International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7968
***Article Received**: 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

Cloud Computing for Effective Cyber Security Attack Detection in Smart Cities

[1]Namita R. Kale, [2]Kalpana V. Metre, [3]Dr. Pankaj Pramod Chitte, [4]Nitin Mahankale, [5]Santosh Gore, [6]Sujata Gore

[1]MET's Institute of Engineering, Nashik.
mrsnrkale@gmail.com
[2]MET's Institute of Engineering, Nashik.
kvmetre@gmail.com
[3]Assistant Professor
Department of Electronics and Computer Engineering,
Pravara Rural Engineering College, Loni.
chittepp@pravaraengg.org.in
[4]Associate Professor Symbiosis Centre for Management Studies,
Symbiosis International (Deemed University),
Pune, India
Nitin.mahankale@scmspune.ac.in
[5]Director, Sai Info Solution, Nashik,
Maharashtra, India
https://orcid.org/0000-0003-1814-59131
sai.info2009@gmail.com
[6]Director, Sai Info Solution, Nashik,
Maharashtra, India
sujatarpatil21@gmail.com

Abstract: An astute metropolis is an urbanized region that accumulates data through diverse numerical and experiential understanding. Cloud-connected Internet of Things (IoT) solutions have the potential to aid intelligent cities in collecting data from inhabitants, devices, residences, and alternative origins. The monitoring and administration of carrying systems, plug-in services, reserve managing, H2O resource schemes, excess managing, illegal finding, safety actions, ability, numeral collection, healthcare abilities, and extra openings all make use of the processing and analysis of this data. This study aims to improve the security of smart cities by detecting attacks using algorithms drawn from the UNSW-NB15 and CICIDS2017 datasets and to create advanced strategies for identifying and justifying cyber threats in the context of smart cities by leveraging real-world network traffic data from UNSW-NB15 and labelled attack actions from CICIDS2017. The research aims to underwrite the development of more effective intrusion detection systems tailored to the unique problems of safeguarding networked urban environments, hence improving the flexibility and safety of smart cities by estimating these datasets.

Keywords: Smart city, Cloud computing, Cloud security, IoT.

I. INTRODUCTION

Cloud computing represents the advancement of internet-based calculating, offering the provision of IT resources as services. This paradigm shift enables the utilization of technology skills on demand. As smart devices extend beyond the confines of cloud infrastructure, the Internet of Things (IoT) [1] gains traction, enhancing productivity, concert, and data material. Clever cities [2] embody domestic areas actively embracing new information and announcement knowledge to realize goals like eco-friendly sustainability, town management efficiency, enhanced health services, educational growth, and network-driven progress.

The challenges that emerge within a fluid, communal setting are the main focal point of the IoT. The Internet of Things (IoT) constitutes a vast classification encompassing a diverse array of flexible and unconventional devices with restricted storage, power availability, and operational capabilities. These limitations [3], which include complicated concerns like compatibility, efficiency, complete functionality, and availability, serve as a wall beside impediment to the advance of IoT organizations [1]. Cloud computing is one of the most promising strategies that might be used in conjunction with IoT to get over these constraints. The cloud offers communal assets [3] (network, storage, computers, and software) recognized for their user-friendliness, affordability, and visual attractiveness. This article outlines the applications of a cloud-based IoT platform designed for intelligent urban areas. These applications encompass communication, computation, and data retention. This framework could utilize cloud-oriented assets and offerings to amass, transmit, handle, assess, and retain data. Moreover, it might employ cloud resources and services to compile, transmit, search, scrutinize, and preserve data produced by intricate scenarios [4].

The primary focus of IoT is addressing challenges within dynamic shared environments. IoT encompasses diverse adaptive policies with constrained storage, power, and presentation. These limitations, including compatibility, efficiency, functionality, and availability, hinder IoT system development. This study delves into an IoT platform for smart cities that is cloud-based, utilizing most resources to collect, process, examine, and collection files. The platform tackles composite data circumstances, utilizing cloud services for data gathering, transmission, search, and analysis [5]. See Figure 1 for the cloud-based IoT app creation boards.

