JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CRNNs FOR AN EFFECTIVE CYBER THREAT DETECTION IN SMART CITIES

T. Udhayakumar
Assistant Professor
Department of Computer science and Engineering
Rathinam technical campus, India

B. Sharmila
2nd Year ME Biometrics and Cyber Security
Department of Computer science and Engineering
Anna university, India

Abstract **:** The extensive implementation of Internet of Things (IoT) applications has aided in the growth of smart cities. These cities employ smart applications to optimize operational efficiency, thereby improving service quality and public health. To reduce the risks associated with IoT cybersecurity in smart cities, I present in this research an attack and anomaly detection method based on machine learning techniques. Notably, I chose Convolutional Recurrent Neural Networks (CRNNs) from the various available machine learning (ML) techniques. Because CRNNs combine the best features of Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), CNNs allow us to study sequential data and extract spatial characteristics, making them ideal for visual data analysis. RNNs, on the other hand, capture temporal dependencies and analyse sequential data. By Combining both CNNs and RNNs I can achieve comprehensive cybersecurity. Results from experiments using the most current attack dataset show that the suggested method can successfully detect cyberattacks and outperform findings from previous research.

Keywords: Cybersecurity, ML, CNNs, threat detection, LSTM,1D Convolutional neural networks, K-Fold Cross validation, confusion Matrix, anomaly detection.

1) INTRODUCTION:

a. **Introduction:** The rise of the Internet of Things (IoT) is weaving a web of interconnected devices, transforming them into intelligent sensors and actuators that collect data and respond to the needs of a city. This paves the way for the development of smart cities, urban environments that leverage technology to improve efficiency, sustainability, and the overall well-being of their citizens. Imagine traffic lights that adjust based on real-time congestion, or waste collection routes optimized to avoid overflowing bins. This is the power of IoT in action. Sensors embedded in everything from buildings to streetlights gather valuable data, providing insights into city operations and resident needs. This data is then used to automate processes and make informed decisions, leading to a more responsive and resource-efficient urban landscape.

b. **Background and Motivation:** The motivation behind this research stems from the imperative to develop proactive approaches to cybersecurity in smart cities. The proliferation of Internet of Things (IoT) devices in smart cities presents a double-edged sword.

While these interconnected systems offer significant operational and sustainability advantages, they also introduce a burgeoning cyber threat landscape. The sheer volume of interconnected devices, often with limited security protocols, creates a vast attack surface for malicious actors. Sensitive data collected by these devices, encompassing traffic flow, energy consumption, and even personal information, becomes a tempting target for breaches or manipulation. The potential consequences of a successful cyberattack on a smart city are severe, ranging from disrupted traffic management and manipulated energy grids to complete paralysis of critical infrastructure. Smart city initiatives powered by the Internet of Things (IoT) face a significant hurdle: the sheer volume of data generated by edge devices (sensors, cameras, etc.). This data deluge can overwhelm traditional cloud-based architectures, leading to delays and congestion. The problem is further amplified when malicious attack detection relies on a centralized cloud system, causing bottlenecks and hindering real-time decision making.

c. **Research Objectives:** The section outlining the research objectives succinctly summarizes the anticipated outcomes of the study, guiding the research direction. These objectives include assessing the efficacy of ML algorithms in detecting cyber-attacks, identifying optimal methodologies, and juxtaposing the findings with conventional security approach. The objective of the research is to develop a new method for detecting cyberattacks in smart city applications that leverages the strengths of machine learning. The research proposes using Convolutional Recurrent Neural Networks (CRNNs) to analyze data from Internet of Things (IoT) devices in smart cities. CRNNs are chosen because they can combine the following:

Spatial feature extraction from CNNs: This allows the model to identify patterns in the data that might indicate an attack.

Temporal dependency analysis from RNNs: This allows the model to understand how the data is changing over time, which can also be helpful in identifying attacks.

