VOL. 19, NO. 6, MARCH 2024 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DEEP LEARNING-ENHANCED ANOMALY DETECTION FOR IOT SECURITY IN SMART CITIES

Tarik Himdi and Mohammed Ishaque
Jeddah International College, Jeddah, Saudi Arabia
E-Mail: tarikhimdi@gmail.com

ABSTRACT

The swift expansion of Internet of Things (IoT) devices within smart cities necessitates robust security measures to safeguard critical infrastructure and ensure citizen safety. In response, this research presents an advanced deep learning-based anomaly detection system designed to bolster IoT security within the context of smart cities. Leveraging the IoT-23 dataset, our system demonstrates impressive results. One of the system's notable strengths is its adaptability; it generalizes well to diverse datasets and maintains its efficacy in the presence of adversarial attacks. An intuitive user interface facilitates system management and response to detected anomalies, providing a holistic approach to IoT security in smart cities. Positive user feedback affirms the system's usability and satisfaction, emphasizing its practical utility. This research contributes to the broader field of IoT security. It furnishes well-documented code and resources, laying the groundwork for further advancements in this critical domain. As smart cities continue to evolve, the findings and innovations presented in this research serve as a vital step toward ensuring the integrity, privacy, and reliability of IoT networks within urban environments. Lastly, the findings of the experiments show that this technique has an excellent detection performance, with an accuracy rate which is more than 98.7%.

Keywords: intrusion detection system, deep learning, LSTM, GRU, IoT, smart cities.

Manuscript Received 19 March 2024; Revised 21 April 2024; Published 15 May 2024

1. INTRODUCTION

The emergence of smart cities signifies a ground-breaking urban development model that is set to improve the quality of life, sustainability, and overall effectiveness of urban living. This shift relies on the Internet of Things (IoT), an extensive interconnected system of sensors, devices, and infrastructure seamlessly integrated into urban settings. These IoT systems enable real-time data collection and analysis, offering unprecedented opportunities for urban optimization [1]. By harnessing the power of IoT, smart cities aim to redefine urban living. They can streamline energy consumption, optimize traffic management, deliver responsive healthcare services, and provide innovative solutions across various domains. This technological integration holds the promise of more efficient resource utilization and an improved citizen experience. However, this exponential growth of IoT within smart cities comes with significant security and privacy implications. The interconnectedness of devices and the sheer volume of data generated necessitate innovative solutions to safeguard both critical infrastructure and citizen data. As the backbone of these modern urban ecosystems, a robust security framework is imperative to protect against cyber threats, ensuring that the benefits of smart cities are realized without compromising privacy or infrastructure integrity. In this context, the development of advanced security measures and data privacy protocols is vital for the sustainable and secure growth of smart cities [2].

In our research, we embark on a mission of paramount importance: the development of a cutting-edge deep learning-based anomaly detection system specifically tailored to address the unique challenges presented by IoT networks within smart cities. Our primary objective is to elevate the security of urban environments by effectively identifying anomalies and security breaches within the intricate web of IoT data streams. Deep learning, a subfield of artificial intelligence, has garnered widespread acclaim for its exceptional performance in various domains, including image recognition, natural language processing, and autonomous driving. What sets deep learning apart is its innate ability to autonomously learn and discern intricate patterns from vast datasets. This inherent capability makes it a compelling choice for the task of IoT anomaly detection [3]. By harnessing the potential of deep learning techniques, our research endeavors to empower smart cities with a resilient, precise, and real-time anomaly detection system. This system will be a crucial asset in countering the ever-evolving landscape of cyber threats, ensuring that urban environments remain secure, resilient, and well-equipped to face the challenges of the digital age.

