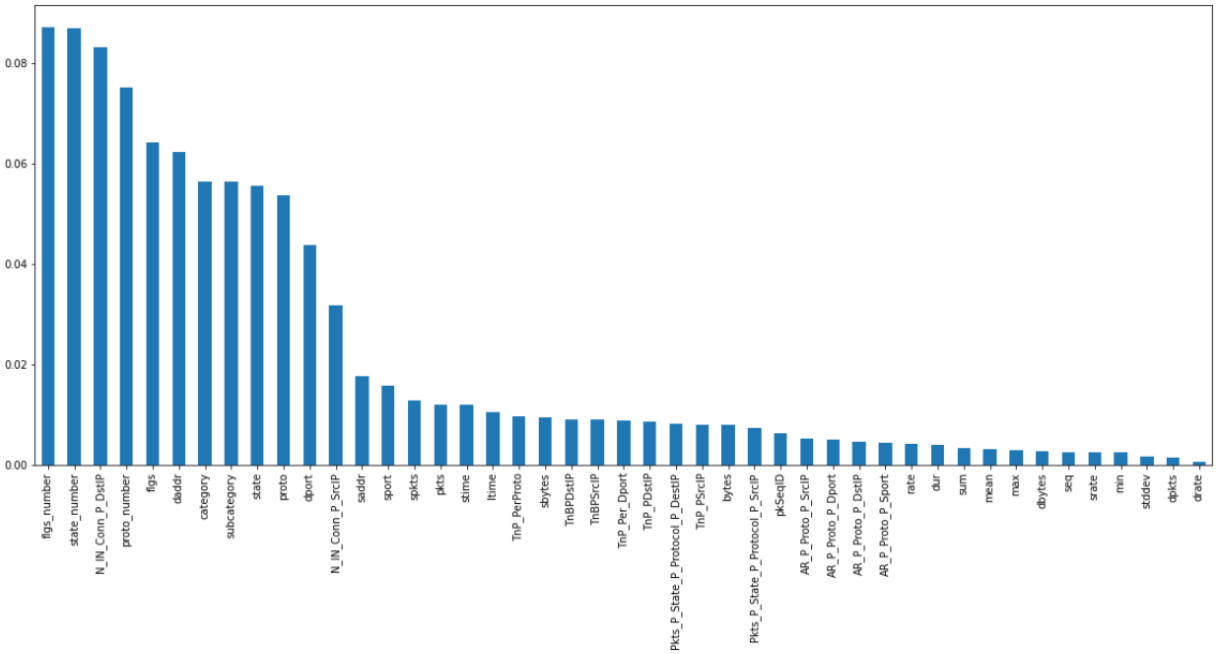


Fig. 10 Significance of characteristics in detecting attacks on the BoT-IoT dataset.

Table 4 Results of measuring achievement on the Edge-IIoT dataset.

Number of epochs	Loss	Accuracy	val_loss	Recall	Precision	val_accuracy	Training time	Validation time
1	0.0055	0.9983	0.0010	1	1	0.9999	418 ms	6 ms
2	0.0015	0.9998	3.7448×10^{-4}	1	1	0.9999	410 ms	5 ms
3	2.5033×10^{-4}	0.9999	9.0823×10^{-6}	1	1	1	411 ms	5 ms
4	3.2126×10^{-4}	0.9999	0	1	1	1	410 ms	5 ms

takes only 4 ms. In addition, 21 characteristics are employed for the effective outcomes, as shown in Fig. 17.

5.2 Multiclass classification

5.2.1 Results from the Edge-IIoT dataset

According to Fig. 18, the result categorization in the Edge-IIoT shows that the proposed model has a DR that is similar to the binary classification approach. The approach offers a high degree of accuracy and precision during training (1) and validation (0.99 and 0.50). The models of FPR and FNR rates are negligible, as illustrated in Fig. 9, this dataset offers a high DR for usual and malignant classes, such as

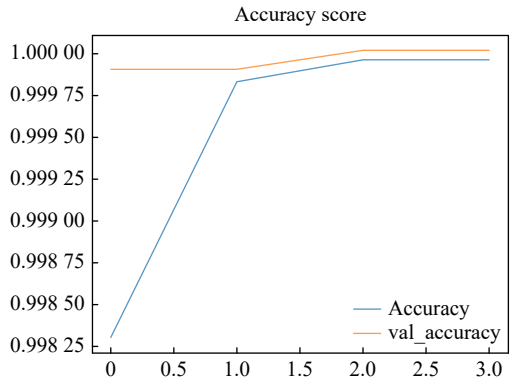


Fig. 11 Training validation accuracy of the developed framework throughout four epochs in Edge-IIoT dataset.