By combining these capabilities, the CRNN-based method aims to achieve more comprehensive cybersecurity for smart cities compared to previous methods. The research then evaluates the effectiveness of the CRNN approach using a recent attack dataset. The results are expected to show that the CRNN method can successfully detect cyberattacks and outperform existing methods.

d. Scope: This research tackles improving cybersecurity in smart cities overflowing with internet-connected devices (IoT). The focus is developing a new method to detect cyberattacks using machine learning. Here, Convolutional Recurrent Neural Networks (CRNNs) are chosen for their ability to analyze both the sequence and patterns within data streams collected from IoT devices. By combining these strengths, the research aims to create a more comprehensive defense system against cyberattacks in smart cities. The effectiveness of this CRNN method will be tested using a recent dataset of cyberattacks, with the goal of surpassing previous detection methods.

2) RELATED WORK

Recognizing the growing dangers of cyberattacks in smart cities filled with interconnected devices, researchers are actively developing new methods for defense. One approach utilizes machine learning, particularly deep learning algorithms, to analyze the data flowing through these networks. By identifying unusual patterns, these algorithms can potentially detect cyberattacks before they cause disruption. Additionally, some studies focus on balancing security with privacy by employing techniques like federated learning. This allows anomaly detection without compromising sensitive data stored on individual devices. Furthermore, researchers acknowledge the limitations of traditional security methods and are exploring novel protocols specifically designed to safeguard the complex infrastructure of smart cities.

3) CYBER THREAT DETECTION IN IOT:

IoT devices, while bringing convenience to smart cities, introduce new cybersecurity vulnerabilities. These internet-connected devices can be attractive targets for hackers due to several reasons:

- **Weak Security:** Many IoT devices have weak security features built-in. They might lack complex password requirements, have outdated software, or be difficult to patch due to limitations on processing power.

- **Vast Attack Surface:** The sheer number and variety of IoT devices in a smart city create a vast attack surface. Hackers only need to find a single vulnerability to gain access to a network.
- **Data Collection:** Many IoT devices collect and transmit data, which can be sensitive. This data could include personal information, information about critical infrastructure, or even be used to control physical systems in the city.
- **Botnets:** Hackers can exploit compromised IoT devices to create botnets, large networks of devices used for launching attacks like Denial-of-Service (DoS) that can cripple online services.

These cyber threats can have serious consequences for smart cities. A successful attack could disrupt essential services, damage infrastructure, or even endanger public safety.

4) LIMITATIONS OF EXISTING APPROACHES:

While Artificial Neural Networks (ANNs) offer promise for cyberattack detection in smart cities, they face limitations that hinder their real-world implementation. Large volumes of data from complex IoT networks can overwhelm ANNs, impacting their scalability. Training them can be computationally expensive and slow, hindering real-time response. Additionally, their "black-box" nature makes it difficult to understand how they identify attacks, limiting our ability to verify their accuracy. Overfitting is another concern, where ANNs perform well on training data but struggle with unseen threats, reducing their effectiveness against evolving attacks. The quality of training data is paramount, as biased or incomplete data can lead to poor performance. Finally, ANNs might not adapt well to constantly changing cyber threats, requiring frequent updates to maintain effectiveness. By acknowledging these limitations, researchers can work towards more robust and efficient cyberattack detection methods for smart city applications.

5) CNN AND LSTM FOR CYBER THREAT DETECTION IN IOT SMRT CITIES

The proposed model " CRNNs FOR AN EFFECTIVE CYBERATTACK DETECTION IN SMART CITIES" addresses the growing cybersecurity threat in smart cities, fueled by the vast network of Internet of Things (IoT) devices. To combat these threats, I propose a novel attack and anomaly detection method utilizing Convolutional Recurrent Neural Networks (CRNNs). CRNNs offer a unique advantage by combining the strengths of both Convolutional Neural Networks (CNNs)[5] and Recurrent Neural Networks (RNNs). CNNs excel at extracting spatial features from data, making them ideal for analyzing the patterns inherent in sensor data. RNNs, on the other hand, excel at capturing temporal dependencies within sequential data. By combining these capabilities, CRNNs offer a comprehensive approach to identifying anomalies and cyberattacks within the IoT network. Experimental results using a recent attack dataset demonstrate the effectiveness of the proposed CRNN model, achieving superior performance in threat detection compared to existing methods. CNN-LSTM (Convolutional Neural Network - Long Short-Term Memory) is a powerful combination technique gaining traction in cyber threat detection for IoT devices in smart cities. Here's how each component contributes:

Convolutional Neural Network (CNN):

- Analyses data streams for spatial patterns.
- Ideal for identifying specific features within the data that might indicate malicious activity.
- In IoT security, CNNs can effectively detect anomalies in sensor data, network traffic patterns, or even image/video feeds from security cameras.