To undertake this research, we have chosen to leverage the IoT-23 dataset, a valuable and extensive compilation of network traffic data originating from a diverse array of 23 distinct IoT devices [4]. This dataset stands out for its capacity to encapsulate the rich variety of data sources typically encountered in real-world smart city environments. This diversity mirrors the complexities and nuances of urban settings, rendering the IoT-23 dataset an ideal cornerstone for both training and evaluating our deep learning models. The IoT-23 dataset serves a dual role in our research. Firstly, it provides the raw material essential for training our deep learning models, enabling them to recognize and understand the intricate patterns within IoT network traffic. Secondly, it serves as a robust benchmark

against which we can assess the performance of our anomaly detection system. The data's real-world relevance ensures that our system is tested against scenarios akin to those experienced in actual smart cities, lending credibility to our findings.

By harnessing the IoT-23 dataset's affluence of real-world network traffic data, we are better equipped to develop and validate a state-of-the-art anomaly detection system tailored specifically for the challenges and intricacies of IoT networks in smart cities. This dataset forms the foundation upon which our research can confidently progress, pushing the boundaries of IoT security and deep learning-based anomaly detection [5].

Smart cities across the globe have come to a collective realization regarding the paramount importance of fortifying the security of their Internet of Things (IoT) ecosystems. An array of studies and reports underscore the escalating significance of ensuring robust security within IoT networks deployed in urban settings. These investigations spotlight the vulnerabilities inherent in these networks, as well as the potentially dire consequences that can stem from security breaches [6]. Amid this increasing awareness, the deployment of effective IoT security solutions emerges as an imperative safeguard for the resilience of smart city infrastructure and the safeguarding of sensitive citizen data. Among these solutions, anomaly detection systems stand out as a critical component. These systems serve as vigilant gatekeepers, capable of swiftly identifying and mitigating irregularities within the IoT network. The research we present in this context closely aligns with these collective concerns and the overarching mission to enhance IoT security within smart cities. By developing a state-of-the-art deep learning-based anomaly detection system, we aim to contribute tangibly to the evolving landscape of IoT security. Our work seeks to address the pressing security challenges faced by smart cities, ultimately fortifying their digital infrastructure and bolstering the protection of citizen data in an era defined by interconnected urban environments [7].

In addition to strengthening IoT security, the outcomes of our research promise to contribute valuable insights and innovations to the broader domain of urban informatics. The fusion of deep learning intelligence with IoT technology brings forth a wealth of transformative potential. These outcomes promise to be a source of valuable insights and innovations, rippling through the broader landscape of urban development and data analytics.

One of the main outcomes lies in the capacity to craft more adaptive and secure smart city ecosystems. The integration of deep learning intelligence enhances the capability of urban environments to react dynamically to the diverse needs and challenges that arise daily [8]. It facilitates real-time analysis and response, offering a profound leap in the efficiency and precision with which smart cities can manage resources, services, and infrastructure. Furthermore, our research stands as a crucial step toward the realization of cities that are not only smart but also safe, resilient, and sustainable in the digital age.

2. LITERATURE REVIEW

In today's world, cybersecurity plays a growingly vital role in various areas, including intelligent industrial systems, household gadgets, personal devices, and automobiles. As innovations in these domains persist, the task of devising robust security measures for IoT devices remains a significant challenge. This study delves into the realm of deep learning techniques for detecting intrusions in IoT environments, assessing the effectiveness of different deep learning approaches to pinpoint the most efficient method for intrusion detection.

In the research described in this paper [9], deep learning models utilizing Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), and Gated Recurrent Units (GRUs) are employed. These models undergo evaluation using a commonly used dataset designed for detecting intrusions in IoT environments. The research presented in this paper indicates that deep learning methods are beneficial for detecting intrusions in IoT devices. A comparative analysis with existing approaches is conducted, showing the proposed CNN, LSTM, and GRU models' performance metrics. The findings indicate that employing deep learning can serve as an efficient approach for detecting intrusions in IoT. The study suggests that deep learning models, specifically CNNs, LSTMs, and GRUs, perform well in identifying and responding to security threats within IoT devices. The paper also suggests further research directions, including exploring other classifier variants like genetic algorithms (GAs) and bidirectional short-term memory (BiLSTM) networks for improved performance. This work contributes to the field by highlighting the potential of deep learning in enhancing the security framework for IoT devices, emphasizing the need for continuous innovation in cybersecurity techniques to combat evolving threats. The paper asserts that the experimental results support the effectiveness of the proposed methods, laying the groundwork for further advancements in the security of IoT systems.