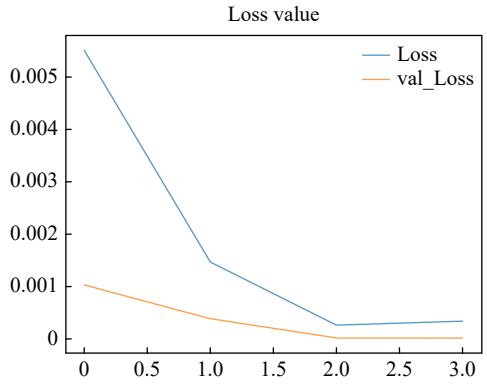


Fig. 12 Training validation loss of the developed framework over four epochs Edge-IIoT dataset.

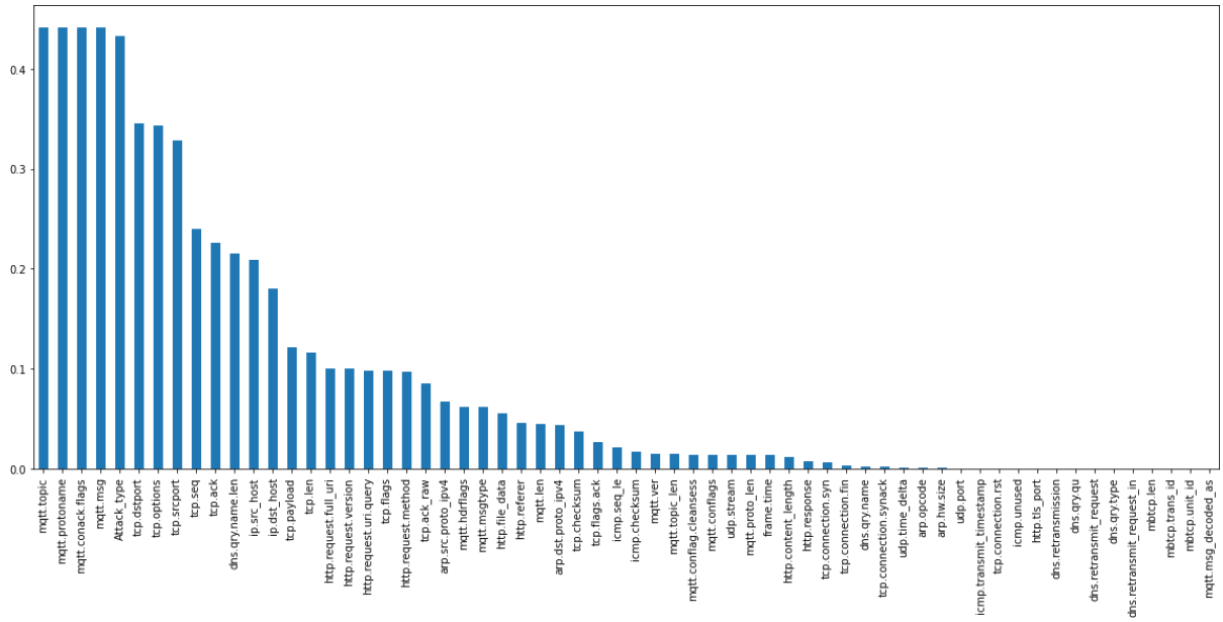


Fig. 13 Significance of characteristics in detecting attacks on the Edge-IIoT dataset.

Table 5 Results of measuring performance on the NDL-KDD dataset.

Number of epochs	Loss	Accuracy	Precision	Recall	val_loss	val_accuracy	Training time	Validation time
1	0.0185	0.9971	0.0184	0.9971	0.9971	0.9971	112 ms	4 ms
2	0.0185	0.9971	0.0184	0.9971	0.9971	0.9971	100 ms	4 ms
3	0.0185	0.9971	0.0184	0.9971	0.9971	0.9971	100 ms	4 ms
4	0.0185	0.9971	0.0184	0.9971	0.9971	0.9971	100 ms	4 ms

MITM, DDoS UDP, DDoS, and ICMP, and all other assaults achieves 1 precision and recall compared to other malicious classes, such as DDoS HTTP and Portscanning, which has a recognition accuracy of 0.98. Furthermore, the model rapidly delivers excellent results with a detection time of only 5 ms across all data. The model continues to function well, and the current research validates its capacity to identify anomalies in multiclass classification.

5.2.2 Results from the BoT-IoT dataset

As depicted in Table 6 and Fig. 19, the categorical classification results in BoT-IoT illustrate the DR achieved by the approach. The model has relatively high precision and accuracy across training (1) and validation (0.9915). The FPR and FNR rates in the current research are poor. Furthermore, Fig. 10 and

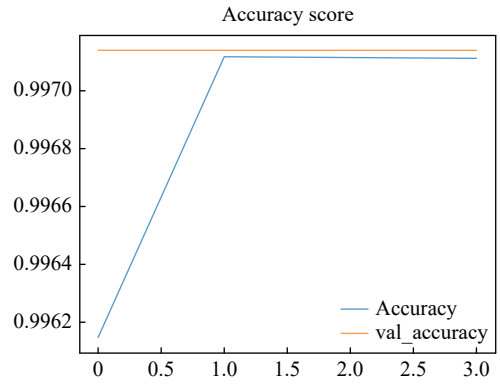


Fig. 14 Training validation accuracy of the proposed strategy in NSL-KDD spanning four epochs.