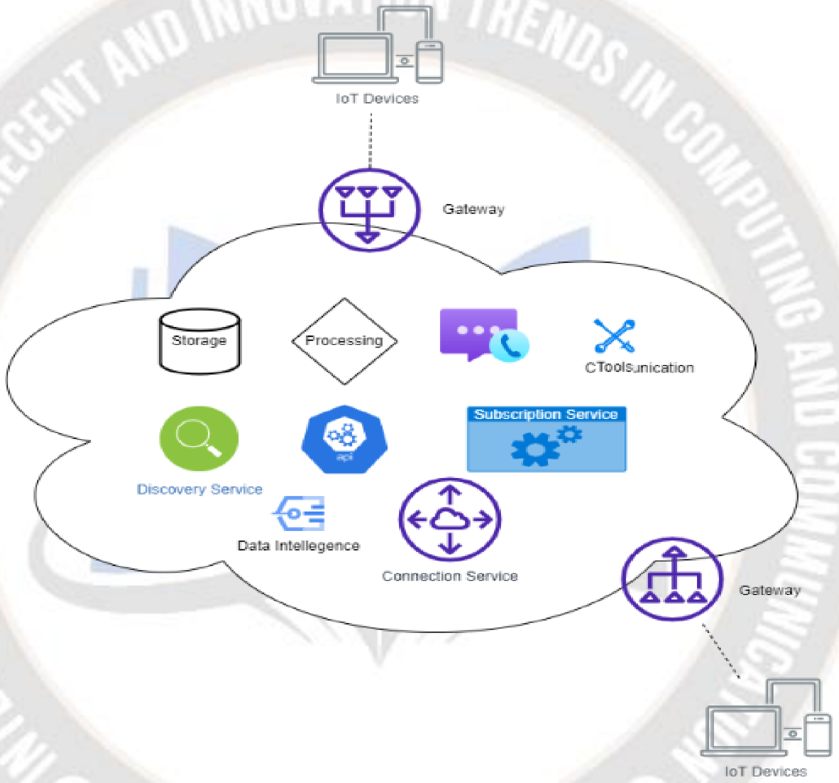

Fig. 1. Example IoT system using the cloud [2].

This paper introduces a novel attack detection model using a four-layer deep convolutional neural network. The model focuses on identifying replay attacks in smart cities by incorporating time-domain analysis. The innovation lies in applying deep learning to enhance detection accuracy. The evaluation measures accuracy in classifying normal and attacked behaviours. Furthermore, the paper compares the model's performance with traditional machine learning and deep learning approaches from existing literature.

II. LITERATURE SURVEY

In the research, the aim is to invest possibilities of integrating cloud computing using IoT into smart cities. The study starts by examining the existing trends and challenges in this market to establish a full overview. In smart cities learning approaches with cloud computing have received a lot of interest in current years. The literature review examines existing research that has studied the applications of smart cities to optimize cloud computing in smart cities.

In [3], A novel defence approach was introduced, featuring trust-based light probes. This innovative method aimed to identify On and Off attacks originating from unauthorized network nodes within an industrial IoT setting. In this context, an "On and Off attack" meant taking advantage of the IoT network when it was active or inactive. The system used a light probe routing approach to detect anomalies, which was followed with assurance assessment measures for each surrounding node. Diro and Chilamkurti [4] suggested a deep-learning approach for detecting widespread threats in an IoT network. Using the NSL-KDD [5] open-source dataset, which contains attack information in equally spread and regional organizations, they connected the presentation of this deep model to that of a trivial neural net. Their assessment includes two-class (normal and attack) and four-class categorizations (normal, DoS, Probe, R2L, and U2R). Their model achieved 99.2% and 98.27% accuracy for binary-class identification, and 95.22% and 96.75% accuracy for multi-class identification, one-to-one.

In their work [6], Pajouh et al. developed a two-stage dimension reduction and classification method for detecting anomalies in IoT backbone networks. They concentrated on identifying low-frequency assaults from the NSL-KDD dataset, such as user-to-root (U2R) and remote-to-local (R2L) attacks, due to their serious consequences. The authors used principle component analysis (PCA) and linear discriminant analysis (LDA) feature extraction methods to decrease dataset characteristics. The author used naive Bayes and K-nearest Neighbors (KNN) to identify anomalies, getting a recognition rate of 84.82%.

