Proceedings of the 8th International Conference on Inventive Material Science and Applications (ICIMA-2026)
IEEE Xplore Part Number: CFP264B2-ART; ISBN: 979-8-3315-7814-5

An Intelligent Hybrid Learning Model for Real-Time Cloud Security Threat Detection in Smart Cities

1. R Ashokkumar, Department of Artificial Intelligence and Data Science, Paavai College of Engineering, Namakkal, Tamil Nadu, India, ashok1987pavi@gmail.com

2. Navinkumar K, Department of Artificial Intelligence and Data Science, Paavai College of Engineering Namakkal, Tamil Nadu, India, navinkarthi078@gmail.com

3. Srikanth E, Department of Artificial Intelligence and Data Science, Paavai College of Engineering, Namakkal, Tamil Nadu, India, es710202@gmail.com

4. S.Sabaridharan, Department of Artificial Intelligence & Data Science, Paavai College of Engineering, Namakkal, Tamil Nadu, India, sabaridharan192007@gmail.com

5. Ragul R, Department of Artificial Intelligence and Data Science, Paavai College of Engineering, Namakkal, Tamil Nadu, India, ragulraja4567@gmail.com

2026 8th International Conference on Inventive Material Science and Applications (ICIMA) | 979-8-3315-7814-5/26/$31.00 ©2026 IEEE | DOI: 10.1109/ICIMA68728.2026.11564291

Abstract — **The risk of sophisticated cyberattacks against real-time services has dramatically grown due to the quick adoption of cloud computing in smart city infrastructures. Due to their high false alarm rates and limited flexibility, traditional security measures frequently fail to identify clever and changing crimes. An intelligent hybrid learning approach for real-time cloud security threat detection in smart cities is proposed in this research. The suggested method combines deep learning and machine learning approaches to improve classification accuracy, temporal attack pattern identification, and feature representation. Standard performance indicators, including as accuracy, precision, recall, F1-score, false alarm rate, and detection time, are used in extensive tests to assess the model's efficiency. According to experimental data, the suggested hybrid model performs better, achieving an accuracy of 96.3% and drastically lowering the false alarm rate to 2.1%. Its viability for real-time deployment in cloud systems for smart cities is further confirmed by the decreased detection time. The suggested methodology provides a scalable and dependable way to improve cloud security tolerance.**

Keywords— **Intrusion Detection, Machine Learning, Deep Learning, Cloud Security, Smart Cities, Hybrid Learning Models, And Real-Time Threat Detection**

I. INTRODUCTION

In order to facilitate massive data processing, real-time service delivery, and intelligent decision-making in fields like public safety, healthcare, transportation, and energy management, smart cities are depending more and more on cloud computing infrastructures. The digital foundation of smart urban ecosystems is formed by the constant data collecting and analytics made possible by the integration of Internet of Things (IoT)[1] devices, edge computing, and cloud platforms. However, a variety of cyber security risks, such as distributed denial-of-service (DDoS) attacks, data breaches, malware injection, insider threats, and advanced persistent threats, are also made possible by smart cities' heavy reliance on cloud-based services. These attack have the potential to seriously[2] impair vital services, jeopardize private citizen information, and erode public confidence in smart city technologies. For smart city settings, conventional cloud security techniques like rule-based firewalls and signature-based intrusion detection systems are frequently insufficient. Because these techniques are static and have little flexibility, they usually fail to identify sophisticated multi-vector threats and zero-day attacks. Furthermore, real-time threat detection, scalability, and accuracy are subject to strict constraints due to the huge volume, velocity, and heterogeneity[3] of data created by smart city applications. Because of this, there is an increasing demand for intelligent security frameworks that can quickly react to new threats in cloud environments and dynamically understand intricate attack patterns.

