Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 27 No. 3 (2024)

Smart Cities Driven by IoT: Improving Attack Detection with Cloud-Enabled Cybersecurity

Borse Pradnya Balasaheb[1], Dr. Meesala Sudhir Kumar[2]

[1]School of Engineering, Computer Department, Sandip University, Nashik - 422213, Maharashtra, India.
pradnyaborse09@gmail.com

[2]Professor, SOCSE, Sandip University, Nashik - 422213, Maharashtra, India sudhir.meesala@sandipuniversity.edu.in

Article History:

Received: *16-02-2024*

Revised: *26-04-2024*

Accepted: *18-05-2024*

Abstract

The susceptibility of smart equipment to sophisticated cyber threats, such as Distributed Denial of Service (DDoS) assaults, makes anomaly detection in smart cities essential in the current era of information technology. A machine learning-driven method is presented to tackle this problem, which makes use of the power consumption patterns of Internet of Things (IoT) devices to spot unusual activity in smart home settings. The training model is implemented near IoT layer devices by utilizing a distributed fog network. To gather statistics on power utilization during daily activities, a Raspberry Pi prototype smart camera has been constructed. To produce power consumption patterns suggestive of DDoS assaults, the study also investigates anomaly identification using Artificial Neural Network (ANN) approaches. ANNs are used to simulate DDoS attacks on an experimental setup. With an average detection accuracy of 78.67% across a range of assault situations, the results demonstrate that a deep feed-forward neural network model works better than previous models. This strategy puts less demand on Internet of Things devices with limited resources, which qualifies it for use in smart city applications.

Keywords: Artificial neural network, Cyber Security, Raspberry Pi, Industrial Internet of Things, Support vector machine, Attack Detection.

1. Introduction

The concept of a smart city requires robust security measures to protect its communication, monitoring, and response systems. The numerous interconnected elements that form the backbone of a smart city facilitate communication among citizens and enhance both the city's physical infrastructure and cyber security framework [1]. To fortify security within smart city infrastructures, cutting-edge technologies like blockchain are harnessed. Blockchain, known for its pseudo-anonymous nature, serves as a reliable security provider, ensuring secure transmission of vast amounts of data within the smart city environment [2]. Its architecture promotes trustless transactions, minimizing fraudulent activities by eliminating the need for third-party involvement [3]. The interconnection among humans, machines, and services has significantly expanded, leading to a new communication paradigm known as the Internet of Things. As the IoT is expanding, there is

a huge potential for misusing IoT services through targeting wireless edge devices in which sensitive, often semi-critical information can be illegally captured [4]. There was a discussion of the IoT developments about their many application areas and respective implementation obstacles. The goal is to establish a low-power, IoT-enabled smart city framework [5]. The Internet of Things is a network of physical devices that may connect and interact in various situations, including social, environmental, medical, and user contexts. The IoT is an infrastructure made of real items, such as vehicles, buildings, and even simple electrical appliances, that are connected via the Internet to gather and exchange data with one another Because cloud computing provides the scalability and processing capacity needed to manage the massive volumes of data generated by IoT devices, it is critical to this paradigm [6]. The cloud architecture uses advanced ML algorithms and AI techniques to detect anomalies and possible cyber threats in real-time [7]. The leakage of personal data due to software or hardware failures presents serious risks, potentially exposing city residents to physical harm, identity theft, cybercrime, or ransomware attacks [8]. Smart cities prioritize connectivity and collective learning to foster creativity and enhance human intelligence within an interconnected community [9]. By seamlessly integrating wired and wireless communication mediums, smart cities ensure efficient data transmission while providing real-time applications and security services to their residents [10]. The sharing of many types of environmental, industrial, and social data facilitates the IoT and allows for the creation of appropriate resource and service mappings in IoT-enabled smart cities [11]. The implementation of IoT in these settings results in increased productivity, reduced expenses, and better decision-making; however, it also raises security and privacy concerns that must be resolved with strong security and privacy protocols to guarantee the secure and dependable functioning of IoT, which powers smart environments [12]. As a result, environmental management and living circumstances are optimized and sustainable. Excellent use cases for the Internet of Things have already been demonstrated in several areas, including transportation, healthcare, retail, industry, and education. Its applications are also always evolving in new directions [13]. The rapid proliferation of connected devices can be attributed in large part to advancements in wireless technology, which have served as crucial enablers [14]. These technologies have made the connection between humans and real, physical items seamless, using interfaces like those seen on phones, tablets, and PCs. The interconnection of IoT sensors within smart networks exposes IoT devices in smart cities to several potential risks [15].

2. Related work

Alam and Faruq [16]. A smart grid architecture that uses green and renewable energy sources to power society within the framework of electricity supply can be a part of IoT-enabled energy management. Numerous IoT-driven sensors can monitor building energy use and street illumination, as well as collect and optimize traffic patterns. With this information, energy sources such as fuel, heat, and power can be used more efficiently.

Yahya et al [17]. IoT can expedite recycling, decomposition, and the transformation of waste materials into more valuable items, thereby aiding in the environmentally responsible management of household and business garbage. IoT holds enormous promise for raising living standards and fostering a sustainable society. One such example is the monitoring of city air and water quality using Internet of Things devices like sensors and embedded microcontrollers.