In their work [7], Kozik and colleagues presented a novel attack detection mechanism utilizing the extreme learning machine technology integrated into the Apache Spark cloud framework. The ELM's design facilitated efficient processing and analysis of organized Netflow data collected from the fog computing environment. The study focused on addressing three significant scenarios prevalent in IoT systems: scanning, command and control, and infected host. The achieved accuracy rates for these specific scenarios were 99%, 76%, and 95% correspondingly.

Hasan et al. presented a data analysis-based approach for identifying assaults on IoT infrastructure in their study. The data processing overhead associated with signature-based approaches was overcome by this method. Their approach detects and prevents system threats by recognizing abnormal activities. The project made use of a freely available IoT dataset [18]. DT, RF, LR, SVM, and ANN were among the machine learning algorithms investigated. Among these, the RF classifier produced the most favourable results.

In their work [26], An anomaly detection system based on the random forest algorithm was introduced for identifying compromised IoT devices across distributed fog nodes. The binary RF classifier, trained on the UNSW-NB15 dataset, demonstrated effective results with the utilization of only 12 out of the dataset's total 49 features. These 12 features were extracted using the ExtraTreeClassifier. The evaluation of system performance showcased an impressive accuracy of 99.34% alongside a false positive rate of 0.02%. Table 1 shows a list of noteworthy publications that use machine learning and collective methods to detect intrusion in addition to anomalies.

TABLE I. machine learning and collective methods to detect intrusions

Author Name	Year	Methodology	Dataset	Metric of Evaluation
Pahl et al[6].	2018	K- means	Own	Accuracy is 96.3%
Pajouh et al. [7]	2018	Naive Bayes, K-Nearest Neighbour	NSL-KDD	Accuracy is 84.82%
Diro et al. [8]	2018	Neural network	NSL-KDD [9]	Accuracy is 98.27%
Alrashdi et al[10].	2019	RF	UNSW-NB15	Accuracy is 99.34%
Kozik et al. [11]	2018	Extreme learning machine	Netflow formatted data	Accuracy is 99%

Many studies have used different datasets and achieved varied outcomes due to machine learning's data dependency and contextual variations. This research focuses on the UNSW-NB15 dataset for IoT attack detection, emphasizing its concurrency. This aims to identify specific attacks in smart city fog nodes.

III. PROPOSED MODEL

Figure 2 depicts the proposed network traffic tracking model. from side-to-side smog nodes, which are closer to IoT sensors, enhancing cyber-attack detection compared to central clouds. Swift alerts enable prompt action by administrators to evaluate and upgrade systems. In this study, They opt for anomaly-based network-based IDS (NIDS) due to its suitability for IoT devices, unlike host-based IDS (HIDS). HIDS is resource-intensive and not ideal for IoT's limited-function devices. Signature-based NIDS is costly and less effective for new attacks. This approach employs anomaly-based NIDS, gathering data to construct an ensemble of ML models for IoT fog network anomaly detection.