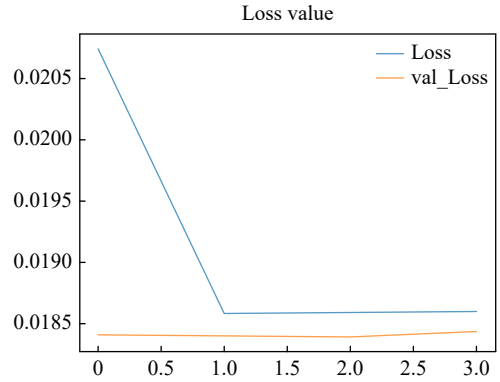


Fig. 15 Training validation loss of the developed framework over four epochs.

Table 6 show that this dataset has large detection results for regular and harmful classes. Moreover, classes such as information theft, DoS HTTP, DoS UDP, and reconnaissance OS fingerprinting demonstrate 1 precision, accuracy, and recall roughly

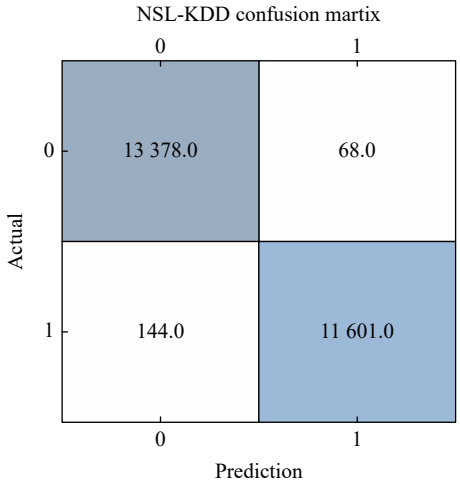


Fig. 16 Binary confusion matrix for NSL-KDD dataset.

equivalent to various types of harmful attacks, such as DDoS HTTP and DoS UDP, which have recall rates of around 0.99. Furthermore, service scan, DoS TCP, and DDos TCP have a recollection of approximately 0.98.

Binary and multiclass classifications are performed by utilizing the proposed algorithm of feature engineering and the LSTM model for training and verification on TPU. Model training is quick, between 100 and 616 ms. Validation recording takes between 6 and 5 ms. IDS accuracy and precision are increased while the computation time is further decreased by the training model validation of the influence features. Additionally, this model benefits from and is influenced by TPU use.

Since their beginnings, IDS has proven to be an excellent tool for protecting systems and infrastructure. In this study,

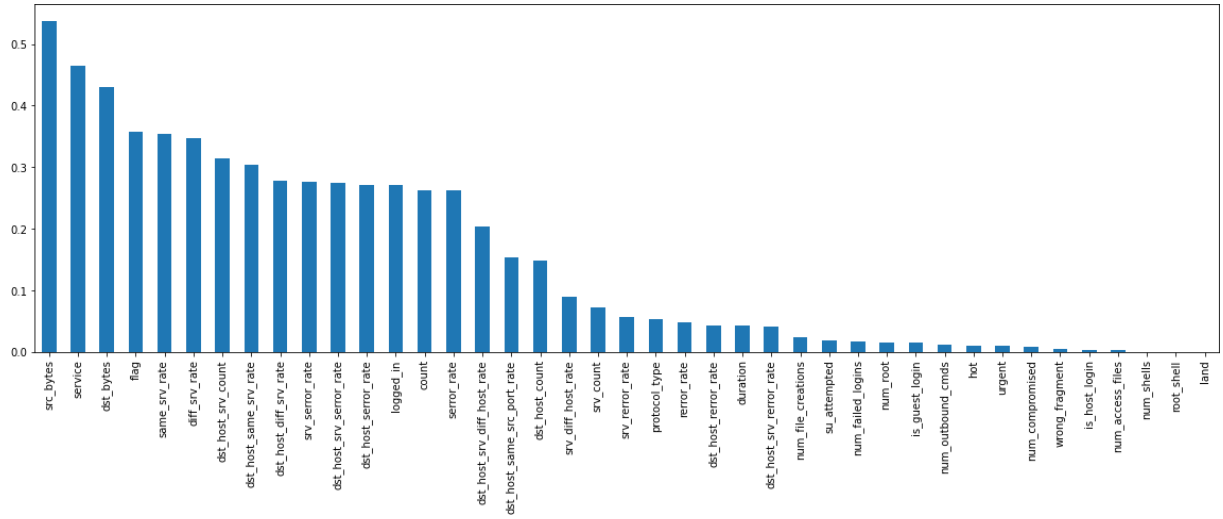


Fig. 17 Relevance of characteristics for recognition attack on NSL-KDD dataset.

