APPLICATION OF MACHINE LEARNING FOR INTRUSION DETECTION IN SMART CITY APPLICATIONS

Abstract

A smart city is one that use technology to deliver services and address urban issues. A smart city works to enhance social services, enhance sustainability, and offer its residents flexibility. The interplay of technology, apps, and ideas is influencing every facet of the digital citizen's existence. Citizens in smart cities engage with their local ecosystems via a variety of devices, including smartphones, mobile gadgets, connected vehicles, and residences. Integration of large no of different kinds of IoT(Internet of Things) devices makes smart city very complicated. As various sensors collects data from different devices , the most important issue is to protection of data. For security concern zero-day attacks must be detected immediately. For this artificial intelligence based intrusion detection system is required. In this chapter, Author suggest an artificial intelligence-based intrusion detection system that can efficiently defend against new or continually changing attacks against IoT based smart city environment in order to resolve these problems.

Keywords: Sustainability, IoT, Sensors, Security, Attacks, Smart City, Artificial Intelligence, Intrusion Detection System

Authors

Kshyamasagar Mahanta
Department of Computer Application
Maharaja Sriram Chandra BhanjaDeo University
Baripada, India.

HimaBindu Maringanti
Department of Computer Application
Maharaja Sriram Chandra BhanjaDeo University
Baripada, India.

I. INTRODUCTION

The Internet of Things (IoT) encompasses a wide range of different kinds of technology, goods, and services. Devices that fall within the IoT's stringent restrictions are easily identified by their limited processing power and memory. They have a radio interface, sensors, and actuators, and run on rechargeable batteries. While wireless communication research has traditionally focused on improving data throughput, Environment-specific applications have particular needs, including smart home security systems, industrial automation, agricultural control systems, vehicle networks, and medical systems. Low data transmission rates, close-proximity communications, limited Internet of Things devices, and affordable hardware are a few of them. As a result, current research is increasingly focused on addressing these specific needs. These requirements must be met. As a result, traditional security and protection standards are not going to be implemented easily in the IoT's constrained context.

On the other hand, privacy and security regulations are among of the most pressing concerns in application-specific IoT networks. There are millions of smart homes that might be targeted by cybercriminals.Customers and businesses put their whole faith in the makers of IoT devices when it comes to providing sensitive information. However, the security of this data is limited to protecting them against known threats and breaches.Zero Day attacks are major concerns for smart city devices.

Intrusion detection systems (IDSs) are crucial security mechanisms that primarily operate at the network layer to prevent unauthorized access in IoT infrastructure. Effective IDS for IoT systems must be able to assess data packets at various IoT network levels utilizing various protocol stacks, adapt to various IoT technologies, and give real-time replies. Specifically, for IoT-based smart systems, an IDS must be capable of handling large volumes of data with minimal computational overhead to be effective. As a result, traditional IDSs may not be enough for IoT environments. Constant and growing threats to the security of IoT devices and networks need a thorough and ongoing investigation into the nature of these threats and the development of effective countermeasures.

The security solution offered by IDSs for IoT-based smart environments is thoroughly examined in this article. The main goal of this study is to provide an overview of the most recent methodologies and developments for IDSs operating in IoT-based systems. Also this research focuses on the critical aspects that influence performance of IDS in smart city applications, for instance, the precision of detection, the frequency of false positives, the size of the energy consumption, the speed of processing, and the size of the performance hit. Furthermore, this study proposed a new method for the creation of smart IDSs for smart environments.

The remaining part of this paper is structured as follows. In the "IoT and smart city applications" section, we address the definitions, aims, and problems of smart city applications, with a special emphasis on smart cities. The section titled "Security concerns in IoT-based smart environments" discusses the security issues that arise in IoT-based smart environments and how they relate to the different levels of the IoT architecture. Preliminary information regarding IDS definitions, IDS kinds, and detection methodologies is provided in the "Intrusion detection systems (IDSs)" section. In the section titled "IDSs developed for IoT systems," you will find a review of IDSs that are either applicable in or are particularly designed for smart city applications. A new model for smart intrusion detection system using machine learning is introduced in "Proposed Method for Intelligent IDS" section.The "Conclusion" section then reports on the study's findings and its intentions for future research.