***Article Received**: 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

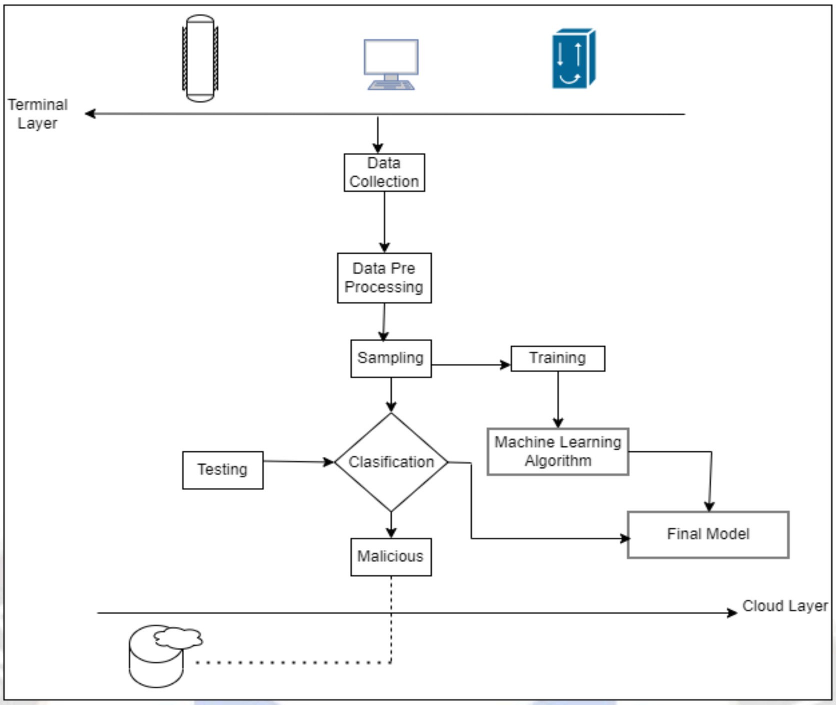

Fig. 2. Application model used for IoT MI based.

Data collection is the process of acquiring information from different sources of a terminal layer. The process of data collection contains three steps of the process is as follows:

Step 1: Data Acquisition:

In smart cities, guaranteeing the security of data collecting requires a methodical strategy. The acquired data is first standardized into a consistent format. Then, anomaly detection techniques are used to discover deviations from expected behaviour, and signature-based methods are used to recognize known attack patterns. Continuous behavioural analysis monitors system activity, whereas network traffic monitoring examines packets for potential hazards. Regular vulnerability evaluations reduce vulnerabilities, and data encryption ensures confidentiality and integrity. Real-time alerts prompt fast action, while collaborative threat sharing strengthens collective protection. Adaptive techniques evolve defences, and an incident response plan guides actions in the event of an attack. This comprehensive method ensures that data acquisition systems in smart cities are adequately protected.

Step 2: Data Augmentation:

Detecting data augmentation assaults in smart cities entails gathering and improving data, followed by anomaly detection and machine learning-based analysis to identify anomalies. Signature-based detection and ongoing behaviour analysis improve threat detection. Regular security audits and coordinated threat sharing improve protection, while a well-defined incident response plan ensures rapid remediation and the integrity of augmented data.

TABLE II. data proportion of various geographies in the UNSW-NB15 dataset [10]

Article Number	Article Name	Ratio
7	Sbytes	1.64
12	Sload	1.268
28	Dmean	0.789
35	Ct_dst_sport_ltm	0.750
1	Dur	0.726
11	Dttl	0.705

TABLE III. Material improvement proportion on the CICIDS2017 dataset [12]

Article Number	Article Name	Quotient
53	Normal Package Size	1.1761
42	Package Size Standard	1.13817
19	Flow, IAT Max,	1.1175
37	Forward Packages	1.06422
16	Flow Packages	1.04504
5	Overall Size of Forward Packets	1.01074

Data Pre-processing is selecting relevant structures, lowering ended correct, increasing correctness, and then trimming exercise intervals to improve model efficacy. The application selects the best 25 relevant structures from both datasets using the data advance quotient method. These features were identified based on their contribution to distinguishing benign and malware applications. For UNSW-NB15, the application transformed categorical features like 'proto' and 'service' into vectors using 'Label Encoding'. Thresholds of 0.5 and 0.85 determined feature inclusion for UNSW-NB15 [10] (University of New South Wales - Network-Based 15) and CICIDS2017 (Canadian Institute for Cyber Security Intrusion Detection Evaluation Dataset 2017) [10] datasets respectively.

Theoretical Consideration

This proposed system employed various machine learning methods, including Logistic regression, Support vector machine, Decision tree, Random forests, and K-nearest neighbours, Artificial neural network, commonly utilized in IDS to construct and evaluate this model. Ensemble methods are prevalent in machine learning, merging multiple base models into an optimal predictive model. By uniting diverse models, an ensemble method produces a final model. This approach harnesses the strength of weak learners, creating a robust learner and enhancing accuracy. In the literature, three ensemble techniques stand out. Bagging, a parallel technique, concurrently generates base learners to bolster the accuracy and potency of ML algorithms. Increasingly, a consecutive joint method creates base beginners to mitigate preference and inconsistency in managed machine learning (ML). Stacking a cooperative approach, amalgamates guesses from multiple base ordering copies interested in a fresh dataset, serving as a contribution for the extra classifier to address the problem. Data collected from sampling will be classified if data is malicious after testing then it will be passed to the cloud. If the data is not malicious then it will process by a machine learning algorithm then the final data model will get ready.