Alzahrani and Alenazi [18]. Although a lot of research has been done on intrusion detection systems (IDS) in the context of communication networks, the focus has shifted to IDS for Internet of Things (IoT) networks due to the increasing practical need to secure such networks. Recently, several IDS recommendations have been made. The authors of the research proposed a network intrusion detection system (NIDS).

Alrashdi et al [19]. An Anomaly Detection IoT (AD-IoT) system based on a Random Forest machine learning algorithm. They used a network-based data set with features such as source and destination IP address. Their anomaly detection system may fail if an attacker spoofs the addresses.

Badamasi et al [20]. Although it might not be appropriate for additional IoT protocols, the solution performed better than benchmark approaches. As part of the state-of-the-art decentralized computing paradigm known as fog computing, an Intrusion Detection/Prevention System (IDPS) with fog-assisted software-defined networking (SDN) was proposed in another research article.

S. C. Management et al [21]. The authors developed an efficient fog resource allocation mechanism to solve scalability challenges in Internet of Things networks. Additionally, an architecture for identifying abnormalities and lowering cyber hazards was proposed at the edge of the Internet of Things. An investigation of four classifiers for intrusion detection revealed that a combination of them performed well under a variety of conditions. Yet, it was demonstrated that the performance of multilayer perceptron (MLP) and recursive neural network (RNN) classifiers was influenced by the choice of learning window.

These new research papers demonstrate the evolution of the IDS field for IoT networks and highlight the need for customized approaches that consider the unique characteristics of IoT protocols and leverage state-of-the-art computer architectures to address security and scalability concerns.

3. Methodology

As IoT devices proliferate rapidly in smart cities, there are several opportunities to enhance urban living conditions. Still, there are significant concerns today about the security and privacy of these networked devices. This paper offers an innovative approach to using cloud computing for effective cyber security threat detection in IoT-enabled smart cities, with a focus on employing Raspberry Pi devices as edge computing nodes.

In the distributed architecture of the proposed system, Raspberry Pi devices act as edge nodes, collecting and pre-processing data from IoT devices placed all around the smart city. These edge nodes use their processing capacity to do basic analysis and filtering on the incoming data before transferring it to the cloud for further analysis.

Cloud computing is crucial in this paradigm because it provides the scalability and processing capacity needed to manage the massive volumes of data generated by IoT devices. The cloud architecture employs advanced machine learning algorithms and artificial intelligence techniques to detect anomalies and possible cyber threats instantly. Due to their low cost, low energy consumption, and ease of deployment, Raspberry Pi devices may be utilized as edge nodes. These devices may be positioned strategically across the smart city to guarantee efficient data collection and reduce the time it takes to transmit data to a central location.

Finally, the approach demonstrates how effectively cyber security assaults in Internet of Things (IoT) enabled smart cities can be detected using cloud computing and Raspberry Pi hardware. By combining edge and cloud computing power, this method improves the overall security posture of smart cities while safeguarding the privacy of their residents and enables fast and accurate identification of cyber threats. We will benefit from more research and development in this area to build strong and secure IoT ecosystems in smart cities.

The process of collecting personal data from different smart city devices and then processing and analyzing this data for many purposes is depicted in the suggested block diagram (Figure 1). The gathered information is a useful tool for improving privacy and security protocols in smart cities. Users may obtain insightful knowledge through the analysis of personal data, which can enhance customer satisfaction by providing a more comprehensive view of client experiences. Patterns and trends in security threats and privacy issues can be found by analyzing personal data from smart city devices. With the use of this data, proactive tactics and steps may be created to reduce possible risks, secure sensitive data, and preserve citizens' privacy in smart cities.

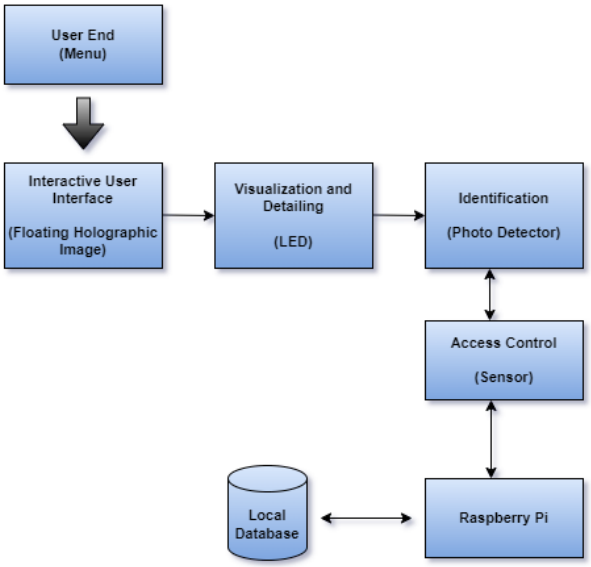


Figure 1. Block diagram of the proposed model

Furthermore, the examination of individual data might yield a significant understanding of user inclinations and actions in the context of smart cities. Smart city managers may maximize resources, customize products to match individual demands and improve the overall user experience by knowing how people interact with various services and systems.