II. IOT AND SMART CITY APPLICATIONS

Smart city applications use sensors to improve human life by making it more efficient and secure. Smart environments powered by IoT facilitate efficient development of intelligent things. Remote monitoring and control of sensors is possible through an IoT network. A fundamental aspect of a smart city is an all-encompassing information center run by an IoT service provider that furnishes information on utilities like gas, water, and electricity. Apart from this, smart cities encompass various other applications, including smart homes, smart buildings, smart industries, and smart healthcare, among others.Fig.1 depicts the architecture of such IoT-based smart city applications. Such smart application's main goal is to deliver services using intelligent ways based on data gathered by IoT-enabled sensors.

Wireless IoT systems are increasingly taking over conventional wired network infrastructure and are fast becoming the norm in both daily life and production. The Internet of Things offers a significant advantage, providing convenient solutions to previously difficult-to-solve problems, which not only enhances people's daily lives but also provides unprecedented opportunities in various industries[1].In such a system, the capacity to make decisions is a crucial attribute. Smart devices should be capable of making intelligent judgments without human involvement by utilizing data mining and other approaches to gather and analyze valid information.

To address issues in traditional public management affairs, Several countries' governments are committed to enhancing their Information and Communication Technology (ICT) infrastructure. Among the most effective and contemporary solutions is the establishment of smart cities[2]. An IoT network is necessary for managing and executing public services in a smart city. However, the development of an IoT-based smart city is not without challenges. The biggest obstacle is the unusual complexity, novelty, and technical difficulties of IoT systems. Furthermore, political and monetary constraints inhibit the efficient application of the smart city idea, while the lack of commonly agreed standards for smart city operations further hinders its implementation. Also we should not ignore about the security concerns while developing such applications.

The growth in the number of users and smart devices within IoT networks, along with the enormous data they produce, calls for the adoption of scalable computing systems, including cloud computing. Quality of service (QoS) in smart environment applications and IoT data management service performance can both benefit from such platforms. An efficient intelligent security system is mandatory for such networks.

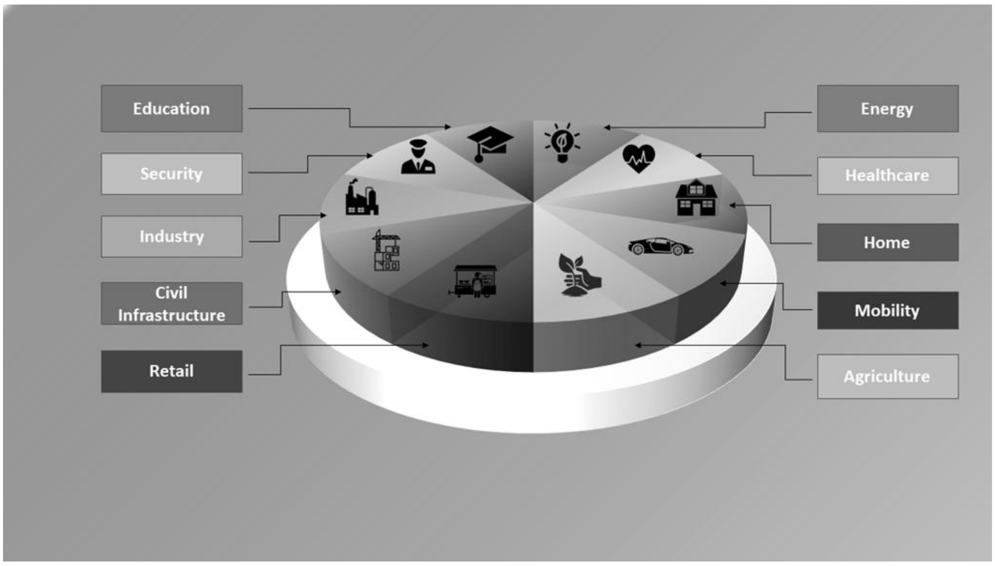


Figure 1: smart city applications

III. SECURITY CONCERNS IN SMART ENVIRONMENTS

The proliferation of IoT services and end-users has made security a top priority concern for the industry. When Internet of Things (IoT) infrastructure and smart surroundings are combined, the efficiency of smart items is greatly increased. Critical smart environments utilised in industries like medical and manufacturing are particularly vulnerable to the effects of IoT security flaws. The integrity of all applications and services within IoT-based smart environments is at risk without proper protection. Information security in IoT systems demands more attention, given that privacy, authenticity, and integrity are critical factors for applications and services in smart environments. The security of IoT systems, along with the complexity and compatibility of IoT devices, remains a significant barrier to the construction of smart environments in real-world scenarios. When smart environments are under attack, the services provided by IoT devices are disrupted.