As above, the outline key performance metrics – correctness, exactness, evoke, F1-Score, and ROC curves – are commonly employed to assess model presentation in irregularity discovery applications. These metrics are formulated through the resulting factors:

$$\mathrm{f_p} = \text{true positive}$$
$$\mathrm{f_n} = \text{true negative}$$
$$\mathrm{t_p} = \text{false positive}$$
$$\mathrm{t_n} = \text{false negative}$$
$$\mathrm{f_p} + \mathrm{t_n} = \mathrm{p}(\text{total positive})$$
$$\mathrm{f_n} + \mathrm{t_p} = \mathrm{n}(\text{total negative})$$

Accuracy measures the model's overall performance in terms of It belongs to both the benign and the assault classes and is defined as follows:

$$Accuracy = \frac{f_p+f_n}{p} + n$$

□□□□□□□□□□□□□□□□□□□□□□

Precision indicates how many of the selected things are relevant among the retrieved objects and are defined as follows:

$$Precision = \frac{f_p}{f_P+t_p}$$ □□□□□□□

Recall describes how many relevant items are chosen from a total number of relevant objects and is defined as follows:

$$Precision = \frac{f_p}{f_P+t_n} \qquad (3)$$

The F1-score can be calculated using both precision and recall as follows:

$$F1 - Score = 2 \times Precision \times \frac{Recall}{Precision} + Recall \qquad (4)$$

The Receiver Operating Characteristic curve serves to describe the performance of a classifier across various decision thresholds. It accomplishes this by plotting the true positive rate (t_{pr}) against the false positive rate (f_{pr}). The calculations for the true positive rate and false positive rate are represented by Equations (5) and (6) correspondingly.

$$f_{pr} = \frac{f_p}{f_P+t_n} \qquad (5)$$

$$t_{pr} = \frac{t_p}{f_P+t_n} \qquad (6)$$

***Article Received**: 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

IV. RESULTS

This proposed model used 10-fold cross-validation (CV) to evaluate both the basic and ensemble classifiers. This procedure partitioned the dataset into ten equal subgroups, nine for model construction and one for testing. This procedure was repeated ten times to ensure that each subset was used as the test set. The average accuracy across folds was computed. Multiple evaluation metrics for various classifiers on training and test datasets are shown in Figure 3.

TABLE IV. Discovery of distinct modules using the UNSW-NB15 dataset

Algorithm	TPR	FPR	F1-Score	Accuracy
LR	0.81	0.052	0.85	72%
SVM	0.81	0.037	0.84	71%
DT	0.92	0.027	0.92	81%
RF	0.91	0.055	0.93	82%
ANN	0.91	0.029	0.90	78%
KNN	0.92	0.027	0.91	75%
Bagging	0.93	0.035	0.93	83%
Stacking	0.993	0.029	0.93	84%

TABLE V. discovery of several programs using the CICIDS2017 dataset

Algorithm	TPR	FPR	F1-Score	Accuracy
LR	0.99	0.17	0.97	95%
SVM	0.980	0.171	0.970	92%
DT	0.995	0.003	0.995	99%
RF	0.995	0.006	0.95	99%
ANN	0.993	0.175	0.940	96%
KNN	0.994	0.006	0.994	98%
Bagging	0.999	0.006	0.999	99%
Stacking	0.999	0.003	1.0	99%
Boosting	0.999	0.003	1.0	98%