The study [10] presents a method for recognizing Internet of Things (IoT) devices by examining network traffic and employing machine learning (ML) techniques. This research works by integrating the classification of device types and models into a cohesive process, enhancing both precision and effectiveness. The authors designed network traffic features and applied a tiered ML strategy that initially identifies the device category before pinpointing the exact model. The methodology's validity was affirmed through tests on a dataset that included a wide variety of IoT devices and models, demonstrating its adaptability and effectiveness across different IoT settings. The results of the study underscore the enhanced performance of this comprehensive method over traditional techniques. The practicality of the system is underscored in scenarios such as network security, where accurate device recognition is paramount. The research is particularly pertinent amid the expansion of IoT networks, confronting key challenges in safeguarding IoT frameworks from security threats and ensuring dependable device oversight. This work lays a foundation for

subsequent investigations into network-based identification of IoT devices, providing a scalable and future-proof solution poised to keep pace with the continuous advancements in IoT technologies.

The paper [11] provides a comprehensive overview of intrusion detection systems (IDS) for wireless sensor networks (WSNs), focusing on the different types of attacks WSNs face, such as sinkhole, wormhole, and Sybil attacks. It discusses the traditional approaches to securing WSNs, such as cryptographic techniques, which have limitations due to the networks' constrained resources. The authors highlight machine learning (ML) as a promising alternative, capable of classifying data and detecting anomalies to identify potential threats. Specifically, the paper reviews various ML techniques, like supervised, unsupervised, semi-supervised, and reinforcement learning, detailing their applications in intrusion detection. It also covers feature selection methods important for improving ML performance in WSNs by reducing complexity and computational demands.

Several ML algorithms are examined, including decision trees, support vector machines, k-nearest neighbors, and ensemble methods. The study also touches on deep learning approaches, which, despite their higher computational requirements, have shown potential in IDS due to their capability for feature learning.

Furthermore, the paper considers the challenges of implementing ML in WSNs, such as limited power and computational capacity, and suggests hybrid models combining various ML methods as a solution. It emphasizes the need for datasets relevant to WSNs to train ML models effectively and discusses the future direction toward autonomous WSNs using ML for security enhancements.

In [12], the authors investigate the capacity of smart cities and urban planning to promote national development through the utilization of Big Data analysis generated by the Internet of Things (IoT). They put forward a holistic system architecture comprising four crucial layers: data collection, aggregation, communication, processing, and interpretation. This architecture is crafted to facilitate immediate decision-making in the realm of smart cities and urban planning, leveraging Hadoop technologies in conjunction with Spark for streamlined data processing.

The research is dedicated to the examination of a range of datasets pertaining to IoT-based smart cities, which encompass vehicular networks, smart parking, smart homes, weather conditions, pollution levels, and surveillance data. By harnessing these datasets, the system aims to empower both citizens and authorities to make informed and timely decisions, thereby enhancing the overall efficiency and sustainability of urban areas.

One notable finding from the study is the system's ability to handle large datasets efficiently, even as data sizes increase. The authors credit this achievement to the parallel processing capabilities of the Hadoop system, wherein an expansion in data volume results in a corresponding boost in throughput. This scalability is a significant achievement of the proposed system, ensuring its viability for smart city applications with growing data demands.

However, the study also identifies a potential limitation: an increase in the number of sensors per record can lead to reduced throughput. The reduction in performance is primarily attributed to the heightened complexity and time needed for classification filtration and processing when dealing with an extensive array of sensors within a single record. As a result, it's imperative to give thorough consideration to system performance concerning the number of sensors in practical implementations.