The integrity of an Internet of Things (IoT) system can be threatened at any of its many layers. In the physical layer, obstacles can include physical damage, hardware failure, and power constraints. At the network layer, threats include denial-of-service attacks, sniffing, gateway assaults, and unauthorized access. Problems that may arise in the application layer include attacks from malicious code, application vulnerabilities, and software defects. Table.1 shows various layers and their security challenges.

Table 1: Various layers in IoT and their security challenges

Perception Layer	Network Layer	Application Layer
• Authentication and Physical threats • hardware failure, Physical damage, power limitations	• Confidentiality risk • Dos Attack, gateway attack,sniffing, unauthorized access	• Data integrity and privacy issues • Malicious code attack, application vulnerability, software bugs

The security of any IoT system can be vulnerable to four categories of threats: authentication and physical risks, confidentiality breaches, data integrity problems, and privacy issues. Below, we will briefly discuss some of the security concerns that can arise across the various layers of the Internet of Things.

- The challenges with authentication and the risks associated with physical threats are the initial obstacles that an Internet of Things (IoT) system must address. Many IoT devices, such as sensors, are part of the perception layer. Since these devices rely on their internal security measures, they are susceptible to direct physical attacks.
- There is a risk of breaching confidentiality when communicating within the network layer, between gateways and IoT devices. Data privacy during transmission in IoT networks is indirectly hampered by the lack of resources in low-level devices utilized in IoT systems.The integrity of data transferred between services and applications is the subject of the third category of security issues. When spoofing attacks or noise harm an Internet of Things system, data integrity issues may surface. Random attacks such as DoS, DDoS, and probing attacks can be detrimental to the applications and services provided by the IoT.
- Privacy concerns are at the heart of the fourth category of challenges. Privacy protection is an essential component of IoT system security. Different components of the internet of things make use of various kinds of item identification technologies. As a result, each item has a unique identifying tag, which includes information about its owner as well as its position and mobility. Information privacy is at stake when administering and watching over an IoT system's applications and services. For instance, it is seen as a breach of information privacy to use a system based on a deep packet inspection method for trusted activities within an IoT system. Any unauthorized intrusions into the management system constitute a risk to the users' ability to maintain the confidentiality of their information.

IV. INTRUSION DETECTION SYSTEM (IDS)

To effectively manage and secure IoT networks, it is important to closely monitor and analyze user data, by passively observing traffic and collecting data about networks and services. An intrusion detection systemis an effective means of keeping track of traffic statistics and detecting and preventing attacks on an information system's security, availability, and confidentiality. By utilizing an IDS, security personnel can quickly locate security issues and take action to prevent further damage. Additionally, IDS can provide valuable insights into network behavior and patterns, allowing for more effective network management and optimization.

The functioning of an IDS can be broken down into three phases. The first phase, called "monitoring," involves collecting data using sensors located in a network or on a host computer. The second phase, called "analysis," involves analyzing the data using techniques such as feature extraction and pattern recognition. The final step, "detection," involves using methods such as anomaly or intrusion detection to identify malicious activity. The IDS takes a snapshot of the data flowing over a network and analyzes it to detect any potential threats to the security, availability, or confidentiality of the system.

The deployment of an IDS necessitates consideration of the unique environment in which it will be employed. A HIDS (host-based intrusion detection system), for example, is intended to be installed on a single computer and defend it from possible intrusions or assaults that may damage its data or operating system. To identify possible threats, a HIDS often depends on measurements inside the host environment, such as log files. These measurements are subsequently supplied into the HIDS's decision-making engine as input. As a result, extracting features from the host environment is a vital component of any HIDS.

A network-based intrusion detection system (NIDS) is a security system that examines data packets traveling across a network for signs of intrusion or other malicious activity. NIDS can be implemented using either hardware or software. To protect larger networks with increasing traffic volumes, hardware-based IDSs like smart sensor architectures are often used. One example of a hardware-based NIDS is built using field programmable gate arrays (FPGAs). These are well-suited for use in NIDS because they can process large amounts of data quickly and can manage dynamic reprogramming and high-speed connections.