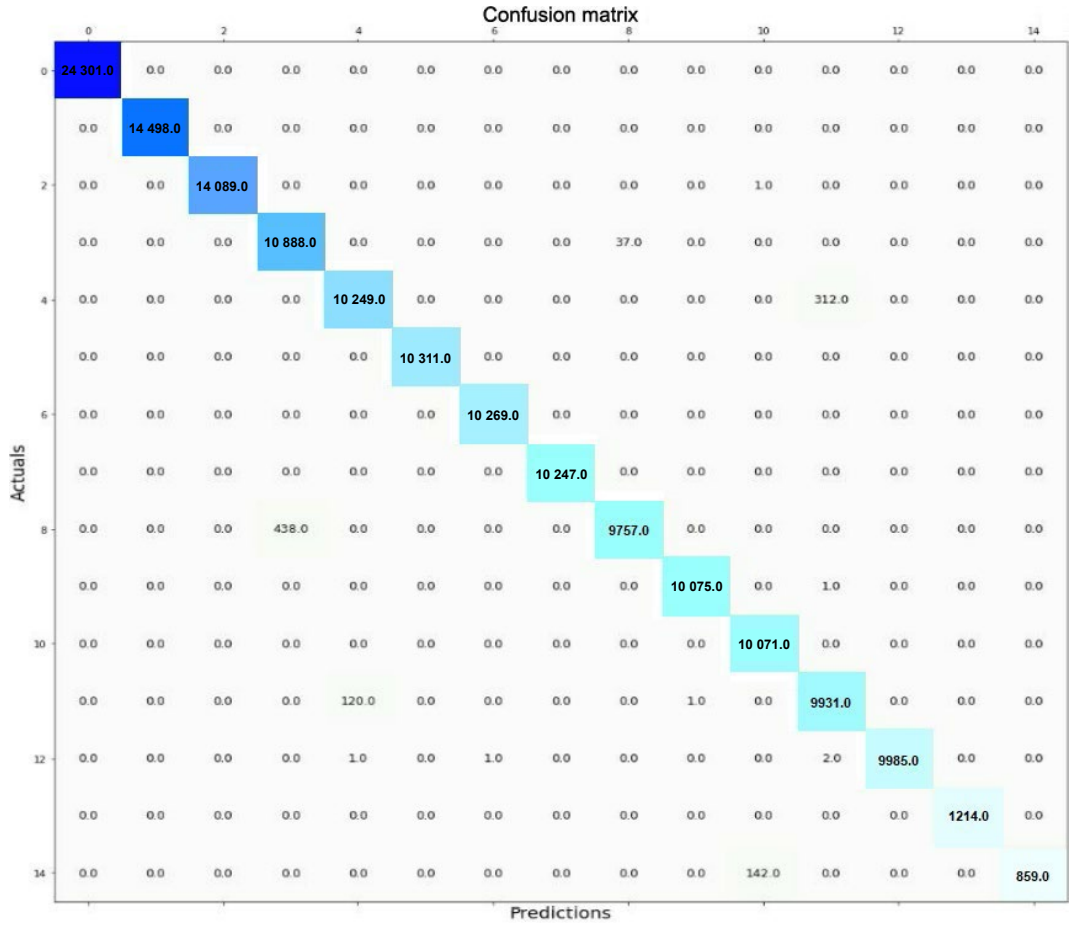


Fig. 18 Edge-IIoT multiclass prediction confusion matrix.

Table 6 BoT-IoT performance measurements of categorical classification results

Attack type	Accuracy	Precision	Recall
Reconnaissance service scan	0.97	0.97	0.97
Reconnaissance OS fingerprinting	0.97	0.97	0.95
DoS TCP	1	0.99	1
DoS UDP	1	1	1
DoS HTTP	0.97	0.97	0.99
DDoS TCP	1	1	1
DDoS HTTP	1	0.99	0.99
DDoS UDP	1	1	1
Information theft keylogging	0.99	1	0.99

6 Conclusion

We present a powerful intrusion detection technique that relies on DL using feature engineering techniques, with data quality being a significant factor in enhancing threat detection using pre-processing subsystems. To choose a subset of the entire dataset, we use several feature selection and extraction approaches, including AE, MI, and GA, and then we use the LSTM model for classification. TPU is used to train the model. The results demonstrate that our method produces good results while drastically lowering training time. Additionally, our work demonstrates that our model is a strong DL. In the future, we intend to leverage blockchain enhancements in combination with DL approaches to strengthen security in smart cities.