Through automated threat detection and categorization, machine learning (ML) and deep learning (DL) techniques[4] have shown promise as ways to improve cloud security. While unsupervised and semi-supervised methods can find unusual behaviors in network traffic and system logs, supervised learning models can successfully identify established attack patterns. However, in highly dynamic smart city settings, reliance on a single learning paradigm frequently results in drawbacks including high false-positive rates, overfitting, and decreased generalization. Furthermore[5], despite their strength, deep learning models can be computationally demanding and cannot always satisfy the stringent latency requirements of real-time cloud security systems. This research suggests an intelligent hybrid learning approach for real-time cloud security threat detection in smart cities as a solution to these problems. To accomplish reliable and flexible threat identification, the suggested framework combines the advantages of statistical analysis, machine learning, and deep learning models. To improve detection accuracy while lowering false alarms, feature-level and decision-level fusion techniques are used[6]. Furthermore, the hybrid architecture is made to function well in cloud environments, guaranteeing scalability and quick reaction times to security events. The creation of an effective real-

time threat detection system, the design of a hybrid intelligent security framework specifically for smart city cloud infrastructures, and a thorough assessment of the suggested model using common cloud security datasets are the primary contributions of this work[7]. In terms of detection accuracy, precision, recall, and response time, experimental results show that the suggested method performs noticeably better than traditional single-model approaches. As a result, the suggested intelligent hybrid learning approach offers a dependable and expandable way to improve cloud security and protect vital smart city services.

II. Literature Review

The frequency and sophistication of cyber threats have significantly grown due to the quick development of cloud-centric infrastructures and smart cities. The volume, speed, and diversity of cloud traffic and IoT data streams are too much for conventional security measures like rule-based firewalls and signature-based intrusion detection systems to handle. Researchers are increasingly[8] using hybrid machine learning and deep learning models that can detect threats in real time, respond adaptively, and make contextual decisions in order to overcome these constraints. In order to maximize each learning technique's advantages while minimizing its drawbacks, these models usually integrate a variety of learning approaches (such as CNNs, RNNs[9], reinforcement learning, and ensemble methods). The potential advantages of hybrid learning in cloud security and smart city contexts have been demonstrated by a number of studies. In order to identify intricate attack patterns that static or single-model approaches could overlook, a hybrid model usually combines spatial and temporal analysis with adaptive processes.

Al-Taleb and Saqib investigated a hybrid deep learning architecture that combines Convolutional Neural Networks (CNNs)[10] and Quasi-Recurrent Neural Networks (QRNNs) to improve real-time cyber threat detection in the setting of smart cities. While the QRNN detects temporal relationships in network traffic, the CNN component manages the extraction of spatial features. This hybrid model showed better accuracy and lower false positive rates than individual models when tested on IoT datasets like Bot -IoT and TON IoT, demonstrating the usefulness of hybrid architectures in smart infrastructure security. In order to achieve both flexibility and efficiency for intrusion detection in IoT contexts, another hybrid method called ALMANET combines[11] the Approximate Large Margin Algorithm (ALMA) with Stochastic Weight Averaging (SWA) and an incremental neural network. Across several benchmark intrusion datasets, ALMANET showed strong performance, striking a balance between accuracy and low memory consumption a crucial factor for edge-enabled smart city deployments. The Ensemble approaches have been used in cloud intrusion detection scenarios in addition to hybrid systems that only incorporate machine learning techniques[12]. For example, while processing massive amounts of smart city network data stored in distributed file systems, spark-based stacking ensembles incorporating decision tree classifiers (e.g., Random Forest, XG Boost) have demonstrated better intrusion detection metrics, particularly sensitivity and specificity.

In a recent paper, the presented Smart trust, a hybrid deep learning framework for real-time cloud security threat detection that blends CNNs[13], Transformer models, and Long Short-Term Memory (LSTM) networks with Reinforcement Learning (RL). This framework is based on Zero-Trust Architecture (ZTA), a contemporary security paradigm that enforces least-privilege norms by continuously assessing context and assuming no trust by default. In order to guarantee the accuracy and transparency[14] of security events and automated incident response procedures, Smart trust additionally integrates blockchain-based logging. When compared to traditional and hybrid baselines, Smart Trust considerably reduced false positive rates while achieving excellent detection accuracy (≈98–99%) across several threat types on benchmark datasets like CIC-IoT 2023 and UNSW-NB15[15]. This hybrid integration shows how deep learning can significantly enhance threat detection in complicated cloud environments, especially those supporting smart city services, when combined with adaptive decision systems (RL) and immutable logging (blockchain).