1. Detection techniques

- **Misuse-based intrusion detection:** In order to recognize well-known assaults, misuse-based intrusion detection techniques rely on a database of known signatures, patterns of harmful program codes and intrusions[3]. Utilizing misuse-based IDSs has three drawbacks, including network packet overload, high signature matching costs, and a high false alarm rate. Furthermore, due to their need to maintain a large database of attack signatures, misuse-based IDSs perform poorly in some types of networks, such as WSNs, which have limited memory capacity.For IDSs that use pattern matching and signature-based authentication, the signature and pattern databases need to be updated on a regular basis.

- **Anomaly-based intrusion detection:** Technique for anomaly-based intrusion detection creates a baseline of normal data patterns based on the behavior of regular users and continuously compares it with the current data patterns to detect anomalies or unusual behavior caused by intrusions[4]. Anomalies are actions that deviate from the expected pattern and leave traces in the computing environment. Unknown attacks can be found using anomaly-based IDSs based on these traces. The IDSs create a model of the expected behavior of the computing environment using data from regular users and update it continuously. The model is then used to identify any unusual activity. Anomaly-based IDSs are useful for detecting unknown attacks and have a lower rate of false alerts compared to misuse-based IDSs. However, anomaly-based IDSs can generate a high number of false positives if the expected behavior model is not updated regularly.

V. IDSS DEVELOPED FOR IOT SYSTEMS

The security risks inherent in IoT systems need the use of approaches that can proactively detect new forms of attack. In order to protect IoT-based smart environments from emerging threats, a reliable intrusion detection system is essential. This section provides a review of the many IDSs that have been suggested for IoT systems recently.

To address the issue of detecting distributed denial of service (DDoS) attacks in smart cities, a team of researchers[5] proposed a machine learning framework. Their approach leverages restricted Boltzmann machines to learn high-level features from raw data. These features are then used to train a feedforward neural network model for detecting attacks. To evaluate the effectiveness of their framework, the researchers tested it using a smart city dataset obtained from a smart water plant. Although it results satisfactory performance but as it is tested using very small dataset, the result may vary for other big datasets.

Another paper[6]proposed a semi-supervised intrusion detection method that combines multiple classifiers to distinguish between normal and anomalous activities in computer systems. Specifically, their approach utilizes decision tree learning with iterative dichotomiser 3 (DTL-ID3) to construct an abuse detection model. This model is trained using a database of gathered data based on an anomaly detection model implemented using a one-class support vector machine (OC-SVM).

An intrusion detection system for connected automobiles in smart cities was proposed by [7]. In their strategy, consumers' expectations for quality of service (QoS) and quality of experience (QoE) are met through the implementation of an automated safe continuous cloud service availability architecture that can identify security assaults. To distinguish between legitimate requests for trusted services and erroneous ones that could be made during intrusion assaults, the intrusion detection mechanism uses a three-phase technique that involves data traffic analysis, reduction, and classification. The authors perform data reduction and classification using deep belief and decision tree machine learning algorithms to do this. Overall accuracy for the suggested answer was 99.43%.

Various machine learning-based anomaly detection methods, including as LR(Logistic regression), SVM(Support Vector Machine), DT(Decision Tree), RF(Random Forest), ANN(Artificial Neural Network), and KNN(K-Nearest Neighbor), were examined in [8] in order to reduce IoT cybersecurity risks in smart city applications. They also looked into ensemble techniques including bagging, boosting, and stacking to enhance the effectiveness of the detection system. Although these methods are promising, the authors advise more research into deep learning techniques to improve the effectiveness of IoT threat detection.

In order to increase the security of IoT-enabled networks utilised for network traffic in smart cities, [9] suggested an ensemble intrusion technique that makes use of a cyborg intelligence framework (combining machine learning with biological intelligence). Using the KDDCUP99 dataset, the authors examined several algorithms to see how well they identified threats and attack-botnets in IoT networks based on cyborg intelligence. Their results show that AdaBoost ensemble learning, based on the Cyborg Intelligence Intrusion Detection framework, can quickly and accurately identify a variety of botnet assaults by using special network aspects.

The threshold-based intrusion detection system (TBIDS) and the multipath-based intrusion detection system (MBIDS) are two light and straightforward intrusion detection and prevention algorithms that [10] can be used in smart cities. To improve intrusion detection, these techniques use a cross-layer approach across the application and network layers. To show the efficacy of their suggested approaches, the authors compared them to three current algorithms (S-LEACH, MS-LEACH, and ABC).