Long Short-Term Memory (LSTM):

- Focuses on temporal dependencies within data sequences.
- Captures how data points change over time, crucial for analysing sequential data like sensor readings or network traffic logs.
- In IoT threat detection, LSTMs can identify sudden spikes in energy consumption, unusual data transmission patterns, or deviations from established baselines, potentially indicating a cyberattack.

Synergy of CNN and LSTM (CNN-LSTM):

- By combining these strengths, CNN-LSTM provides a comprehensive approach to cyber threat detection:
  - CNNs identify suspicious patterns within individual data points.
  - LSTMs analyse the sequence of these data points to understand if they represent a coordinated attack.
- This combined approach offers better accuracy and adaptability in detecting evolving cyber threats compared to using either CNN or LSTM alone.

Here are some benefits of using CNN-LSTM for cyber threat detection in IoT smart cities:

- **Improved Accuracy:** By leveraging both spatial and temporal information, CNN-LSTMs can achieve higher accuracy in identifying malicious activity compared to individual techniques.
- **Real-Time Analysis:** CNN-LSTMs can be trained to analyze data streams in real-time, enabling faster detection and response to cyber threats.
- **Adaptability:** The ability to learn from new data patterns allows CNN-LSTMs to adapt to evolving cyber threats and maintain effectiveness over time.

Overall, CNN-LSTM offers a promising approach for robust cyber threat detection in the complex and ever-growing world of IoT-powered smart cities.

6) PROPOSED MODEL:

In the proposed model Every fog node's network traffic is tracked by the model. It will be more successful to detect cyberattacks at fog nodes rather than cloud centres because fog nodes are nearest to IoT sensors. The fog nodes plays a critical role in mitigating cyber threats within an IoT smart city by acting as a robust defence line between resource-constrained devices and the cloud. Fog nodes have more processing power than individual devices. They can aggregate data from multiple devices and run more sophisticated intrusion detection systems (IDS)[7] with CRNNs or other machine learning techniques and it also have a broader view of the network activity compared to individual devices. This allows them to identify suspicious communication patterns across multiple devices, potentially indicating a coordinated attack.

Fog Nodes:

Processing power: Fog nodes are closer to IoT devices and have more processing power than individual devices.

- Broader view: They can analyse data from multiple devices, providing a wider perspective of network activity.
- Faster response: Early attack detection at fog nodes allows for quicker response compared to cloud-based systems.

The Model's Approach:

1. **Data Collection:** Traffic data is collected from various IoT devices in the network.
2. **Preprocessing:** The collected data undergoes cleaning, visualization, feature engineering, and conversion into a format suitable for the model (feature vectors).
3. **Machine Learning Algorithm:**
   - **1D CNNs:** These are used to identify patterns within the data that might indicate an attack. They excel at analysing sequential data like network traffic.
   - **LSTMs:** These capture long-term dependencies in the data. They can remember past data points and analyse how they relate to current ones, helping identify gradual changes or unusual sequences potentially linked to attacks.

4. **Training and Testing:** The model is trained using a portion of the data (training set) and then tested on another portion (testing set) to evaluate its effectiveness.

Benefits of the Proposed Model:

- **Improved Accuracy:** Combining CNNs and LSTMs allows the model to identify both spatial patterns and temporal relationships in the data, potentially leading to more accurate attack detection.
- **Real-Time Analysis:** The model can be used for real-time analysis of network traffic, enabling faster response to threats.
- **Scalability:** The chosen algorithms (1D CNNs and LSTMs) are well-suited for handling large amounts of data generated by numerous IoT devices in a smart city.