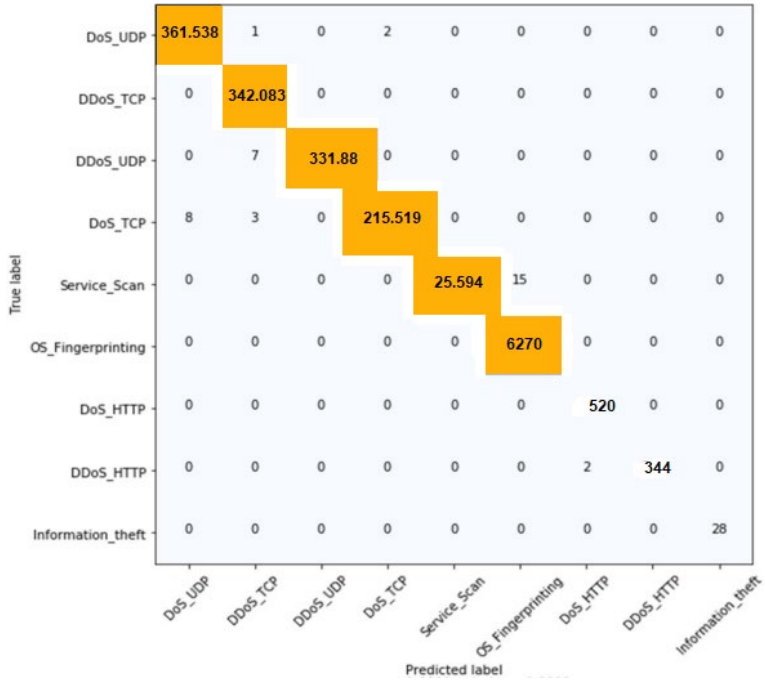


Fig. 19 BoT-IoT multiclass prediction confusion matrix.

References

[1] M. M. Salim, S. Rathore, and J. H. Park, Distributed denial of service attacks and its defenses in IoT: A survey, *J. Supercomput.*, vol. 76, no. 7, pp. 5320–5363, 2020.

[2] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert, Industrial Internet of Things and cyber manufacturing systems, in *Industrial Internet of Things*, D. Serpanos and M. Wolf, eds. New York, NY, USA: Springer, 2017, pp. 3–19.

[3] L. Sai Ramesh, S. S. Sundar, K. Selvakumar, and S. Sabena, Tracking of wearable IoT devices through WAP using intelligent rule-based location aware approach, *J. Inf. Knowl. Manag.*, vol. 20, p. 2140005, 2021.

[4] K. Kimani, V. Oduol, and K. Langat, Cyber security challenges for IoT-based smart grid networks, *Int. J. Crit. Infr. Prot.*, vol. 25, pp. 36–49, 2019.

[5] G. B. Mohammad, S. Shitharth, and P. R. Kumar, Integrated machine learning model for an URL phishing detection, *Int. J. Grid Distrib. Comput.*, vol. 14, no. 1, pp. 513–529, 2021.

[6] N. Angelova, G. Kiryakova, and L. Yordanova, The great impact of Internet of Things on business, *Trakia J. Sci.*, vol. 15, no. 1, pp. 406–412, 2017.

[7] G. Thamilarasu and S. Chawla, Towards deep-learning-driven intrusion detection for the Internet of Things, *Sensors*, vol. 19, no. 9, p. 1977, 2019.

[8] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, Internet of Things security: A survey, *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, 2017.

[9] P. M. Chanal and M. S. Kakkasageri, Security and privacy in IoT: A survey, *Wirel. Pers. Commun.*, vol. 115, no. 2, pp. 1667–1693, 2020.

[10] A. Borkar, A. Donode, and A. Kumari, A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS), in *Proc. 2017 Int. Conf. Inventive Computing and Informatics* (*ICICI*), Coimbatore, India, 2018, pp. 949–953.

[11] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, Anomaly detection model based on gradient boosting and decision tree for IoT environments security, *J. Reliab. Intell. Environ.*, pp. 1–12, 2022.

[12] T. T. Bhavani, M. K. Rao, and A. M. Reddy, Network intrusion detection system using random forest and decision tree machine learning techniques, in *Proc. 2022 Int. Conf. Advances in Computing, Communication and Applied Informatics* (*ACCAI*), Chennai, India, 2022, pp. 1–9.

[13] J. Gu, L. Wang, H. Wang, and S. Wang, A novel approach to intrusion detection using SVM ensemble with feature augmentation, *Comput. Secur.*, vol. 86, pp. 53–62, 2019.

[14] Y. Jiang, W. Wang, and C. Zhao, A machine vision-based realtime anomaly detection method for industrial products using deep learning, in *Proc. 2019 Chinese Automation Congress* (*CAC*), Hangzhou, China, 2020, pp. 4842–4847.

[15] M. A. Istiake Sunny, M. M. S. Maswood, and A. G. Alharbi, Deep learning-based stock price prediction using LSTM and Bi-directional LSTM model, in *Proc. 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference* (*NILES*), Giza, Egypt, 2020, pp. 87–92.

[16] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, A novel network intrusion detection system based on CNN, in *Proc. 2020 Eighth Int. Conf. Advanced Cloud and Big Data* (*CBD*), Taiyuan, China, 2021, pp. 243–247.

[17] W. Zhou, J. Li, Y. Chen, and L. C. Shen, Strategic interaction multi-agent deep reinforcement learning, *IEEE Access*, vol. 8, pp. 119000–119009, 2020.

[18] X. Yuan, J. Chen, N. Zhang, X. Fang, and D. Liu, A federated bidirectional connection broad learning scheme for secure data sharing in Internet of Vehicles, *China Commun.*, vol. 18, no. 7, pp. 117–133, 2021.