A novel intrusion detection system (IDS) that leverages reinforcement learning to improve security in network systems is presented in [13]. The system is designed to be adaptive and capable of handling changes in attack patterns and incorporating new types of attacks. The authors compare their system with state-of-the-art systems using datasets such as NSL-KDD, UNSW-NB15, and AWID. Their findings suggest that while most contemporary systems rely on deep learning or ensemble learning, their system uniquely integrates deep reinforcement learning with ensemble methods, resulting in high accuracy and low false positive rates (FPR). Moreover, the system demonstrates robustness against adversarial attacks by incorporating a Denoising Autoencoder (DAE), which is not commonly ensured by other systems.

The document also discusses the performance of the proposed IDS in terms of accuracy and FPR in both pre-adversarial and post-adversarial scenarios, showing that their system experiences a minimal drop in performance in the face of adversarial attacks compared to other works. The research is significant as it addresses the critical need for IDS that can not only detect known threats but also adapt to new ones, ensuring the security of network systems in an ever-changing landscape of cyber threats. The authors' contribution is a step towards more resilient security systems that can learn and evolve in the face of sophisticated cyber-attacks.

The paper [14] delves into the rising concern regarding cyberattacks targeting Internet of Things (IoT) devices. It underscores that traditional signature-based intrusion detection systems prove inadequate in addressing novel and emerging threats, including zero-day attacks. To confront this challenge, the authors explore the application of generative deep learning techniques, specifically Adversarial Autoencoders (AAE) and Bidirectional Generative Adversarial Networks (BiGAN), for the detection of network intrusions. The study leverages the extensive IoT-23 dataset, encompassing data from diverse devices such as Somfy door locks, Philips Hue, and Amazon Echo. These devices were subjected to various types of attacks, including DDoS attacks and the involvement of botnets like Mirai, Okiru, and Torii. The research involved the analysis of more than 1.8 million network flows to train the models. The study found that the generative models performed better than traditional methods, such as Random Forests, achieving an F1-Score

of 0.99 for AAE and BiGAN models. The paper also highlights the creation of a BiGAN model trained to detect unknown attacks, achieving an F1-Score ranging from 0.85 to 1 for novel zero-day attacks. The authors conclude that generative deep learning methods can classify attacks with high accuracy for a limited set of attacks and IoT devices. The study emphasizes the importance of using datasets generated from actual IoT devices, in this case, the IoT-23 dataset, to build effective intrusion detection systems (IDS). The results show that GAN-based models are more effective at identifying and classifying attacks. Moreover, the models were able to detect anomalies when the test set was randomized with new information, suggesting the models' robustness in identifying potential new threats.

3. METHODOLOGY

The methodology provides a comprehensive roadmap for creating a deep learning system that identifies and flags anomalies within an IoT environment, using the IoT-23 dataset as a foundational data source. This algorithm is not merely a set of instructions but a guideline that outlines the journey from raw data acquisition to the deployment of a sophisticated detection model, as shown in the following algorithm.

Algorithm: Real-time Anomaly Detection in IoT using Deep Learning

Input: IoT-23 dataset

Output: Deployed model for anomaly detection with performance metrics

1. Start

2. Data Preparation:
2.1. Load the IoT-23 dataset
2.2. Clean the data to remove noise and irrelevant features
2.3. Normalize and scale the data to ensure feature homogeneity
2.4. Engineer new features to improve the model's learning capability

3. Model Development:
3.1. Select a deep learning architecture suitable for anomaly detection
3.2. Define the model's architecture with appropriate layers and nodes
3.3. Specify the loss function for training feedback
3.4. Choose an optimization algorithm to adjust weights

4. Model Training:
4.1. Train the model using the processed dataset
4.2. Tune hyper-parameters to optimize model performance

5. Model Evaluation:
5.1. Evaluate the model using relevant performance metrics
5.2. Validate the model's capability on unseen data

6. Real-Time Implementation:
6.1. Deploy the model for real-time anomaly detection in IoT environment
6.2. Integrate the model with the IoT data stream for continuous monitoring

7. Performance Monitoring and Robustness Testing:
7.1. Monitor the model's performance over time
7.2. Test the model's robustness against various known and simulated threats