The Dataset:

The research uses the UNSW-NB15 dataset, which is a valuable resource for intrusion detection system development. It includes:

- A mix of real network traffic and simulated attacks, providing a realistic training environment.
- 49 specific features extracted from the data, offering a detailed picture of each network event.
- Pre-configured training and testing sets for model evaluation.
- Over 2.5 million records covering various attack categories.

This comprehensive dataset allows to train and test their model effectively for real-world scenarios.

Data Cleansing:

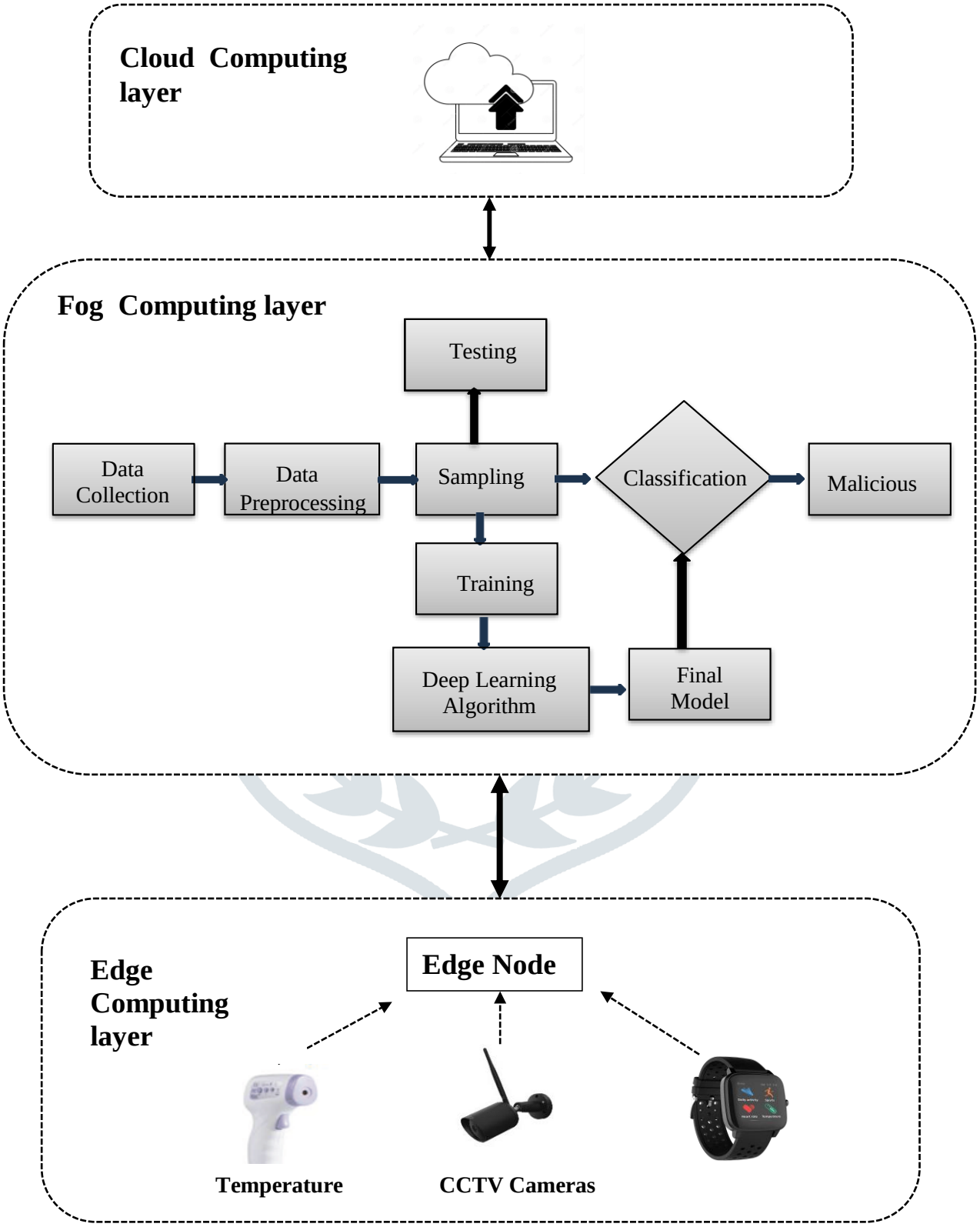
The explanation mentions that the UNSW-NB15 dataset used doesn't have missing values, so no specific techniques for handling missing data were required. This is a fortunate situation, as missing data can be challenging to address effectively.