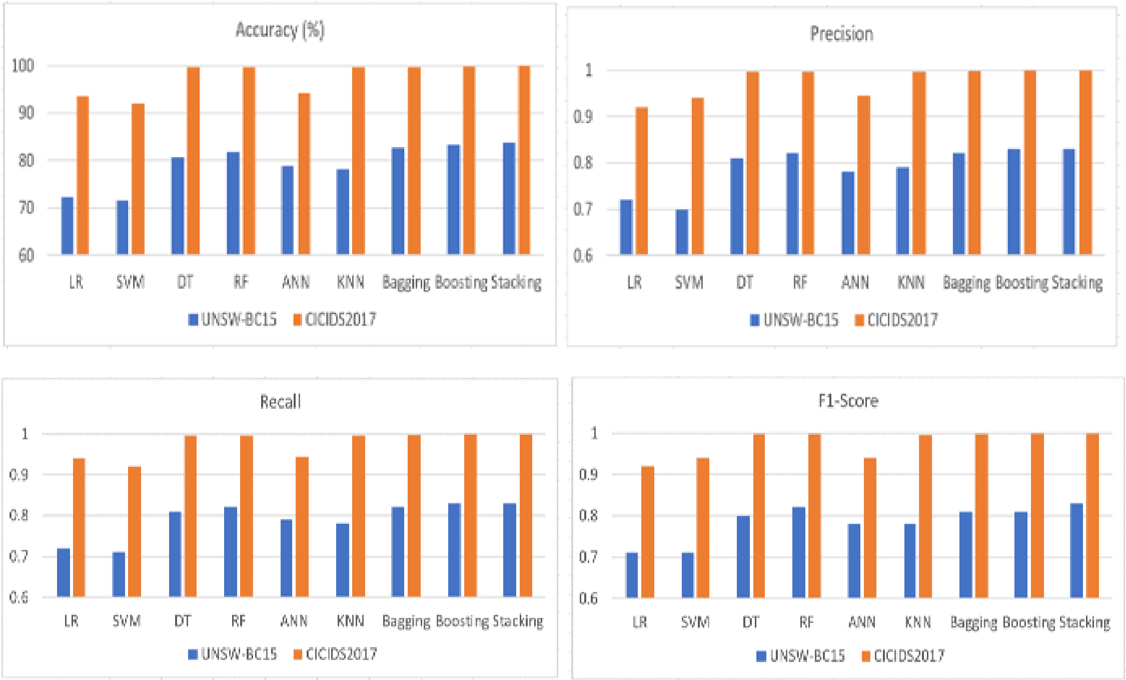

Fig 3. Proposed method performance in terms of accuracy, precision, recall and F1 score.

Figure 3 depicts the accuracy performance of many classifiers. The goal was to assign an unknown sample to one of ten classes for the UNSW-NB15 dataset and eight classes for the CICIDS2017 dataset. The accuracy of LR, SVM, DT, RF, ANN, and KNN on the test dataset in the UNSW-BC15 and CICIDS2017 datasets is as follows: 72.32% and 93.60%, 71.49% and 92%, 80.69% and 99.7%, 81.77% and 99.7%, 78.89% and 94.2%, and 78.23% and 99.7%.

The outcomes reveal that ensemble learning models outperform individual ideal classifiers on both check datasets. This suggests that, despite the prevailing focus on single-learning models in previous research, ensemble classifiers like stacking present a promising avenue for applications in this domain. The findings demonstrate that, across various attack types, DT and RF outperform other algorithms. Notably, the stacking communal system exhibits substantial improvements compared to trapping and enhancing in certain scenarios. For instance, on the UNSW-NB15 dataset, in DoS attacks, assembling achieves an F1-score of 0.45, surpassing bagging and boosting with scores of 0.24 and 0.33, respectively. Similarly, in Worm attacks, assembling earnings F1-score of 0.57, outperforming bagging (0.37) and enhancing (0.33). Stacking consistently achieves F1 scores above 0.75 for most other attack types. On the CICIDS2017 dataset, the stacking ensemble achieves an F1-score of 0.950 for the Bot attack, surpassing bagging (0.898) and boosting (0.942).