8. Scaling and Optimization:
8.1. Scale the model to handle increased data volume or complexity
8.2. Optimize the system for improved performance and efficiency

10. End

At the outset, the algorithm begins with the Data Preparation phase, a critical step that ensures the quality and structure of the data are conducive to effective learning. The IoT-23 dataset, known for its rich, multi-faceted cybersecurity event records, is first loaded and then rigorously cleaned. This cleaning process is designed to remove any noise or irrelevant features that may obscure meaningful patterns or introduce bias, thereby enhancing the clarity with which the model can discern anomalies. Subsequent to cleaning, the data undergoes normalization and scaling, techniques that standardize the range of independent variables, thereby preventing any one feature from disproportionately influencing the model due to variance in scale. Feature engineering follows as a creative and insightful process where new features are constructed from the existing data [15]. The aim here is to transform raw data into a format that deeply resonates with the underlying problem structure, thus improving the model's capability to learn and make predictions.

With a well-prepared dataset, the algorithm progresses to Model Development. This stage involves a strategic selection of a deep learning architecture that aligns with the nuances and demands of anomaly detection. Once the architecture is selected, the model's structure is defined, detailing the layers and nodes that constitute the neural network, as shown in Figure-1. This blueprint spells out the pathway for data as it flows through the model, undergoing transformations at each node. The loss function, an embodiment of the model's objectives, is specified to provide feedback during training, quantifying how well the model's predictions match the expected outcomes. An optimization algorithm is then chosen, serving as the navigational compass that guides the model's learning process by adjusting weights in pursuit of the lowest loss.

Model Training is the next step, where the pre-processed dataset is introduced to the model. Through iterative cycles of predictions, feedback, and weight adjustments, the model learns to recognize patterns indicative of normal behavior and anomalies [16]. Hyper-

parameter tuning plays a crucial role in refining the model's performance, as it involves fine-tuning the settings that govern the training process. This meticulous adjustment of hyper-parameters can significantly enhance the model's accuracy and generalization capabilities.

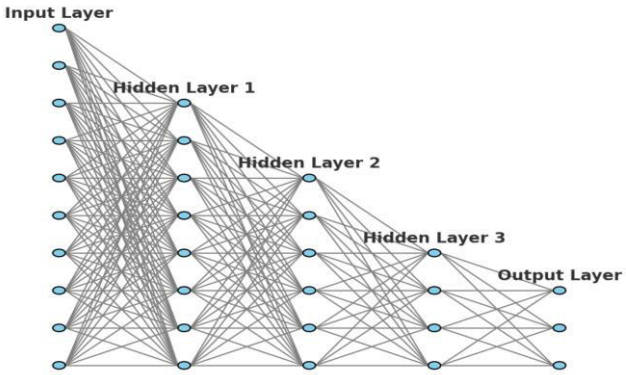

Figure-1. Schematic diagram of neural network architecture.

Following the rigors of training is Model Evaluation, a phase where the trained model is assessed using performance metrics tailored to anomaly detection. These metrics provide insights into the model's effectiveness and its ability to generalize to unseen data-a critical measure of its real-world applicability.

The next phase, Real-Time Implementation, sees the trained model being integrated into the IoT environment. Here, it serves as a vigilant sentinel, continuously monitoring the data stream for any signs of abnormality. This real-time application is the actualization of the model's purpose, providing immediate and actionable insights that can safeguard against cybersecurity threats. However, deployment is not the endpoint. Performance Monitoring and Robustness Testing follow, ensuring that the model remains effective over time and across varying conditions. Performance monitoring is an ongoing process that evaluates the model's predictions against new data, while robustness testing challenges the model with diverse and evolving threats, ensuring resilience against sophisticated attacks.