Data Processing:

Here's what the research covers regarding data processing:

- **Categorical Feature Conversion:** The dataset contains features like "port," "service," and "state" which aren't numerical. Machine learning algorithms typically work best with numbers. Therefore, these categorical features need conversion.

- **Label encoding:** This is the chosen technique for converting categorical features. It assigns a unique numerical value to each category within the feature. For example, "port 80" might be converted to "3" if it's the third unique port value encountered in the data. This allows the machine learning algorithms to understand the relationships between these features and others in the dataset.


Cloud Computing layer
Fog Computing layer
Testing
Data Collection
Data Preprocessing
Sampling
Classification
Malicious
Training
Deep Learning Algorithm
Final Model
Edge Computing layer
Edge Node
Temperature
CCTV Cameras

7) PERFORMANCE EVALUATION METRICS

a. Accuracy, Precision, Recall, F1-Score

Accuracy: Accuracy serves as a measure of the overall correctness of the model's predictions, representing the ratio of correctly identified instances to the total instances. However, accuracy might be deceptive when handling imbalanced datasets where one class dominates. Therefore, additional metrics are employed:

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

Precision: Precision denotes the proportion of true positive predictions out of all positive predictions made by the model. A higher precision indicates fewer false positives, which are instances incorrectly identified as positive.

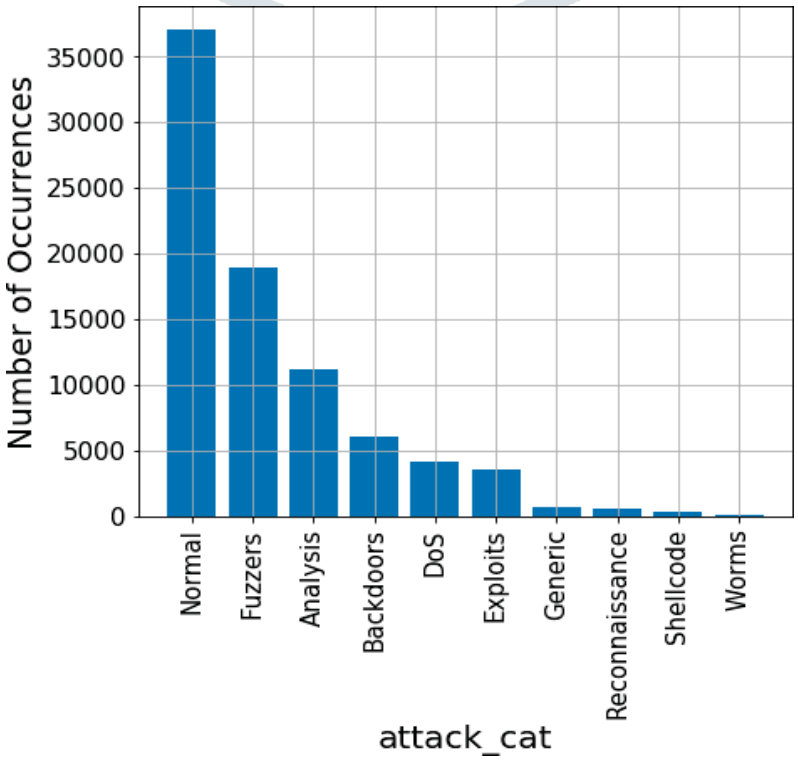
$$\text{Precision} = \frac{TP}{TP + FP}$$

Recall (Sensitivity or True Positive Rate): Recall measures the proportion of true positive predictions out of all actual positive instances. It showcases the model's capability to accurately identify positive instances. A higher recall implies fewer false negatives, which are positive instances incorrectly identified as negative.