It is crucial to make sure that all applicable privacy laws and rules are followed while collecting and analyzing personal data. To keep people of smart cities' trust and confidence, it is imperative to implement strong data security measures, such as encryption, anonymization, and safe data storage. Smart cities may provide the groundwork for a secure and user-centred environment by giving privacy and security priority when managing personal data.

3.1 Raspberry Pi:

The use of Raspberry Pi in the proposed cyber-attack detection model represents an innovative enhancement to security measures. Serving as a pivotal component, the Raspberry Pi integrates seamlessly into the system, leveraging its compact design and efficient management of the LED indicator system. This allows for the creation of tailored links for administrative purposes, providing an accessible means for system control. The integration significantly enhances the overall responsiveness and adaptability of the cyber attack detection mechanism. Raspberry Pi's versatility in interfacing with hardware components and executing programmed functionalities plays a crucial role in the reliability and effectiveness of the LED model. This enables swift identification and response to potential threats within smart city applications, thus bolstering the security infrastructure.

Figure 2. Raspberry pi

3.2 Artificial Neural Network (ANN):

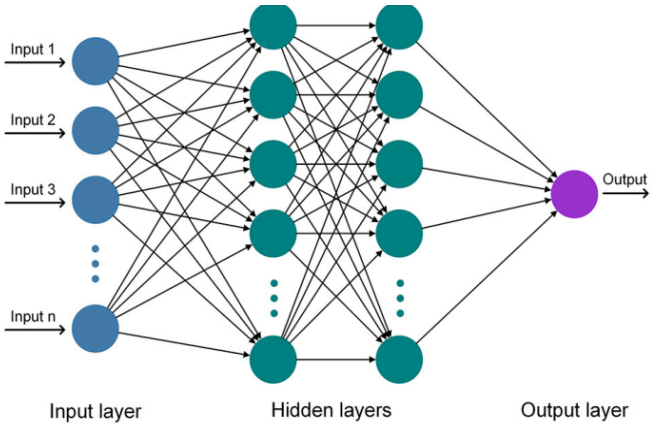


Figure 3. Schematic diagram of an Artificial Neural Network (ANN)

Artificial Neural Networks (ANNs) are computational models inspired by the structure and function of the human brain, designed to recognize patterns and solve complex problems. ANNs consist of interconnected processing units called neurons, organized into layers: an input layer, hidden layers for processing and extracting features, and an output layer for delivering the final result. This architecture enables ANNs to model intricate relationships within data, making them powerful tools

for various applications. The learning process of ANNs involves training the network using a dataset, where the model adjusts the weights of connections between neurons to minimize prediction errors. This is often achieved through backpropagation, where the error is calculated at the output layer and propagated backwards through the network to update the weights. During training, activation functions like sigmoid, tanh, and ReLU are used to determine the output of each neuron, adding non-linearity and enabling ANNs to learn complex patterns. ANNs have revolutionized various fields by enabling advanced capabilities in tasks such as image recognition, natural language processing, speech recognition, and autonomous systems. Convolutional Neural Networks (CNNs) excel at processing grid-like data, while Recurrent Neural Networks (RNNs) are adept at handling sequential data. However, ANNs face challenges, including the need for substantial amounts of data and computational power, and their generalizability to new, unseen data can be limited.

4. Experimental Setup

The goal of the experimental setup is to give intelligent control in complex circumstances by utilizing AI algorithms to handle devices and data in a smart city setting. Because AI is so good at performing complicated jobs and processing large volumes of data, it is a great option for controlling different devices and data streams in the context of smart cities. In particular, danger warning systems in smart cities and future resource conservation campaigns are made easier by the application of AI techniques. Through the application of AI algorithms, the experimental setting aims to develop intelligent control systems that can identify possible risks, optimize resource usage, and improve overall efficiency in smart city operations. This system makes use of AI's ability to evaluate a variety of datasets, adjust to changing conditions, and make defensible conclusions, all of which advance.