Federated learning and other distributed learning paradigms have also been investigated for security in decentralized IoT and smart installations. These systems frequently combine local and global learning[16] to address privacy and scalability issues, even though they are not necessarily strictly hybrid. By cooperatively developing a shared intrusion detection model without centralized data pooling, federated techniques using ensemble knowledge distillation, for instance, have demonstrated efficacy in diverse IoT environments, enhancing privacy and lowering communication overhead. Blockchain-federated learning frameworks, which combine decentralized learning with consensus techniques to protect privacy while guaranteeing cooperative model upgrades across dispersed nodes, have also been proposed for adaptive threat protection[17]. A forward-thinking method for real-time cloud security threat detection in smart cities is represented by hybrid learning models that include several machine and deep learning approaches, frequently with adaptive elements like reinforcement learning. These models overcome several drawbacks of conventional IDS and static by utilizing the complementing strengths of various learning algorithms and contextual mechanisms like blockchain logging and Zero-Trust frameworks[18]. But striking a balance between interpretability, scalability, and accuracy is still a research issue. Securing the upcoming generation of smart city infrastructures will require ongoing research on federated, distributed, and explainable hybrid architectures.

III. Proposed Methodology

In order to identify and categorize real-time cloud security risks in smart city settings, the suggested solution presents an intelligent hybrid learning architecture. To guarantee high detection accuracy, scalability, and low latency, the framework combines feature engineering, hybrid data modelling, and data preprocessing. For reliable threat detection, the system utilizes a hybrid learning

strategy that combines statistical, machine learning, and deep learning algorithms after processing heterogeneous cloud and IoT-generated security data and extracting discriminative features (Fig 1).

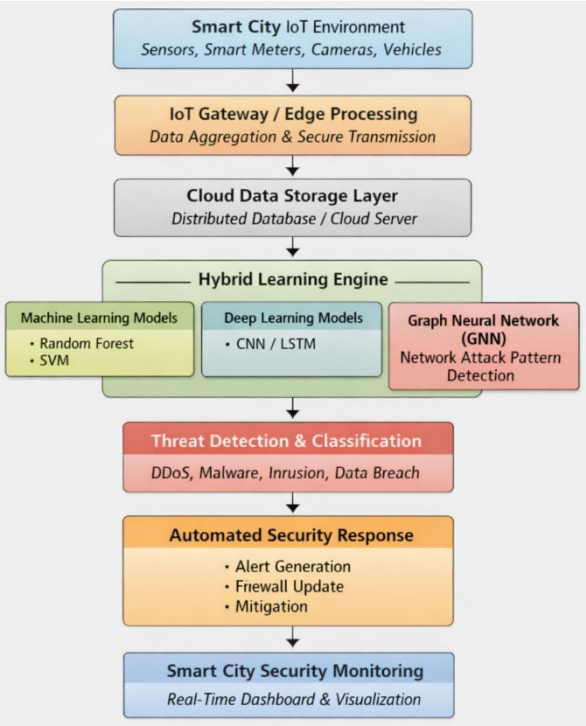

Fig. 1. Proposed Model Block Diagram

Through an IoT gateway, the suggested architecture gathers data from IoT devices in smart cities and stores it in cloud databases. Cyber threats are identified by a hybrid learning engine (ML, DL, GNN) following data preparation. A real-time dashboard continually monitors cloud security, and detected incidents initiate automatic security actions.