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

F1-score: The F1-score strikes a balance between precision and recall by computing their harmonic mean. It proves particularly useful when minimizing both false positives and false negatives is imperative.

$$F1score = \frac{2 * TP}{2 * TP + FP + FN}$$



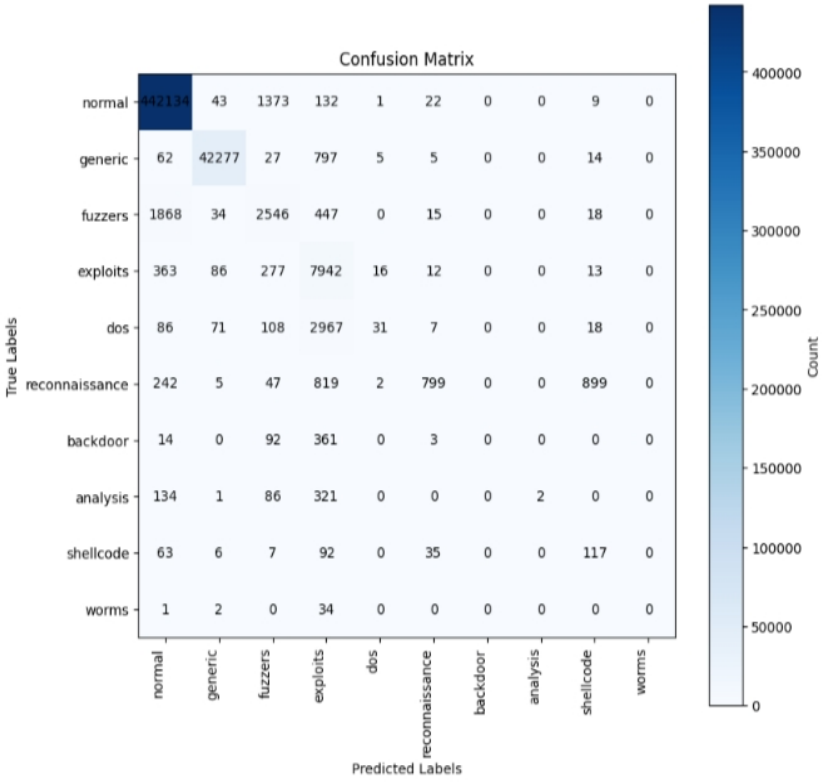
8) RESULTS & DISCUSSION

The table below shows promising results for the CNN-LSTM model in detecting cyberattacks within the smart city's fog nodes. The model achieves high accuracy, precision, and recall while maintaining a relatively low loss during training. These metrics suggest the model can effectively identify attacks with a low rate of false positives and false negatives.