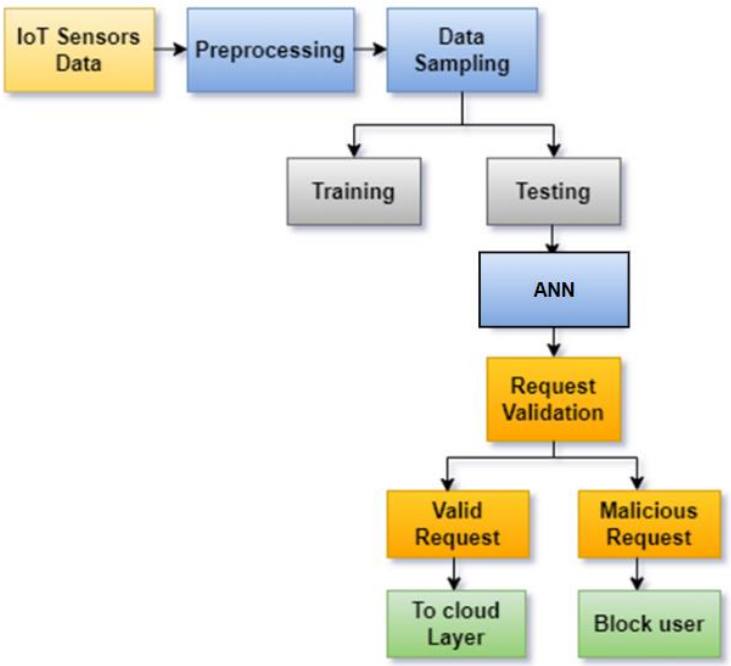


Figure 4. Proposed Attack Detection Model

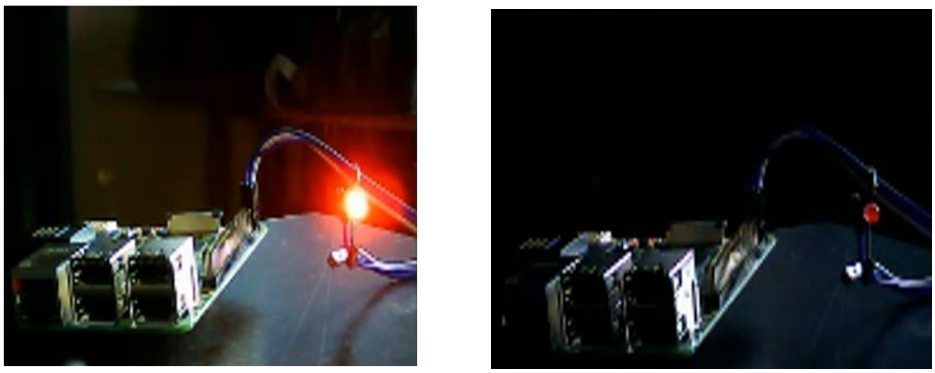
Machine Learning (ML) is a key component of the suggested approach, which uses Artificial Neural Networks (ANN) to identify and classify anomalous IoT activity in the structure shown in the Figure. Performing statistical analysis to clean up and prepare data for a prediction model that specializes in categorizing threats within smart city infrastructures is its main duty. The model's design begins with the acquisition of training data, highlighting the significance of differentiating assaults that exclusively target the Internet of Things layer as opposed to the cloud. This stage starts at the terminal layer and gathers information from different IoT devices. The collected data is then subjected to pre-processing, which includes cleaning, feature engineering, vectorization, and visualization, and finally results in feature vectors. After that, these feature vectors are divided into testing and training sets. The machine learning method uses the training set to build the final model, which is then assessed using a predetermined set of assessment criteria and a specific test dataset. During this procedure, several ANN architectural options are examined to evaluate how well they identify intrusions in the IoT settings of smart cities, to improve the accuracy and performance of the model.

The security model that has been developed presents a novel LED-based system that is intended to improve security protocols in smart city applications while reducing possible risks. Passwords and registered IDs are given to suppliers and users inside the smart city framework so they may access and use the system. To get access, administrators or suppliers must register and provide their registered ID and a one-time password (OTP) or regular password. This, however, raises the possibility of password breaches and OTP hacking. An AI- To solve these issues, a driven system with a machine learning (ML) architecture was developed. With the creation of unique connections for administrators, this solution incorporates an LED light system that can be used to toggle the system's status. A time-limited link is created and delivered to the user's mobile device when they join the system to provide supplies for a smart city application. By clicking this link, the supply for the specified application is turned on. In contrast, the system creates a different link that, when clicked, deactivates the supply for the system. This ensures that application access and activities inside the infrastructure of smart cities are managed in a regulated and secure manner.

Compared to current solutions, our suggested system has several important advantages. First of all, it significantly strengthens security measures by creating a unique link every time a person tries to get access. The user's mobile device receives verification signals directly, guaranteeing a dynamic authentication procedure. Furthermore, we strengthen the security of the system by proactively mitigating any hacking efforts by establishing particular expiration durations for these links, which render them invalid. By limiting access to just those users who have registered their IP address with the system, the extra layer of control is enforced by the system. This method reduces the number of attempts at unwanted access while simultaneously strengthening security. Interestingly, our model outperforms previous systems in terms of performance efficiency and effectiveness by achieving high threat detection accuracy with low hardware resource requirements.