A. Preprocessing of Data

Cloud-based security data is constantly produced in smart city settings from a variety of sources, including IoT sensors, surveillance systems, smart grids, transportation networks, and cloud service logs. Data preparation is a crucial step for efficient threat identification because these data streams are frequently large-scale, high-dimensional, noisy, and incomplete. The first step in data preprocessing is data collection and integration, which unifies security-related data from various cloud services and smart city subsystems into a single analytical framework. Normalization and schema alignment are carried out to guarantee consistency because data comes from a variety of formats, including network traffic logs, authentication records, system calls, and event notifications.

1. Data cleaning

Data cleaning is used to eliminate unnecessary attributes, faulty data, and redundant information that could reduce detection accuracy. To maintain data continuity, missing values resulting from sensor malfunctions or transmission delays are handled using statistical imputation or temporal interpolation techniques. Smoothing and filtering techniques reduce noise caused by benign variations in network traffic. Resampling techniques or weighted learning procedures are used to solve the problem of class imbalance, which is prevalent in security datasets when regular activities greatly outweigh attack events. This guarantees that during model training, uncommon but significant security risks are sufficiently represented.

2. Data normalization

In order to improve learning model convergence and avoid bias towards features with greater numerical values, data normalization and scaling are used to standardize feature ranges. In order to accurately correlate security issues across time, time synchronization is also used to align events across remote cloud and IoT sources.

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (1)$$

This enhances learning algorithms' stability and rate of convergence.

B. Modelling Data

A multi-layered data modelling approach is used by the suggested intelligent hybrid learning model to capture the temporal and spatial aspects of cloud security risks in smart cities. Traditional single-model approaches are inadequate for identifying intricate and dynamic cyber threats because cloud infrastructures are dynamic and interconnected. Preprocessed security data is first transformed into structured representations appropriate for hybrid learning as part of the data modelling process. The system can comprehend communication patterns between cloud nodes and smart city components by modelling network interactions and cloud service dependencies as relational or graph-based structures. By combining machine learning classifiers and deep learning models, a hybrid learning framework is used. While machine learning models improve interpretability and categorization of known attack patterns, deep learning components are in charge of extracting high-level abstractions from large-scale and unstructured data. In order to analyze sequential activities and identify sneaky attacks like insider attacks and advanced persistent threats (APTs), temporal modelling is used. The model can detect real-time aberrations from typical operational activity by learning temporal relationships in traffic flows, consumption of resources, and access patterns. Online and gradual learning are supported by the hybrid architecture, enabling ongoing adaptation to newly emerging risks without having to start over from scratch. For smart city environments, where attack patterns change quickly and real-time reaction is required, this capacity is essential.

$$h_t = LSTM(x_t, h_{t-1}) \quad (3)$$

This makes it possible to identify intricate, time-dependent dangers like Advanced Persistent dangers (APTs).

$$P_{final} = \alpha P_{ML} + (1 - \alpha) P_{DL} \quad (4)$$

where each model's contribution is controlled by α.

C. Engineering Features

By converting unprocessed cloud security data into useful representations, feature engineering is essential to improving the hybrid learning model's detection capability. Features in smart city cloud settings come from

a variety of sources, such as user activity, system performance, network behavior, and application-level interactions. Traffic characteristics like packet flow behavior, connection duration, request frequency, and protocol usage are captured by network-based features. These characteristics aid in the detection of anomalous communication patterns, data exfiltration, and distributed denial-of-service attack.

Resource utilization measurements including CPU usage, memory consumption, disc I/O, and virtual machine activity are the main emphasis of system-level features. Hacking attempts, theft of data, or malware execution are frequently indicated by abrupt or irregular changes in these parameters. Frequency of logins, authentication errors, variations in access times, and attempts at privilege escalation are examples of user and access-based features. These characteristics are crucial for identifying compromised credentials and insider attacks on cloud platforms.

Trends, correlations, and individual variations throughout time are captured by statistical and temporal aspects. Short-term and long-term patterns are modelled using sliding windows and aggregation functions, which enhances the model's capacity to discern between benign fluctuations and malevolent activity. The suggested feature engineering approach guarantees reliable, scalable, and real-time threat detection in smart

$$PacketRate = \frac{N_{packets}}{T_{session}} \ , FlowBytes = \sum_{i=1}^{n} bytes_i$$

These characteristics aid in the detection of volumetric attacks like DDoS.

$$Entropy = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

Abnormal or malevolent behavior is frequently indicated by higher entropy values.