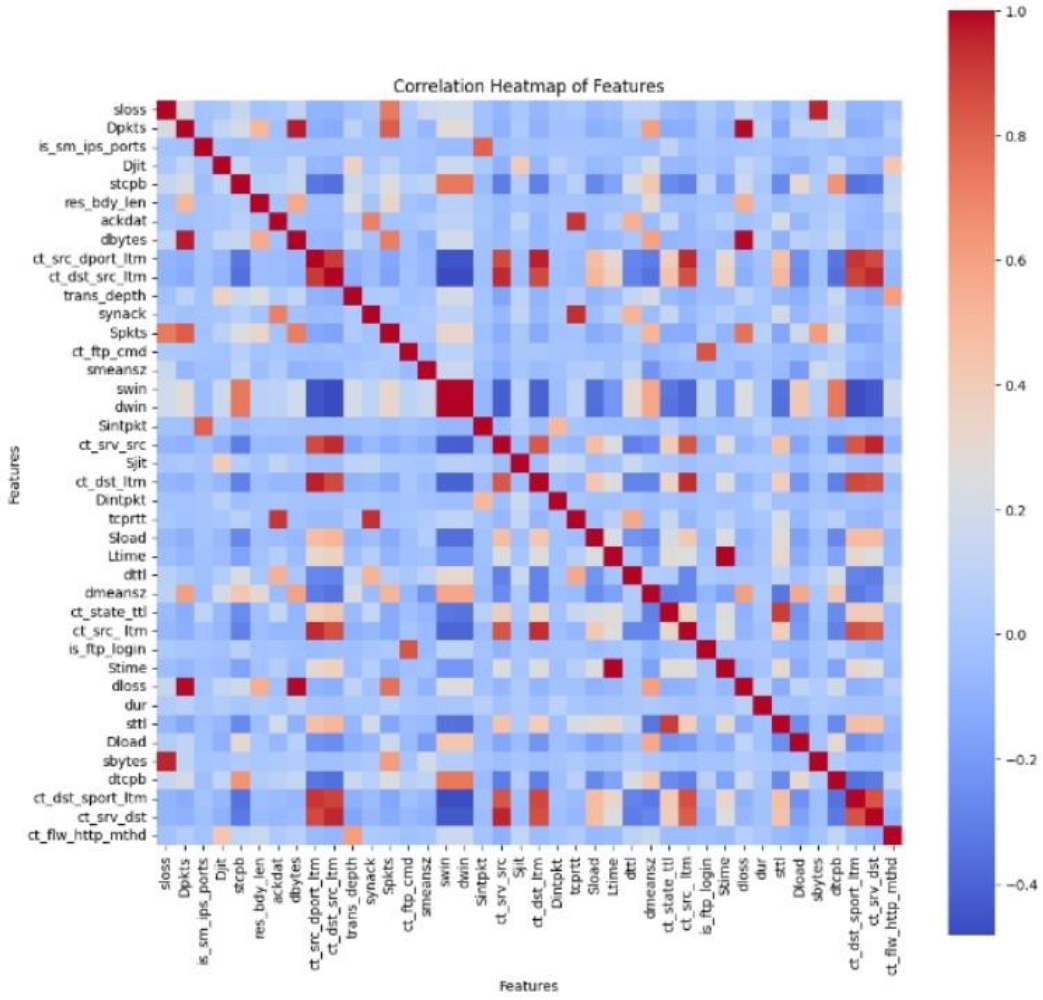
CNN-LSTM model's performance on intrusion detection using a dataset with 45 features. The model achieved an impressive 97.69% accuracy, meaning it correctly classified most network traffic as normal or malicious. It also showed a good balance between precision (98%) and recall (96%). Precision indicates the model rarely flagged normal traffic as attacks, while recall reflects how well it identified actual attacks. Finally, a loss of 58% during training suggests the model learned effectively. Overall, these results demonstrate the CNN-LSTM model's potential for accurate and reliable cyberattack detection in smart city fog nodes.

Method	No. of Features	Accuracy (%)	Precision (%)	Recall (%)	Loss (%)
CNN-LSTM	45	97.69	98	96	58

The result can also be visualized using the confusion matrix and K-Fold Cross validation evaluation metrics.



We have used two approaches to evaluate our proposed model, Stratified K-Fold cross validation metrics and confusion matrix. K-Fold CV provides a more statistically sound evaluation compared to a single train-test split while the confusion matrix offers valuable insights into how the model performs for each class, helping identify potential issues like class imbalance. As we can see in the figure 4 the Confusion Matrix for the proposed Model where the diagonal represent the where we can see that for each class the entire region under the curves is almost equal to the value of one.



9) CONCLUSION

We explore the different architecture of CNN and RNN to find its effectiveness in detecting intrusion for the smart city IoT con- text. This research builds upon existing work in the field. While a previous study [15] employed

TABLE IV: Performance comparison with existing work

	Method	Accuracy
Existing Model	ANN	85.10 %
Proposed Model	CNN-LSTM	97.69 %

Artificial Neural Networks (ANNs) for a similar data set, it focused on comparing different machine learning algorithms rather than delving into the specifics of the ANN parameters used. In contrast, our work offers a more detailed exploration of a specific model architecture, including the chosen parameters. We, by contrast, focus combining CNNs and LSTMs, the model can learn both spatial and temporal patterns, potentially leading to more accurate threat detection. CNN-LSTMs can be adapted to handle different types of IoT data and cyber threats by adjusting the network architecture and training data. Overall, CNN-LSTMs represent a promising approach for cyber threat detection in IoT smart cities. By leveraging their ability to learn from both spatial and temporal features in data, these models can contribute to a more secure and resilient smart city environment.