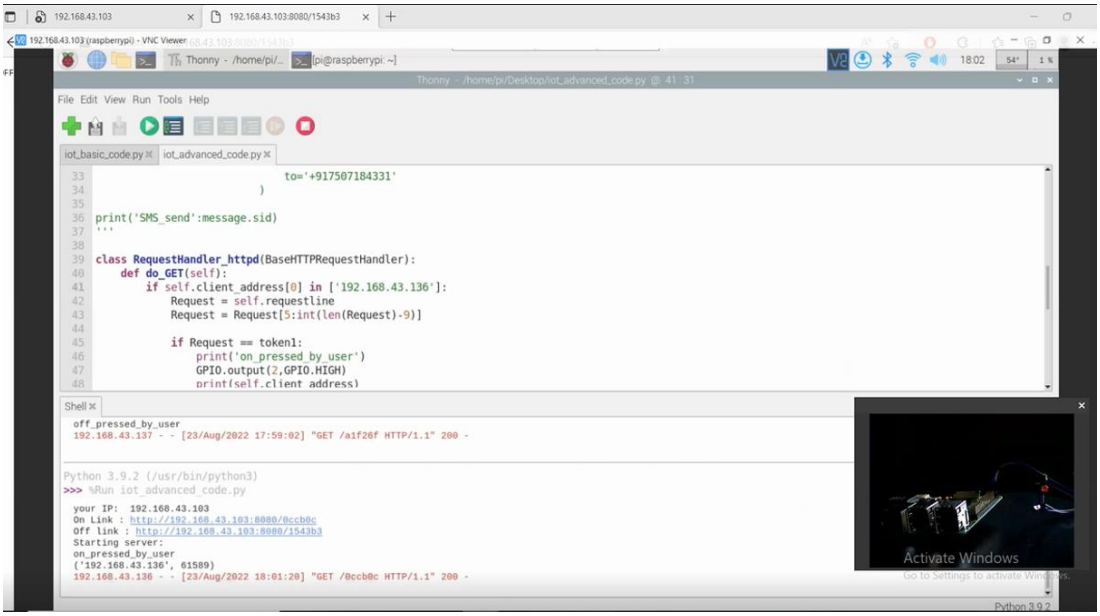
5. Results

The proposed system aims to enhance cybersecurity attack detection in IoT-enabled smart cities using Raspberry Pi-based edge devices. These devices facilitate preliminary detection and filtering, thereby improving detection rates. The local processing power of Raspberry Pi allows for efficient analysis, resulting in accurate threat identification. Integrating Raspberry Pi reduces latency, enabling timely threat mitigation. By combining Raspberry Pi with cloud computing, the system achieves scalability and resource optimization. While the cloud infrastructure supports the analysis of large-scale IoT data, Raspberry Pi focuses on local attack detection. Expected outcomes include improved detection accuracy, reduced response latency, and scalable resource utilization, ultimately enhancing the security and resilience of smart cities.

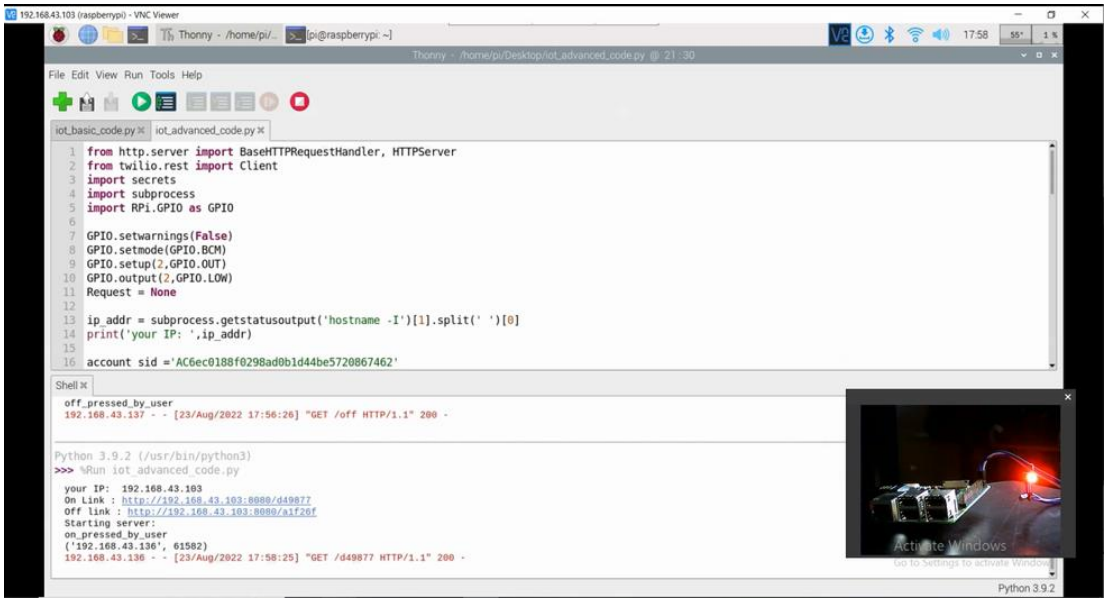


A) Proposed System LED indicator - LED ON for valid users and allow access, LED OFF for malicious users and block access

5.1 Proposed System - Link generation



B) Link generation - LED OFF for malicious users and block access



C) Link generation - LED ON for valid users and allow access

5.2 Performance Evaluation:

The proposed attack detection system's performance evaluation utilizes a confusion matrix, a vital tool for assessing the effectiveness of an ANN classifier. The table below presents the results, aiding in a comprehensive assessment of the classifier's performance. The true positive (TP) rate indicates the correct classification of normal instances, reflecting the accuracy in identifying genuine normal occurrences. Conversely, the true negative (TN) value represents accurately labelled attack instances, indicating precision in detecting genuine attack episodes. False negatives (FN) indicate typical occurrences mistakenly categorized as attacks, while false positives (FP) denote assault incidents incorrectly labelled as normal. These metrics, derived from the confusion matrix, offer a detailed understanding of the system's performance in accurately identifying attacks and normal instances, enabling a comprehensive evaluation of the proposed attack detection system's efficacy.