Using the constrained application protocol (CoAP), [11] provided a framework to assess lightweight intrusion detection methods for smart city apps operating on resource-limited devices. The authors used this framework to assess intrusion detection methods for a CoAP-based smart public transportation application. According to their findings, this approach may be used to create an intrusion detection system with higher detection rates at a reasonable cost.

In order to defend IoMT equipment in smart healthcare environments from cybersecurity threats, [12] suggested using intrusion detection systems (IDS). In order to decrease the amount of characteristics, the author used principal component analysis (PCA), and ensemble-based classifiers were used to forecast network intrusion risks. Performance was assessed in terms of accuracy, precision, recall, and F-score using the KDDCup-'99 dataset. The study discovered that 93.2% accuracy was obtained utilising bagged decision trees and the bagging method, which is not the optimum outcome. To enhance the effectiveness of the intrusion detection system, more research is required.

A deep migration learning model is employed in the proposed work by [1] to develop an IoT intrusion detection method for smart cities. To extract characteristics from data, the programme integrates deep learning and intrusion detection technologies. The migration learning model and data feature extraction method are introduced in the paper. With 10% of the data used for training, the experimental dataset is the KDD CUP 99 dataset. The outcomes of the experiments demonstrate that the suggested algorithm has a greater detection efficiency and a shorter detection time. However, the compression procedure may result in a reduction in categorization accuracy. Therefore, more research is necessary to increase the categorization accuracy.

Paper [13] provide a unique method for identifying replay assaults in smart cities using a deep learning-based model. This methodology's primary contribution is the use of deep learning models to increase the precision of replay attack detection. The effectiveness of this model is assessed using a dataset from a real-world smart city where replay assaults were modelled. The suggested model outperforms both conventional classification and deep learning techniques in its ability to accurately discriminate between normal and attack behaviours. The detection system's overall performance may be improved by combining the deep learning model with an ensemble learning strategy.

In their study, [14] proposed two methods: semi-distributed and distributed, with the goal of addressing the drawbacks of centralised IDS for resource-constrained devices. These techniques combine effective feature extraction and selection with possible coordinated fog-edge analytics. In the semi-distributed method, parallel models operate side by side in feature selection while running on the edge. A single multi-layer perceptron classifier operating on the fog side then makes use of these chosen attributes. In the distributed method, parallel models each carry out multi-layer perceptron classification and feature selection independently. The outputs are then blended by a coordinating edge or fog to arrive at the final choice. Using the NSL-KDD dataset, these strategies were assessed and contrasted with other cutting-edge approaches. The results showed that the proposed methods outperformed the other techniques in terms of detection accuracy, demonstrating their potential in improving the effectiveness of IDS for resource-constrained devices. The result shows that the semi distributed approach achieved 99.97% accuracy and the distributed approach achieved 97.80% accuracy. By using complete temporal-features removal technique the result may change which leads to further investigation.

A framework and a hybrid algorithm are suggested in the study by [15] for recognisingIoT attack traffic and enhancing security. Using an IoT anomaly and intrusion identification dataset, the authors picked 44 useful characteristics from a wider collection of features, and then assessed the effectiveness of five machine learning algorithms using standard evaluation measures. In order to identify the best machine learning technique for detecting IoT anomalies and intrusion traffic, the scientists also used a bijective soft set approach. According to the findings, the Naive Bayes algorithm is good for detecting abnormalities and intrusions in IoT networks, and the suggested model and approach are helpful for choosing the best machine learning algorithm from a variety of available choices.

A video-based intrusion detection system (IDS) that employs deep learning to automatically identify unauthorised entrance or infiltration to critical places and warn concerned authorities in real-time has been developed in response to the growing need for intelligent security systems. A novel intrusion detection system (IDS) based on the You Only Look Once (YOLO) algorithm for object detection and a novel method based on the shifting centre of mass of the observed item for object detection were developed in a recent work by [5]. The invader was also tracked in real-time using the Simple Online and Real-time Tracking (SORT) method. Numerous smart city applications, such as no-entry zones for automobiles, no-parking zones, and smart home security, may be implemented using this technology.