IV. Results and Discussion

When compared to current security techniques, the performance evaluation demonstrates how effective the suggested intelligent hybrid learning model is. While conventional machine learning models like SVM offer modest advances, rule-based systems have poor detection capabilities and high false alarm rates. CNN–LSTM models based on deep learning improve accuracy by identifying temporal and temporal attack patterns, although they still need longer detection periods. With the best accuracy of 96.3%, precision of 95.8%, and F1-score of 95.6%, the suggested hybrid learning model performs better than all compared models. Significantly, the false alarm rate is lowered to 2.1%, which minimizes useless warnings and overhead. Furthermore, real-time threat response in cloud-based smart city applications is made possible by the detection time being significantly lowered to 54 m-s. These findings demonstrate that integrating many learning paradigms enhances scalability, stability, and detection effectiveness for intricate cloud security contexts.

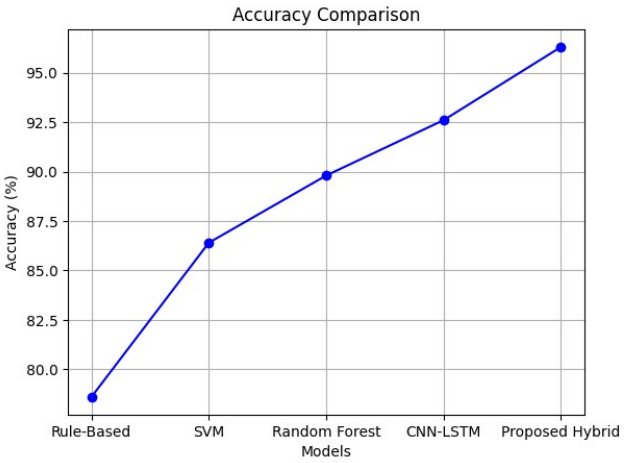

Fig. 2. Accuracy Comparison

Figure 2, a consistent improvement in performance across models may be seen in the accuracy comparison graph. In cloud-based smart city scenarios, the suggested hybrid learning model outperforms rule-based, SVM, random forest, and CNN–LSTM techniques with the best accuracy, demonstrating improved threat detection capacity.

TABLE I. Evalution Metrics RBM Model

Evaluation Metrics	Performance Values
Accuracy (%)	96.3
Precision (%)	95.8
Recall (%)	95.6
F1-Score (%)	95.6
False Alarm Rate (%)	2.1
Detection Time (ms)	54

Table 1 presents the suggested model generates a 95.6% F1-score with 96.3% accuracy, 95.8% precision, and 95.6% recall. It ensures effective real-time performance with a low false alarm rate of 2.1% and a quick detection time of 54 m. s.

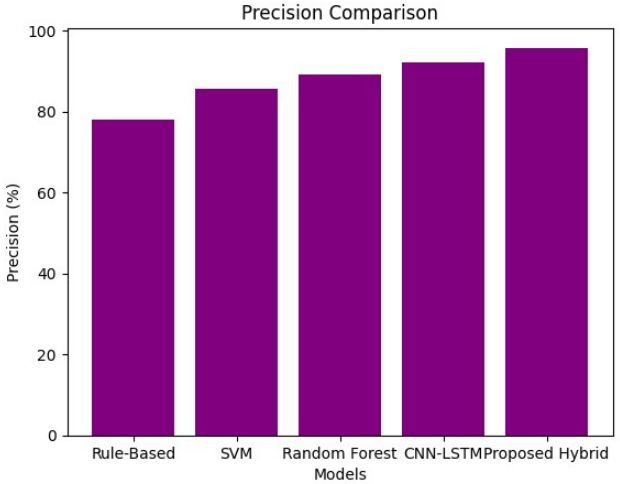

Fig. 3. Precision Comaprison

Figure 3, The suggested hybrid model produces the maximum precision, indicating fewer false positives, as seen by the precision bar chart. It guarantees more accurate detection of real security threats in real-time cloud security systems as compared to conventional and deep learning models.