[19] D. Wang, B. Ding, and D. Feng, Meta reinforcement learning with generative adversarial reward from expert knowledge, in *Proc. 2020 IEEE 3rd Int. Conf. Information Systems and Computer Aided Education* (*ICISCAE*), Dalian, China, 2020, pp. 1–7.

[20] A. Ashiquzzaman, H. Lee, T. W. Um, and J. Kim, Energy-efficient IoT sensor calibration with deep reinforcement learning, *IEEE Access*, vol. 8, pp. 97045–97055, 2020.

[21] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, Towards a deep learning-driven intrusion detection approach for Internet of Things, *Comput. Netw.*, vol. 186, p. 107784, 2021.

[22] I. Ullah and Q. H. Mahmoud, Design and development of a deep learning-based model for anomaly detection in IoT networks, *IEEE Access*, vol. 9, pp. 103906–103926, 2021.

[23] M. Al-Kasassbeh, M. A. Abbadi, and A. M. Al-Bustanji, LightGBM algorithm for malware detection, *Intell. Comput*., pp. 391–403, 2020.

[24] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, A reliable network intrusion detection approach using decision tree with enhanced data quality, *Secur. Commun. Netw.*, vol. 2021, pp. 1–8, 2021.

[25] A. Guezzaz, A. Asimi, Y. Asimi, Z. Tbatou, and Y. Sadqi, A lightweight neural classifier for intrusion detection, *Gen. Lett. Math.*, vol. 2, no. 2, pp. 57–66, 2017.

[26] S. M. Kasongo, An advanced intrusion detection system for IIoT based on GA and tree based algorithms, *IEEE Access*, vol. 9, pp. 113199–113212, 2021.

[27] A. Guezzaz, M. Azrour, S. Benkirane, M. Mohy-Eddine, H. Attou, and M. Douiba, A lightweight hybrid intrusion detection framework using machine learning for edge-based IIoT security, *Int. Arab J. Inf. Technol*., vol. 19, no. 5, 2022.

[28] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, and M. Azrour, An effective intrusion detection approach based on ensemble learning for IIoT edge computing, *J. Comput. Virol. Hacking Tech*., pp. 1–13, 2022.

[29] C. Zhou and R. C. Paffenroth, Anomaly detection with robust deep autoencoders, in *Proc. 23rd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, Halifax, Canada, 2017, pp. 665–674.

[30] D. J. Murray-Smith, *Modelling and Simulation of Integrated Systems in Engineering*. Amsterdam, the Netherlands: Elsevier, 2012.

[31] M. A. Istiake Sunny, M. M. S. Maswood, and A. G. Alharbi, Deep learning-based stock price prediction using LSTM and Bi-directional LSTM model, in *Proc. 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference* (*NILES*), Giza, Egypt, 2020, pp. 87–92.

[32] T. Yigitcanlar, Smart cities in the making, *Int. J. Knowl.-Based Develop.*, vol. 8, no. 3, pp. 201–205, 2017.

[33] I. M. F. Oomens and B. M. Sadowski, The importance of internal alignment in smart city initiatives: An ecosystem approach, *Telecommun. Policy*, vol. 43, no. 6, pp. 485–500, 2019.

[34] M. Lytras, A. Visvizi, and A. Sarirete, Clustering smart city services: Perceptions, expectations, responses, *Sustainability*, vol. 11, no. 6, p. 1669, 2019.

[35] L. Nicholls, Y. Strengers, and J. Sadowski, Social impacts and control in the smart home, *Nat. Energy*, vol. 5, no. 3, pp. 180–182, 2020.

[36] Z. Xu, Y. Gao, M. Hussain, and P. Cheng, Demand side management for smart grid based on smart home appliances with renewable energy sources and an energy storage system, *Math. Probl. Eng.*, vol. 2020, pp. 1–20, 2020.

[37] M. Li, H. Tang, A. R. Hussein, and X. Wang, A sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community, *IEEE Open J. Commun. Soc.*, vol. 1, pp. 282–292, 2020.

[38] G. V. Pereira, P. Parycek, E. Falco, and R. Kleinhans, Smart governance in the context of smart cities: A literature review, *Inf. Polity*, vol. 23, no. 2, pp. 143–162, 2018.

[39] H. Park and S. B. Rhee, IoT-based smart building environment service for occupants' thermal comfort, *J. Sensors*, vol. 2018, pp. 1–10, 2018.

[40] A. Kusiak, Smart manufacturing, *Int. J. Prod. Res.*, vol. 56, nos. 1&2, pp. 508–517, 2018.

[41] M. Taylor, Climate-smart agriculture: What is it good for? *J. Peasant. Stud.*, vol. 45, no. 1, pp. 89–107, 2018.

[42] N. Sharma, I. Kaushik, B. Bhushan, S. Gautam, and A. Khamparia, Applicability of WSN and biometric models in the field of healthcare, in *Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks*, K. Martin Sagayam, B. Bhushan, A. D. Andrushia, and V. H. C. Albuquerque, eds. Hershey, PA, USA: IGI Global, 2020, pp. 304–329.