VI. PROPOSED METHOD FOR INTELLIGENT IDS

Here a smart Intrusion detection technique has been proposed for smart city applications.The process of feature selection (FS) is a challenging optimization problem in the fields of data mining and artificial intelligence. Instead of analyzing all the features of a dataset, FS involves selecting relevant features associated with a particular problem with the goal of improving classification accuracy and reducing computational time[16]. This model is a combination of Random Monarch Butterfly (RMB) optimization and Gated Recurrent Unit(GRU) in an RNN model. RMB algorithm is used for optimization of feature selection.The first stage is preparing the features for analysis. After the first processing, we use an RMB computation to narrow in on the most pertinent features to increase the sensitivity of our detection. Following this, we anticipate data behavior based on less features by employing RNN. A training phase and a testing phase are included in this approach.

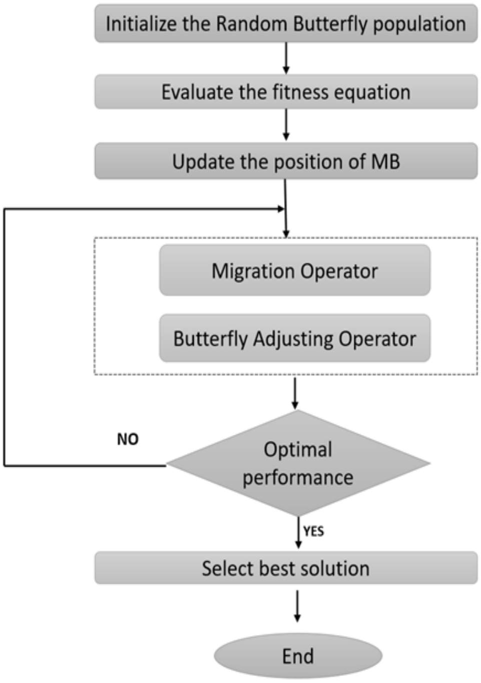
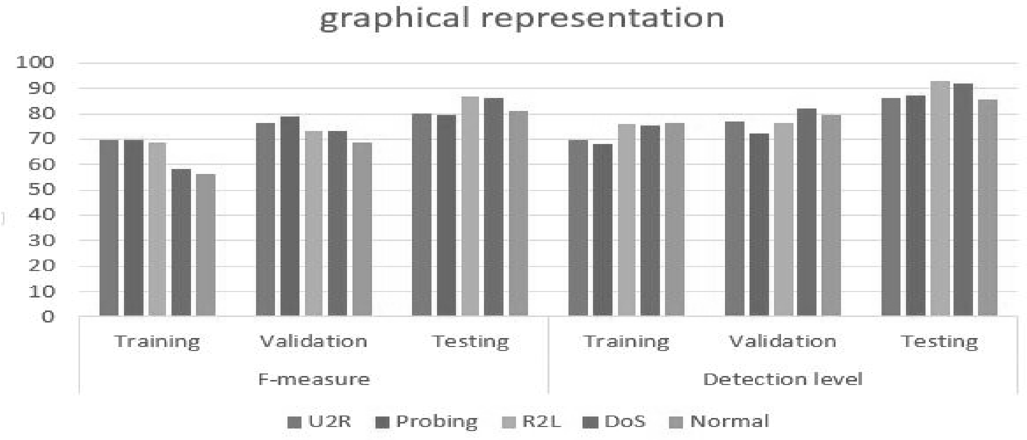

Initialize the Random Butterfly population
Evaluate the fitness equation
Update the position of MB
Migration Operator
Butterfly Adjusting Operator
NO
Optimal performance
YES
Select best solution
End

Figure 2: Feature selection flow chart

The forward and backward pass are essential to the RNN process. The primary motivation for GRU is to enhance this identifier in the context of smart city applications. The hidden unit is the most crucial part of an RNN since it determines which data to remember and which to forget. We next put the incoming data through its paces when the training process is complete. The data is sent to the service provider from the cloud server during testing. The provider now decides whether or not the incoming data is legitimate or malicious.We implement an RNN classifier into the testing procedure. The RNN is then fed test data with the lowered attribute. It is the testing process that receives the weights learned by the trained RNN. The score is calculated at the end. The RNN score value is used to determine if the test data is typical or tampered with, thereby forming the basis of the classification conclusion. The suggested detection method limits the access of smart city administrators to network devices and data, which may be crucial for comprehensive management of safety and security.