This paper presents a novel machine learning approach using a Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) network (CNN-LSTM) to identify cyberattacks within an IoT-based smart city. This method leverages distributed fog layers for attack detection, bypassing the cloud layer. Our performance analysis demonstrates that the CNN-LSTM model significantly outperforms existing methods in terms of accuracy. We plan to further investigate ensemble learning and explore advanced deep

learning techniques to potentially improve the model's performance even further.

REFERENCES:

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, K. Han,"Enhanced Network Anomaly Detection Based on Deep Neural Networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018.

[2] W. Wang, Y. Sheng and J. Wang, "HAST-IDS: Learning hierarchical spatial- temporal features using deep neural networks to improve intrusion detection," *IEEEAccess*, vol. 6, no. 99, pp. 1792-1806, 2018.

[3] M. K. Hussein, N. Bin Zainal and A. N. Jaber, "Data security analysis for DDoS defense of cloud-based networks," *2015* IEEE Student Conference on Research and Development (Scored), Kuala Lumpur, 2015, pp. 305-310.

[4] C. Dong, C. C. Loy, K. He and X. Tang, "Image Super-Resolution UsingDeep Convolutional Networks," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 38, no. 2, pp. 295- 307, 1 Feb. 2016.

[5] Hubbell and V.Surya narayana False alarm minimization techniques in signature-based intrusion detection systems: A survey,'' Compute. Common., vol. 49, pp. 1- 17, Aug. 2014.

[6] A. Naser, M. A. Majid, M. F. Zolile and S. Anwar, "Trusting cloud computing for personal files," 2014 International Conference on Information andCommunication Technology Convergence (ICTC), Busan, 2014, pp. 488- 489.

[7] Y. Shen, E. Marconi, P. Verviers, and Gianluca Stringham, "Tiresias: PredictingSecurity Events Through Deep Learning," *In Proc. ACM CCS 18*,

Toronto, Canada,2018, pp. 592-605.

[8] Kyle Soaks and Nicolas Christin, "Automatically detecting vulnerable websites before they turn malicious,", *In Proc. USENIX Security Symposium.*, San Diego, CA,USA, 2014, pp.625-640.

[9] K. Veerama channid, I. Arnaldo, V. Koraput, C. Basis, K. Li, "AI2: training a bigdata machine to defend," In Proc. IEEE Bigdata Security HPSC IDS, New York, NY,

USA, 2016, pp. 49-54

[10] Mahmood Lavallee, Ebrahim Bagheri, Wei Lu and Ali A. Ghobadi, "A detailed analysis of the kid cup 99 data set," In Proc. of the Second IEEE Int. Conf. Comp. Int. for Sec. and Def. App., pp. 53-58,

2009.

[11] I. Sharfuddin, A. H. Lashari, A. A. Ghobadi, "Toward generating a new intrusion detection dataset and intrusion traffic characterization", Proc. Int. Conf.Inf. Syst. Scur. Privacy, pp. 108- 116, 2018.

[12] [online] Available: http://www.takakura.com/Kyoto_data/

[13] N. Shone, T. N. Ngoc, V. D. Phail and Q. Shi, "A deep learning approachto network intrusion detection," IEEE Trans. Emerge. Topics Compute. Intel., vol. 2, pp. 41-50, Feb. 2018

[14] R. Vijayakumar, Mamoon Alazar, K. P. Soman, P. Poorna Chandran, AmeerAl- Namrata and Sit Lakshmi Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525- 41550,Apr. 2019.

[15] W. Hu, W. Hu, S. Maybank, "Ad boost-based algorithm for network intrusiondetection," IEEE Trans. Syst. Man B Cybernet., vol. 38, no. 2, pp.

577-583, Feb.2008.

[16] T.-F. Yen et al., "Beehive: Large-scale log analysis for detecting suspiciousactivity in enterprise networks", Proc. 29th Annul. Compute. SecurityAppl. Conf., New York, NY, USA, 2013, pp. 199- 208.

[17] M. Alazar, S. Venkatraman, P. Watters, and M. Alazar, “Zero-day malware detection based on supervised learning algorithms of API call signatures,” In Proc. 9th Australis. Data Mining Conf., vol. 121. Ballarat, Australia, Dec. 2011, pp. 171- 182.