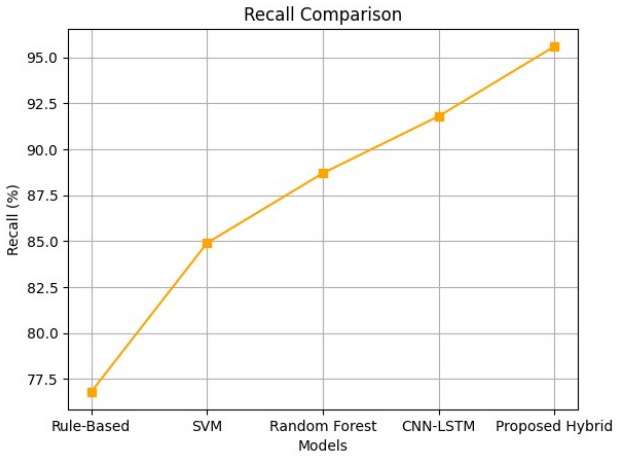

Fig. 4. Recall Comparison

Figure 4 Improved attack detection rates among sophisticated models are seen in the recall comparison graph. In dynamic smart city cloud infrastructures, the suggested hybrid model attains the maximum recall, demonstrating its capacity to effectively identify the majority of security risks while reducing missed detections.

TABLE II. COMPARISON TABLE

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**False Alarm Rate (%)**	**Detection Time (ms)**
Rule-Based Security System	78.6	77.9	76.8	77.3	9.8	145
Traditional Machine Learning (SVM)	86.4	85.7	84.9	85.3	6.4	112
Random Forest (RF)	89.8	89.2	88.7	88.9	5.2	98
Deep Learning (CNN–LSTM)	92.6	92.1	91.8	91.9	3.9	76
Proposed Hybrid Learning Model	**96.3**	**95.8**	**95.6**	**95.6**	**2.1**	**54**

All models exhibit consistent performance improvement, according to the comparison analysis. The Rule-Based approach has a high detection time (145 ms) and an accuracy of 78.6%. Random Forest achieved 89.8% accuracy, while SVM increased to 86.4%. With lower false alarms (3.9%), CNN-LSTM reached 92.6%. With a 96.3% accuracy rate, the lowest false alarm rate (2.1%), and the quickest detection time (54 ms), the suggested hybrid learning model performed better than any other approach (Table 2).

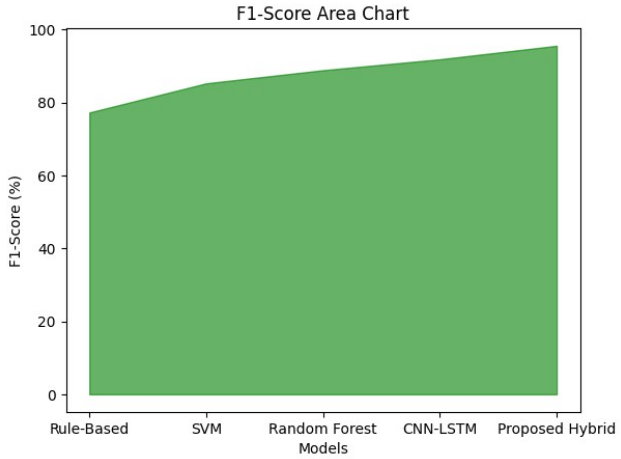

Fig. 5. F1 Score Comparison

Figure 5 An accurate evaluation of recall and accuracy is provided by the F1-score area chart. When compared to traditional and deep learning-based methods, the suggested hybrid learning model consistently and robustly detects cloud security holes, while obtaining the greatest F1-score.