[43] A. Khamparia, P. K. Singh, P. Rani, D. Samanta, A. Khanna, and B. Bhushan, An Internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning, *Trans. Emerg. Telecommun. Technol*., vol. 32, no. 7, p. e3963, 2021.

[44] S. Goyal, N. Sharma, B. Bhushan, A. Shankar, and M. Sagayam, IoT enabled technology in secured healthcare: Applications, challenges and future directions, in *Cognitive Internet of Medical Things for Smart Healthcare*, A. E. Hassanien, A. Khamparia, D. Gupta, K. Shankar, and A. Slowik, eds. New York, NY, USA: Springer, 2021, pp. 25–48.

[45] C. Vorakulpipat, R. K. L. Ko, Q. Li, and A. Meddahi, Security and privacy in smart cities, *Secur. Commun. Netw.*, vol. 2021, pp. 1–2, 2021.

[46] Z. Khan, A. Anjum, and S. L. Kiani, Cloud based big data analytics for smart future cities, in *Proc. 2013 IEEE/ACM 6th Int. Conf. Utility and Cloud Computing*, Dresden, Germany, 2014, pp. 381–386.

[47] A. Koubaa, A. Aldawood, B. Saeed, A. Hadid, M. Ahmed, A. Saad, H. Alkhouja, A. Ammar, and M. Alkanhal, Smart palm: An IoT framework for red palm weevil early detection, *Agronomy*, vol. 10, no. 7, p. 987, 2020.

[48] M. J. O'Grady, D. Langton, and G. M. P. O'Hare, Edge computing: A tractable model for smart agriculture? *AIIA*, vol. 3, pp. 42–51, 2019.

[49] K. Pardini, J. J. P. C. Rodrigues, S. A. Kozlov, N. Kumar, and V. Furtado, IoT-based solid waste management solutions: A survey, *J. Sens. Actuator Netw.*, vol. 8, no. 1, p. 5, 2019.

[50] J. Dutta, C. Chowdhury, S. Roy, A. I. Middya, and F. Gazi, Towards smart city: Sensing air quality in city based on opportunistic crowd-sensing, in *Proc. 18th Int. Conf. Distributed Computing and Networking*, Hyderabad, India, 2017.

[51] F. Al-Turjman and A. Malekloo, Smart parking in IoT-enabled cities: A survey, *Sustain. Cities Soc.*, vol. 49, p. 101608, 2019.

[52] R. Varejão Andreão, M. Athayde, J. Boudy, P. Aguilar, I. de Araujo, and R. Andrade, Raspcare: A telemedicine platform for the treatment and monitoring of patients with chronic diseases, in *Assistive Technologies in Smart Cities*, A. R. G. Ramirez and M. G. G. Ferreira, eds. London, UK: IntechOpen, 2018.

[53] P. A. Keane and E. J. Topol, With an eye to AI and autonomous diagnosis, *NPJ Digit. Med.*, vol. 1, p. 40, 2018.

[54] G. Trencher and A. Karvonen, Stretching "smart": Advancing health and well-being through the smart city agenda, *Local Environ.*, vol. 24, no. 7, pp. 610–627, 2019.

[55] F. Tao, J. Cheng, and Q. Qi, IIHub: An industrial internet-of-things hub toward smart manufacturing based on cyber-physical system, *IEEE Trans. Ind. Inform.*, vol. 14, no. 5, pp. 2271–2280, 2018.

[56] J. Wan, J. Yang, Z. Wang, and Q. Hua, Artificial intelligence for cloud-assisted smart factory, *IEEE Access*, vol. 6, pp. 55419–55430, 2018.

[57] M. Weber and M. Boban, Security challenges of the Internet of Things, in *Proc. 2016 39th Int. Convention on Information and Communication Technology, Electronics and Microelectronics* (*MIPRO*), Opatija, Croatia, 2016, pp. 638–643.

[58] W. Elmasry, A. Akbulut, and A. H. Zaim, Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic, *Comput. Netw.*, vol. 168, p. 107042, 2020.

[59] M. Ahmed, A. N. Mahmood, and J. Hu, A survey of network anomaly detection techniques, *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2016.

[60] I. Butun, S. D. Morgera, and R. Sankar, A survey of intrusion detection systems in wireless sensor networks, *IEEE Commun. Surv. Tutor.*, vol. 16, no. 1, pp. 266–282, 2014.

[61] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, Intrusion detection systems for IoT-based smart environments: a survey, *J. Cloud Comput. Adv. Syst. Appl.*, vol. 7, no. 1, p. 123, 2018.

[62] J. Ashraf, M. Keshk, N. Moustafa, M. Abdel-Basset, H. Khurshid, A. D. Bakhshi, and R. R. Mostafa, IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities, *Sustain. Cities Soc.*, vol. 72, p. 103041, 2021.