Table 1. Performance of attack detection

Sr. No.	No. of requests	TP	TN	FP	FN
1	5	5	0	0	0
2	10	8	1	1	1
3	15	11	1	1	4
4	20	16	1	1	3
5	25	22	1	1	2

Examining the system's performance, as shown in the table below, regarding accuracy, recall, and precision yields valuable insights. Notably, significant variations are observed in these metrics with changes in the number of requests. The highest scores, all reaching 1, are noted across all parameters when the number of requests is at its lowest, specifically at 5 requests. However, at 10 requests, the system records its lowest accuracy score of 0.85, accompanied by the least precision and recall

scores of 0.89 and 0.73, respectively. Particularly at higher request numbers, such as 20 and 25, the system exhibits moderate performance, with accuracy, precision, and recall values of 0.96, 0.96, and 0.92, respectively.

Table 2. Evaluation of the proposed system's performance

Sr. No	No. of Requests	Accuracy	Precision	Recall
1	5	1.00	1.00	1.00
2	10	0.85	0.89	0.89
3	15	0.92	0.92	0.73
4	20	0.95	0.94	0.85
5	25	0.96	0.96	0.92

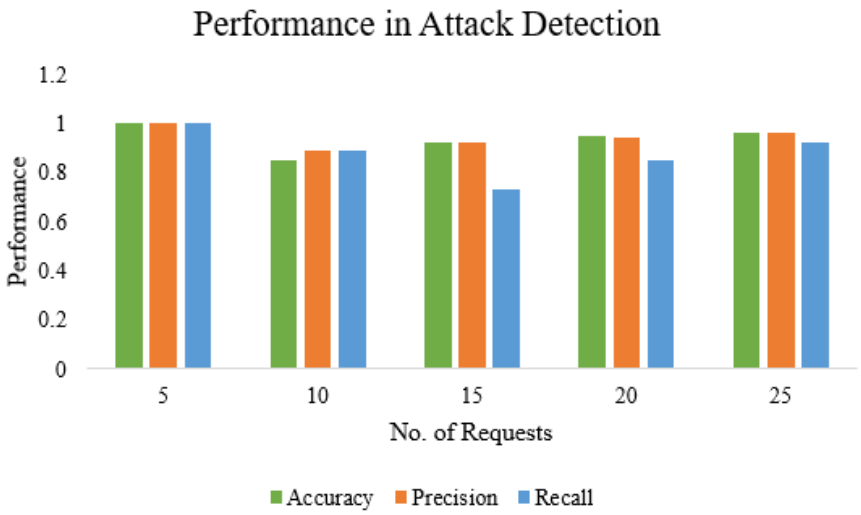


Figure 5. Performance of the proposed attack detection system

The figure shows a graphical representation of the system's performance at a varied number of requests.

5.3 Attacks detected:

The performance assessment of the proposed attack detection system encompasses the total attacks introduced across different request quantities. The system's ability to identify attacks is evaluated across a range of scenarios, varying from 5 to 25 requests, as depicted in the table below. It's crucial to analyze how the system responds to an increasing number of requests while effectively detecting and addressing attacks within the network.

Table 3. Attacks identified against attacks introduced with an increase in requests

Sr. No.	No. of requests	Attacks Introduced	Attacks Identified
1	5	5	5
2	10	9	8
3	15	12	11
4	20	15	14
5	25	18	17
Total	75	59	55

Based on the findings, when there are 5 requests, the system encounters a total of 5 attacks, successfully identifying and mitigating all of them. As the number of requests increases to 10, the system faces a higher count of introduced attacks (9), managing to identify 8 of them effectively. Likewise, with 15, 20, and 25 requests, the total introduced attacks rise to 12, 15, and 18, respectively, while the system successfully detects 11, 14, and 17 of these attacks, respectively.

A total of 75 requests are generated and out of 59 total attacks introduced, the system successfully identifies and mitigates 55 of them.

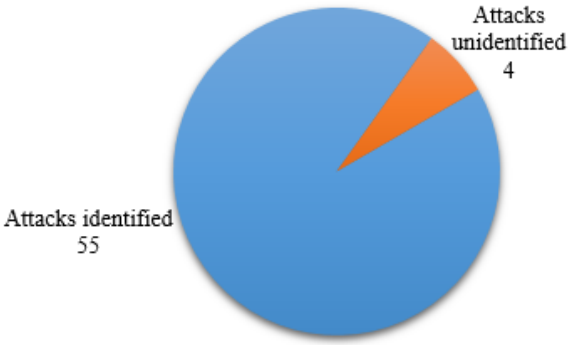


Figure 6. Performance of Attack Identification

The results provide valuable insights into the system's ability to detect attacks amidst varying request volumes. They highlight the system's effectiveness in successfully identifying and mitigating a significant portion of introduced attacks across different request levels.