V. DISCUSSION

The study employed 10-fold cross-validation to evaluate individual and ensemble classifiers on UNSW-NB15 and CICIDS2017 datasets. Ensemble models, especially stacking, outperformed individual classifiers, showing promise in intrusion detection. Decision Trees (DT) and Random Forests (RF) excelled in various attack types. Stacking consistently improved over other ensemble methods. Overall, the study underscores the value of ensemble learning for network security. The results suggest that the proposed approach detects cyber-attacks effectively. The stacking ensemble model outperforms other examined models in terms of accuracy, precision, recall, and F1-Score. This underscores stacking's potential to enhance cyber-attack detection. Comparison between UNSW-NB15 and CICIDS2017 datasets shows in the following table:

TABLE VI. Comparison between UNSW-NB 15 and CICID2017 dataset

Parameters	UNSW-NB15 dataset	CICIDS2017 dataset
Class size	10	8
Accuracy	Stacking:83.84% Best Individual:81.77%	Stacking:99.9% Best Individual:99.5%
Substandard performance classifier	SVM (72.32%)	SVM (71.49%)
Improvement via stalking	Substantial improvement across attacks	Consistently high accuracy
Projecting performance algorithms	DT, RF	DT, RF
F1-score for various attacks	Above 0.75	High
Conclusion	Stacking enhances classification across attacks	Stacking excels in cyber-attack detection

Detecting attacks in smart cities requires a dataset that closely represents the types of network traffic and attack patterns specific to smart city environments. While both the UNSW-NB15 and CICIDS2017 datasets are widely used for intrusion detection. The CICIDS2017 dataset gives more accuracy than the UNSW-NB15 dataset.

VI. APPLICATIONS

Effective attack detection in smart cities offers a wide range of applications since it blends cloud computing technology with cyber security and smart city infrastructure. Here are a few possible fields of use:

Smart city security: To maximize municipal operations and enhance the quality of life for citizens, smart cities make use of a variety of networked devices, sensors, and systems. However, because of their interconnection, they may be more susceptible to cyber-attacks. The security and dependability of vital smart city infrastructure may be ensured by using cloud-based cyber security technologies to assist identify and prevent possible cyber-attacks [13], [14].

Network monitoring and Intrusion detection: Cloud-based cyber security tools can continually monitor network traffic and detect suspicious behaviour. The system can detect possible cyber threats, such as DDoS assaults, malware, and unauthorized access attempts, by evaluating data from numerous sources inside the smart city ecosystem [15].

Data protection and privacy: Massive volumes of data are produced by smart cities, most of them delicate and private. Cloud computing may assist in securing this data by putting in place strong encryption, access restrictions, and data privacy methods, protecting the personal data of citizens [15].

Real-time threat analysis: Cloud computing enables the present capture and examination of enormous capacities of data from several smart city systems and devices. With the use of this skill, new risks may be detected and cyber events can be handled right away [15].

In general, the use of cloud computing in cyber security attack detection improves the security, resilience, and dependability of smart city infrastructure, eventually creating a safer and more effective urban environment for residents.

VII. CONCLUSION

The combination of UNSW-NB15 and CICIDS2017 datasets gives a highly effective strategy for improving smart city cyber-security using cloud computing. These datasets provide a significant source of information for developing improved intrusion detection systems by leveraging real-world network traffic data and labelled attack occurrences. This integration allows for the deployment of a complex defence strategy that includes anomaly detection, behavioural analysis, signature-based identification, and cutting-edge machine learning techniques. The resulting approach not only improves attack detection accuracy but also flexibility to changing threat landscapes. As smart cities evolve, harnessing insights from these datasets will become increasingly important in reinforcing vital infrastructure, maintaining data integrity, and ultimately developing resilient urban environments that thrive in the face of cyber threats.

VIII. LIMITATIONS AND FUTURE WORKS

Cloud-based cyber security solutions rely on data transmission between smart city devices and cloud servers for analysis. This data transfer can introduce latency, leading to delays in detecting and responding to cyber threats. In time-critical situations, this delay may have significant consequences.

If the internet connection is disrupted or unavailable, it can impair the ability to detect and respond to cyber threats promptly.

Smart city data often contains personal and confidential information, and outsourcing this data to third-party cloud providers can raise regulatory and compliance challenges.

As the amount of data generated by smart city devices increases, cloud-based cyber security systems need to scale accordingly to handle the growing data volumes.

While cloud providers implement robust security measures, they are not immune to cyber-attacks themselves.