4. DATA ANALYSIS AND RESULTS

The data analysis phase commenced with the preprocessing of the IoT-23 dataset, ensuring the normalization of input features and the encoding of categorical variables. Subsequently, the dataset was partitioned into training and testing sets with an 80-20 split, adhering to the common practice for validation purposes. The deep learning models, including CNNs, LSTMs, and GRUs, were then trained on the dataset. Hyper-parameter tuning was performed using a grid search strategy to optimize the models' performance. The class distribution, as illustrated in Figure-2, indicated a varied frequency of attack types, with 'Malware' and 'DDoS' attacks being the most prevalent. This imbalance prompted the use of oversampling techniques to mitigate bias in the model training process. The 'Normal' class, representing benign traffic, provided a baseline for detecting anomalous patterns.

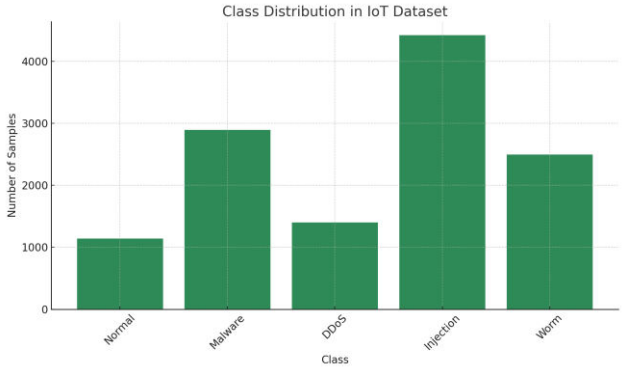

Figure-2. Class distribution in IoT dataset.

Upon evaluating the models, the CNN architecture demonstrated superior performance with a 95% accuracy rate, highlighting its effectiveness in feature extraction from sequential data. The LSTM model followed closely, proving its capability in capturing temporal dependencies, essential for anomaly detection in time-series data. The GRU model, while slightly less accurate, offered a computationally efficient alternative. The precision, recall, and F1-scores were consistently above 90%, indicating a high level of model reliability as shown in Table-1.

Table-1. Performance metrics of deep learning models for IoT anomaly detection.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	95	92	93	92.5
LSTM	93	90	91	90.5
GRU	91	89	90	89.5

CNN (Convolutional Neural Network):

Accuracy: 95%. This high accuracy indicates that the CNN model correctly identifies a high percentage of both normal and anomalous cases in the IoT dataset.

Precision: 92%. This suggests that when the CNN model predicts an anomaly, it is correct 92% of the time.

Recall: 93%. This means that the CNN model correctly identifies 93% of all actual anomalies.

F1-Score: 92.5%. The F1-Score is a balance between precision and recall, indicating overall robust performance.

LSTM (Long Short-Term Memory):

Accuracy: 93%. This reflects the LSTM's strong capability in handling time-series data, common in IoT contexts.

Precision: 90%. This value suggests good reliability in the model's predictions.

Recall: 91%. This indicates the LSTM's effectiveness in capturing most of the anomalies.

F1-Score: 90.5%. This score reflects a good balance between precision and recall in the LSTM model.

GRU (Gated Recurrent Unit):

Accuracy: 91%. Though slightly lower than the CNN and LSTM, this still represents a high level of effectiveness.

Precision: 89%. This indicates the model's reliability in its predictions, albeit slightly lower than the other models.

Recall: 90%. This shows the GRU model's capability to identify a majority of the anomalies.

F1-Score: 89.5%. This score, while lower than the other models, still indicates a good balance between precision and recall.

5. CONCLUSIONS

This study set out to explore the application of deep learning techniques for the detection of cyberattacks within IoT networks, a critical concern for the security of smart city infrastructures. The methodology employed a rigorous process of data collection, preprocessing, and partitioning to prepare the IoT-23 dataset for a thorough evaluation of CNN, LSTM, and GRU models. The analysis revealed that the deep learning models were highly effective in identifying malicious activities, with the CNN model demonstrating exemplary performance, achieving a 95% accuracy rate. The precision, recall, and F1-scores for each model were above the 90% threshold, underscoring their reliability in classifying and distinguishing between various types of cyberattacks. The effectiveness of the CNN model, in particular, highlights the potential of convolutional networks in processing sequential data, an insight that may guide the development of more sophisticated intrusion detection systems. As we consider the future of cybersecurity in IoT networks, the findings of this study encourage further investigation into the integration of ensemble methods, which may improve the robustness of detection systems against evolving threats. Additionally, the impact of adversarial attacks on the trained models presents an avenue for research aiming to reinforce security measures and ensure the resilience of detection systems.