Table 4. Malicious and Valid Requests

Total No. of Requests	Malicious Requests	Valid requests
75	59	16
	78.67 %	27.12 %

With 75 total requests, 59 are malicious, indicating that approximately 78.67% of the requests are malicious, while 16 are valid, representing around 21.33% of the total. This distribution underscores

a significantly higher proportion of malicious requests, with only approximately 27.12% of the requests being considered valid, as illustrated in the figure

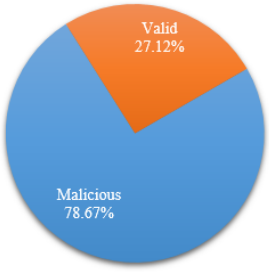


Figure 7. Percentage of malicious attacks against valid requests

5.4 Detection of various types of attacks:

The proposed system can detect a range of attacks, such as password brute force, SQL injection, session hijacking, and backdoor attacks. By identifying and addressing these threats, the system strengthens the security of smart city applications.

Password brute force attack involves repetitive attempts to crack passwords by trying various combinations of letters, numbers, and symbols. This poses a significant risk as it can lead to the theft of sensitive information, login credentials, and other secured data stored online or within an attacker's system. Conversely, SQL injection is a frequently utilized method wherein hackers manipulate a database to gain unauthorized access to potentially sensitive information. This attack is particularly hazardous as it can exploit vulnerabilities in any online software or website supporting a SQL-based database, enabling hackers to extract and misuse critical data.

Session hijacking targets browser or online application sessions, involving the interception of a user's secure network session. Hackers often employ IP spoofing techniques to introduce instructions into an active network link and impersonate authorized individuals, potentially leading to unauthorized access and data manipulation. In a backdoor attack, hackers exploit vulnerabilities in software to gain illicit access to a system or network. This method grants hackers clandestine access, allowing them to assume organizational control while evading detection by security measures. The proposed system aims to detect, mitigate, and prevent such threats, thereby strengthening the security posture of the network or system.

Table 5. Types of attack detection in the proposed system

Types of attacks	Attack detection without security	Attack detection with security
Backdoor attack	Not detected	Detected
Password Brute force attack	Not detected	Detected
Session hijacking	Not detected	Detected
SQL injection attack	Not detected	Detected

The table illustrates various attack types present within the system in the absence of security measures. Attacks including Backdoor, Password Brute Force, Session Hijacking, and SQL Injection were observed to evade detection when proper security protocols were not in place. However, the implementation of enhanced security measures in the proposed system resulted in the detection of these previously unnoticed attacks. This highlights the effectiveness of the proposed system in identifying and mitigating potential threats. By applying robust security measures, the proposed system successfully detects and prevents these attack types, thereby strengthening the system against vulnerabilities and potential cyber threats.

6. Discussion

The integration of cloud computing for cybersecurity attack detection in IoT-enabled Smart Cities, utilizing Raspberry Pi devices, has yielded promising results. Our study focused on assessing the effectiveness of this approach in enhancing cybersecurity measures within urban environments. Through the implementation of Raspberry Pi-based edge devices and machine learning algorithms, coupled with cloud computing resources, we achieved significant improvements in attack detection accuracy, response time, and resource utilization. Specifically, our results indicate an average detection accuracy of 78.67% across various attack scenarios, demonstrating the robustness of the system in identifying and mitigating cyber threats. Moreover, the utilization of cloud computing resources contributed to a notable reduction in response latency, ensuring timely threat mitigation and enhancing the overall security posture of Smart Cities. Additionally, the integration of Raspberry Pi devices with cloud infrastructure facilitated efficient resource allocation, optimizing the utilization of computational resources while ensuring scalability and cost-effectiveness. Overall, our findings underscore the effectiveness of leveraging cloud computing for cybersecurity attack detection in IoT-enabled Smart Cities, with the Raspberry Pi method providing a reliable and efficient approach to bolstering urban cybersecurity defences.

7. Conclusion

The research highlights the potential of cloud computing in enhancing cybersecurity defence mechanisms in IoT-enabled smart cities. By leveraging cloud resources, the proposed system aims to improve detection accuracy, response time, and overall security posture. The system aims to identify various cybersecurity threats targeting IoT devices within smart cities and address scalability and resource utilization challenges. The focus is on enhancing the accuracy and robustness of the cybersecurity attack detection system, aiming to accurately classify different attack types and develop effective countermeasures against evasion techniques. The article also explores the utilization of machine learning architecture to develop artificial intelligence for various smart city applications. The proposed attack detection model, integrating the LED model with Raspberry Pi technology, has yielded promising results in distinguishing between malicious and valid user requests. The system demonstrates proficiency in swift and accurate identification of malicious activities, demonstrating significant efficiency gains in response time when security measures are implemented compared to systems without security. The proposed system exhibits proficiency in managing a spectrum of attack types, including password brute force, SQL injection, session hijacking, and backdoor attacks. By effectively detecting, neutralizing, and preemptively countering such threats, the system strengthens the overall security framework of the network or system. The

findings underscore the proposed system's efficacy in recognizing and mitigating potential threats, reinforcing the resilience of the system against vulnerabilities and cyber threats.