To overcome these limitations, smart cities must carefully evaluate their specific requirements and potential risks when adopting cloud-based cyber security solutions. Implementing a well-rounded strategy that includes a combination of cloud and on-premise security measures can enhance the overall cyber security posture of smart cities.

As part of upcoming endeavour, the research intend to investigate the incorporation of deep learning techniques to improve the detection performance of IoT threats. As smart cities gain popularity, they also face growing exposure to cyber threats. Cyber-attacks, including access denials and privacy intrusions, pose significant risks to individuals and jurisdictions, carrying potential economic and social costs. Moreover, compromised systems handling emergencies like accidents or fires can lead to health hazards. The research findings, which highlight the effectiveness of stacked classifiers in detecting cyber-attacks within smart city systems, extend beyond technical contributions, carrying implications for economics and society. Future research endeavours will continue to offer deeper insights into these dimensions.

REFERENCES

[1] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garces, “A Comprehensive Study of the IoT Cybersecurity in Smart Cities,” IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3046442.

[2] S. Gore et al. “Innovations in Smart City Water Supply Systems,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 9s, pp. 277–281, Jul. 2023, Accessed: Aug. 18, 2023. [Online]. Available: https://www.ijisae.org/index.php/IJISAE/article/view/3118

[3] M. Tholkapiyan, S. Ramadass, J. Seetha, A. Ravuri, S. S. S, and S. Gore, “INTELLIGENT SYSTEMS AND APPLICATIONS IN Examining the Impacts of Climate Variability on Agricultural Phenology : A Comprehensive Approach Integrating Geoinformatics , Satellite Agrometeorology , and Artificial Intelligence,” vol. 11, pp. 592–598, 2023, Accessed: Aug. 18, 2023. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/2891

[4] Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, “Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities,” IEEE Access, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.

***Article Received**: 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

[5] S. Aguiar et al., “Grape bunch detection at different growth stages using deep learning quantized models,” Agronomy, vol. 11, no. 9, Sep. 2021, doi: 10.3390/agronomy11091890.

[6] R. A. Hamid, N. S. Khalid, N. A. Abdullah, N. H. A. Rahman, and C. C. Wen, “Android Malware Classification Using K-Means Clustering Algorithm,” IOP Conf. Ser. Mater. Sci. Eng., vol. 226, no. 1, 2017, doi: 10.1088/1757-899X/226/1/012105.

[7] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” Comput. Networks, vol. 174, 2020, doi: 10.1016/j.comnet.2020.107247.

[8] A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” Futur. Gener. Comput. Syst., vol. 82, pp. 761–768, 2018, doi: 10.1016/j.future.2017.08.043.

[9] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, 2009. doi: 10.1109/CISDA.2009.5356528.

[10] S. Liu and M. Whitty, “Automatic grape bunch detection in vineyards with an SVM classifier,” J. Appl. Log., vol. 13, no. 4, pp. 643–653, 2015, doi: 10.1016/j.jal.2015.06.001.

[11] Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, “A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook,” Ad Hoc Networks, vol. 130, no. 2008784, p. 102790, 2022, doi: 10.1016/j.adhoc.2022.102790.

[12] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, “Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques,” Int. J. Environ. Res. Public Heal. 2020, Vol. 17, Page 9347, vol. 17, no. 24, p. 9347, Dec. 2020, doi: 10.3390/IJERPH17249347.

[13] Kakderi, N. Komninos, and P. Tsarchopoulos, “Smart cities and cloud computing: lessons from the STORM CLOUDS experiment,” J. Smart Cities, vol. 2, no. 1, pp. 3–13, 2016, doi: 10.18063/jsc.2016.01.002.

[14] P. Su, Y. Chen, and M. Lu, “Smart city information processing under internet of things and cloud computing,” J. Supercomput., vol. 78, no. 3, pp. 3676–3695, 2022, doi: 10.1007/s11227-021-03972-5.

[15] R. Andrade, J. Torres, and L. Tello-Oquendo, “Cognitive security tasks using big data tools,” Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018, no. December, pp. 100–105, 2018, doi: 10.1109/CSCI46756.2018.00026.