[63] M. M. Rashid, J. Kamruzzaman, M. Mehedi Hassan, T. Imam, S. Wibowo, S. Gordon, and G. Fortino, Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications, *Comput. Secur.*, vol. 120, p. 102783, 2022.

[64] T. Gaber, A. El-Ghamry, and A. E. Hassanien, Injection attack detection using machine learning for smart IoT applications, *Phys. Commun.*, vol. 52, p. 101685, 2022.

[65] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, lIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning, *Cluster Comput*., vol. 54, no. 1, pp. 1–15, 2022.

[66] S. Hochreiter and J. Schmidhuber, Long short-term memory, *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[67] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset, *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, 2019.

[68] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, *IEEE Access*, vol. 10, pp. 40281–40306, 2022.

[69] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in *Proc. 2009 IEEE Symp. on Computational Intelligence for Security and Defense Applications*, Ottawa, Canada, 2009, pp. 1–6.

[70] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, Network traffic classifier with convolutional and recurrent neural networks for Internet of Things, *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

[71] M. Kumar, *Deep Learning Approach for Intrusion Detection System* (*IDS*) *in the Internet of Things* (*IoT*) *Network Using Gated Recurrent Neural Networks* (*GRU*). Dayton, OH, USA: Wright State University, 2017.

[72] B. Roy and H. Cheung, A deep learning approach for intrusion detection in Internet of Things using Bi-directional long short-term memory recurrent neural network, in *Proc. 2018 28th Int. Telecommunication Networks and Applications Conference* (*ITNAC*), Sydney, Australia, 2019, pp. 1–6.

[73] A. A. Diro and N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018.

[74] M. Roopak, Y. T. Gui, and J. Chambers, Deep learning models for cyber security in IoT networks, in *Proc. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference* (*CCWC*), Las Vegas, NV, USA, 2019, pp. 0452–0457.

[75] Y. Otoum, D. Liu, and A. Nayak, DL-IDS: A deep learning–based intrusion detection framework for securing IoT, *Trans. Emerg. Telecommun. Technol*., vol. 33, no. 3, p. e3803, 2022.

[76] S. Pande, A. Khamparia, D. Gupta, and D. N. H. Thanh, DDOS detection using machine learning technique, in *Recent Studies on Computational Intelligence*, J. Kacprzyk, ed. Singapore: Springer, 2021, pp. 59–68.

[77] S. Pande, A. Khamparia, and D. Gupta, An intrusion detection system for health-care system using machine and deep learning, *World J. Eng.*, vol. 19, no. 2, pp. 166–174, 2022.

[78] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. A. S. Alrimy, DeepIoT.IDS: hybrid deep learning for enhancing IoT network intrusion detection, *Comput. Mater. Continua*, vol. 69, no. 3, pp. 3945–3966, 2021.

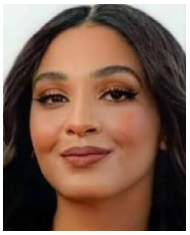
[79] A. Guezzaz, A. Asimi, A. Mourade, Z. Tbatou, and Y. Asimi, A multilayer perceptron classifier for monitoring network traffic, in *Big Data and Networks Technologies*, Y. Farhaoui, ed. New York, NY, USA: Springer, 2020, pp. 262–270.

[80] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, Intrusion detection framework for IoT-based smart environments security using ensemble learning, *Cluster Comput.*, vol. 26, pp. 4069–4083, 2023.

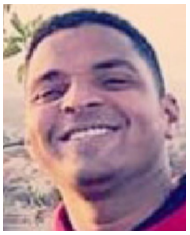
[81] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, An improved anomaly detection model for IoT security using decision tree and gradient boosting, *J. Supercomput.*, vol. 79, no. 3, pp. 3392–3411, 2023.

Said Benkirane obtained the MEng degree in networks and telecommunications from National Institute of Posts and Telecommunications, Morocco in 2004. He obtained the MS degree in computer and network engineering from Sidi Mohamed Ben Abdellah University of Fez in 2006, and the PhD degree in computer science from Chouaib Doukkali University of El-Jadida, Morocco in 2013. Since 2014, he works as a professor at Cadi Ayyad University, Morocco. His areas of research are artificial intelligence, multi agents, and systems security.

Mourade Azrour received the PhD degree from Moulay Ismail University, Morocco. He received the MS degree in computer and distributed systems from Ibn Zouhr University, Morocco in 2014. He currently works as a computer sciences professor at Faculty of Sciences and Technologies, Moulay Ismail University, Morocco. His research interests include authentication protocol, computer security, Internet of Things, and smart systems.



Chaimae Hazman received the MS degree in network and systems from Sultan Molay Solaimane University, Morocco in 2021. She is currently a PhD student of computer security at Cadi Ayyad University, Morocco. Her research interests are deep learning, IoT architectures and privacy, and security in smart cities.



Azidine Guezzaz received the PhD degree from Ibn Zohr University, Morocco in 2018. He is currently a professor of computer science and mathematics at Cadi Ayyad University, Morocco. His research interests are computer security, cryptography, artificial intelligence, intrusion detection, and smart cities.