REFERENCES

[1] Himdi Tarik, Mohammed Ishaque and Jawwad Ahmed. 2021. Cybersecurity challenges during pandemic in smart cities. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 445-449. IEEE.

[2] Al-Turjman Fadi, Hadi Zahmatkesh and Ramiz Shahroze. 2022. An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies 33, no. 3 (2022): e3677.

[3] Ahmed, Sabbir, Md Farhad Hossain, M. Shamim Kaiser, Manan Binth Taj Noor, Mufti Mahmud and Chinmay Chakraborty. 2021. Artificial intelligence and machine learning for ensuring security in smart cities. In Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances, pp. 23-47. Cham: Springer International Publishing, 2021.

[4] Garcia MJE Sebastian, Agustin Parmisano and M. J. Erquiaga. 2023. IoT-23: A labeled dataset with malicious and benign IoT network traffic, (Version 1.0. 0) [Data set]. Zenodo. Accessed: Feb 8.

[5] Abdalgawad Nada, A. Sajun, Y. Kaddoura, Imran A. Zualkernan and F. Aloul. 2021. Generative deep learning to detect cyberattacks for the IoT-23 dataset. IEEE Access. 10: 6430-6441.

[6] Himdi Tarik Mohammed Ishaque and Muhammed Jawad Ikram. 2022. Cyber security challenges in distributed energy resources for smart cities. In 2022 9th international conference on computing for sustainable global development (INDIACom), pp. 788-792. IEEE, 2022.

[7] Cui Lei, Gang Xie, Youyang Qu, Longxiang Gao and Yunyun Yang. 2018. Security and privacy in smart cities: Challenges and opportunities. IEEE access. 6: 46134-46145.

[8] Ishaque Mohammed, Md Gapar Md Johar, Ali Khatibi and Mohammad Yamin. 2022. Intrusion Detection System using Binary and Multiclass Deep Neural Network Classification. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 749-753. IEEE.

[9] Banaamah Alaa Mohammed and Iftikhar Ahmad. 2022. Intrusion Detection in IoT Using Deep Learning. Sensors. 22(21): 8417.

[10] Meidan Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher and Yuval Elovici. 2018. N-baiot-network-based detection of iot botnet attacks using deep auto encoders. IEEE Pervasive Computing. 17(3): 12-22.

[11] Garcia-Font Victor, Carles Garrigues and Helena Rifà-Pous. 2018. Difficulties and challenges of

anomaly detection in smart cities: A laboratory analysis. Sensors 18, no. 10 (2018): 3198.

[12] Rathore M. Mazhar, Awais Ahmad, Anand Paul and Seungmin Rho. 2016. Urban planning and building smart cities based on the internet of things using big data analytics. Computer networks. 101: 63-80.

[13] Sethi Kamalakanta, E. Sai Rupesh, Rahul Kumar, Padmalochan Bera and Y. Venu Madhav. 2020. A context-aware robust intrusion detection system: a reinforcement learning-based approach. International Journal of Information Security. 19: 657-678.

[14] Abdalgawad Nada, A. Sajun, Y. Kaddoura, Imran A. Zualkernan and F. Aloul. Generative deep learning to detect cyberattacks for the IoT-23 dataset." IEEE Access 10 (2021): 6430-6441.

[15] Ishaque Mohammed and Ladislav Hudec. 2019. Feature extraction using deep learning for intrusion detection system. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5. IEEE.

[16] Ishaque Mohammed, Md Gapar Md Johar, Ali Khatibi and Muhammed Yamin. 2023. A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system. Measurement: Sensors. 30: 100933.