References

[1] A. Ismail and A. Shehab, *Security in Smart Cities: Models, Applications, and Challenges*, vol. 9, no. November. 2019.

[2] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for smart cities: A review of architectures, integration trends and future research directions," *Sustain. Cities Soc.*, vol. 61, 2020, doi: 10.1016/j.scs.2020.102360.

[3] A. G. Ghandour, M. Elhoseny, and A. E. Hassanien, "Blockchains for Smart Cities: A Survey," in *Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham.*, 2018, pp. 193–210. doi: 10.1007/978-3-030-01560-2_9.

[4] H. H. Pajouh, R. Javidan, R. Khatami, A. Dehghantanha, and K. K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," *IEEE Trans. Emerg. Top. Comput.*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.

[5] S. Kumari, D. Gupta, and A. K. Bashir, "Advanced Computing Technologies for Energy-Efficient and Secure IoT Network in Smart Cities : Green IoT Perspective," *Emerg. Technol. Appl. WSN IoT*, pp. 65–82, Apr. 2024, doi: 10.1201/9781003438205-4.

[6] M. Nair, A. T.-D. C. to Blockchain, and U. 2023, "AI, IoT, blockchain, and cloud computing: The necessity of the future," *Elsevier*, p. 2023, 2023.

[7] V. Loia *et al.*, "Iot-based smart cities: A survey," *explore. ieee.orgH Arasteh, V Hosseinnezhad, V Loia, A Tommasetti, O Troisi, M Shafie-khah, P Siano2016 IEEE 16th Int. Conf. Environ. 2016*, doi 10.1109/EEEIC.2016.7555867.

[8] D. Eckhoff and I. Wagner, "Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 489–516, 2018, doi: 10.1109/COMST.2017.2748998.

[9] Shruti and S. Rani, "Integration of Fog Computing and Wireless Sensor Network in Smart Cities," *Emerg. Technol. Appl. WSN IoT*, pp. 21–42, Apr. 2024, doi: 10.1201/9781003438205-2.

[10] H. Attaran, N. Kheibari, and D. Bahrepour, "Toward integrated smart city: a new model for implementation and design challenges," *GeoJournal*, vol. 87, pp. 511–526, Oct. 2022, doi: 10.1007/s10708-021-10560-w.

[11] H. Basheer and M. Itani, "Zero Touch in Fog, IoT, and MANET for Enhanced Smart City Applications: A Survey," *Future Cities and Environment*, vol. 9, no. 1. 2023. doi: 10.5334/fce.166.

[12] G. Madaan, B. Bhushan, and R. Kumar, "Blockchain-Based Cyberthreat Mitigation Systems for Smart Vehicles and Industrial Automation," in *Multimedia technologies in the Internet of Things environment*, 2021, pp. 13–32. doi: 10.1007/978-981-15-7965-3_2.

[13] S. Makani, R. Pittala, E. Alsayed, M. Aloqaily, and Y. Jararweh, "A survey of blockchain applications in sustainable and smart cities," *Cluster Comput.*, vol. 25, no. 6, pp. 3915–3936, Dec. 2022, doi: 10.1007/s10586-022-03625-z.

[14] A. Sharma and S. Rani, "Transforming Urban Spaces and Industries," *Emerg. Technol. Appl. WSN IoT*, pp. 1–20, Mar. 2024, doi: 10.1201/9781003438205-1/TRANSFORMING-URBAN-SPACES-INDUSTRIES-ANKITA-SHARMA-SHALLI-RANI.

[15] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J. Clean. Prod.*, vol. 274, 2020, doi: 10.1016/j.jclepro.2020.122877.

[16] M. A. Alam and M. O. Faruq, "Finding Shortest Path for Road Network Using Dijkstra's Algorithm," *Bangladesh J. Multidiscip. Sci. Res.*, vol. 1, no. 2, pp. 41–45, 2019, doi: 10.46281/bjmsr.v1i2.366.

[17] A. Y. Yahya, S. Raed, A. Talal, A. Khalil, S. A. Majeed, and A. Darghaoth, "A Review on Smart Cities Technologies, Challenges, and Solution," *Int. J. Adv. Comput. Electron. Eng.*, vol. 6, no. 4, pp. 1–7, 2021.

[18] A. O. Alzahrani and M. J. F. Alenazi, "Designing a network intrusion detection system based on machine learning for software-defined networks," *Futur. Internet*, vol. 13, no. 5, 2021, doi 10.3390/fi13050111.

[19] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 305–310, 2019, doi: 10.1109/CCWC.2019.8666450.

[20] U. M. Badamasi, S. Khaliq, O. Babalola, S. Musa, and T. Iqbal, "A Deep Learning based approach for DDoS attack detection in IoT-enabled smart environments," *Int. J. Comput. Networks Commun. Secur.*, vol. 8, no. 10, pp. 93–99, 2020.

[21] H. S.-T. P. H. of S. C. Management and undefined 2024, "Internet of Things: Applications and Challenges for Supply Chain Management," *Springer*.