Table 2: Statistics from experiments and effectiveness of attacks

	F-measure			Detection level		
Attack	**Training**	**Validation**	**Testing**	**Training**	**Validation**	**Testing**
U2R	69.78	76.22	80.05	69.48	76.89	86.44
Probing	69.85	79.22	79.45	68.22	72.25	87.11
R2L	68.42	73.50	86.48	76.11	76.22	93.14
DoS	58.22	73.15	86.22	75.15	82.14	91.85
Normal	56.25	68.78	81.11	76.22	79.48	85.45



The KDD CUP 99 dataset is used for examination.Four types of threats, which includes DoS, a Probe, a Remote-to-Local (R2L), and a User-to-Root attack, are represented in the dataset with one normal class (U2R). When the training set data are properly provided, our suggested approach achieves its highest F-measures in the testing model.Statistics from experiments and effectiveness of attacks rate are shown in Table 1. Therefore, when compared with the approval and planning phases, the rate at which an attack on a smart city's application may be detected is between 85.55 and 93.14%. On the other hand, the efficacy and efficiency of the algorithm have been significantly improved, as evidenced by the fact that its detection rate and error detection rate have both gone up in relation to a number of different threats.

VII. CONCLUSION

As a result of numerous attacks and weaknesses, system security has become an urgent concern, especially in for smart city applications. Therefore, identifying intrusions is a fundamental part of keeping a system secure. Due to the large amount of data and unnecessary, extra characteristics, building the expectation model for an anomaly detection method is challenging. With the improved feature extraction provided by the suggested RMB, a fast and accurate detection technique may be implemented. This approach encourages continuous monitoring for network intrusions. Our suggested procedure achieves rates of 93.658% for detection, 92.1125% for FAR, and 0.262% for doing it correctly. Comparative exactness studies and the F-measure all favor the suggested work. Simulation results demonstrated that the proposed method improves productivity without sacrificing detection accuracy or introducing an excessive number of false positives. The initiative aspires to improve the security of the underpinnings of smart cities and to contribute to the building of an end-to-end integrated security stage for many smart apps already in use and influencing many aspects of people' daily lives.

REFERENCES

[1] Li, D., Deng, L., Lee, M., & Wang, H. (2019). International Journal of Information Management IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. International Journal of Information Management, 49(April), 533–545.

[2] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32.

[3] Bul'ajoul, W., James, A., & Pannu, M. (2015). Improving network intrusion detection system performance through quality of service configuration and parallel technology. Journal of Computer and System Sciences, 81(6), 981–999.

[4] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys and Tutorials, 16(1), 303–336.

[5] Elsaeidy, A., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2019). A machine learning approach for intrusion detection in smart cities. IEEE Vehicular Technology Conference, 2019-September, 1–5.

[6] Zou, X., Cao, J., Guo, Q., & Wen, T. (2018). A novel network security algorithm based on improved support vector machine from smart city perspective R. Computers and Electrical Engineering, 65(3), 67–78.

[7] Aloqaily, M., Otoum, S., Al, I., & Jararweh, Y. (2019). Ad Hoc Networks An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks, 90, 101842.

[8] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in iot-based smart city applications using machine learning techniques. International Journal of Environmental Research and Public Health, 17(24), 1–21.

[9] Onyema, E. M., Dalal, S., Romero, C. A. T., Seth, B., Young, P., & Wajid, M. A. (2022). Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities. Journal of Cloud Computing, 11(1).

[10] Ramadan, R. A. (2020). Efficient intrusion detection algorithms for smart cities-based wireless sensing technologies. Journal of Sensor and Actuator Networks, 9(3), 1–22.

[11] Krimmling, J., & Peter, S. (2014). Integration and evaluation of intrusion detection for CoAP in smart city applications. 2014 IEEE Conference on Communications and Network Security, CNS 2014, 73–78.

[12] Saba, T. (2020). Intrusion Detection in Smart City Hospitals using Ensemble Classifiers. Proceedings - International Conference on Developments in ESystems Engineering, DeSE, 2020-December, 418–422.

[13] Elsaeidy, A. A., Jagannath, N., Sanchis, A. G., Jamalipour, A., & Munasinghe, K. S. (2020). Replay Attack Detection in Smart Cities Using Deep Learning. IEEE Access, 8, 137825–137837.

[14] Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Hai Tao, M., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61(June), 102324.

[15] Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Future Generation Computer Systems, 107, 433–442.

[16] Alweshah, M., Alkhalaileh, S., Gupta, B., Almomani, D. A., Hammouri, A., & Al-Betar, M. (2022). The monarch butterfly optimization algorithm for solving feature selection problems. Neural Computing and Applications, 34.