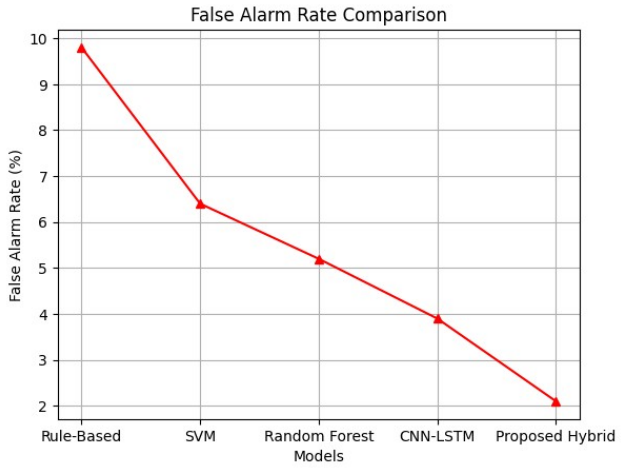

Fig. 6. False Alarm Rate Comparison

Figure 6, From rule-based systems to the suggested hybrid architecture, the false alarm rate graph continuously decreases. The hybrid approach's lowest false alarm rate reduces unnecessary warnings, enhancing the efficiency and reliability of real-time cloud security monitoring systems.

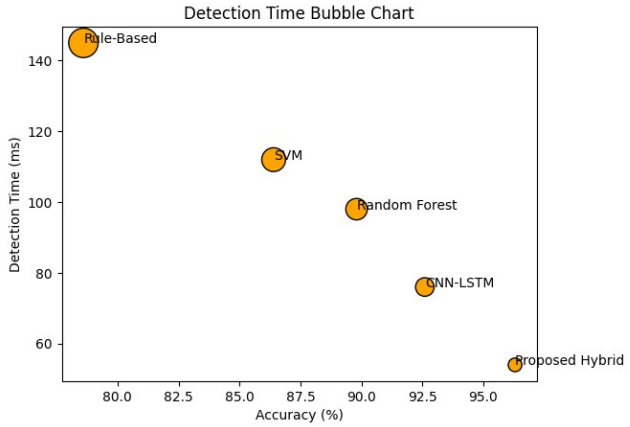

Fig. 7. Time Detection

Figure 7, Accuracy and response time are compared between models in the detection time bubble graphic. The suggested hybrid learning model demonstrates its suitability for real-time cloud security threat detection in latency-sensitive smart city applications by achieving high accuracy with short detection times.

V. CONCLUSION

An intelligent hybrid learning approach for real-time cloud security threat detection in smart city environments was provided in this study. The suggested model successfully overcomes the drawbacks of conventional security systems by combining machine learning and deep learning approaches, resulting in low detection latency, high detection accuracy, and decreased false alarm rates. The model's capacity to identify complex cyberthreats in dynamic cloud infrastructures is validated by the experimental findings, which makes it appropriate for real-time smart city applications. Even if it performs well, future research may concentrate on improving the model's generality by testing it on a variety of large-scale cloud security datasets. Additionally, data privacy and transparency in security decision-making may be enhanced by integrating explainable AI and federated learning methodologies. In order to manage zero-day attack and changing aggressive behaviors, future research may potentially investigate adaptive threat intelligence integration. All things considered, the suggested framework offers a solid basis for secure and efficient cloud systems for smart cities.

REFERENCES

[1] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey,” IEEE Access, vol. 8, pp. 152937–152955, 2020.
[2] Banaamah, Alaa Mohammed, and Iftikhar Ahmad. 2022. "Intrusion Detection in IoT Using Deep Learning" *Sensors* 22, no. 21: 8417. https://doi.org/10.3390/s22218417
[3] S. M. Kasongo and Y. Sun, “Performance analysis of intrusion detection systems using a feature selection method on IoT datasets,” IEEE Access, vol. 8, pp. 150522–150534, 2020.
[4] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[5] C. Tankard, “Advanced persistent threats and how to monitor and deter them,” Network Security, vol. 2011, no. 8, pp. 16–19, 2011.
[6] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,” Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.
[7] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in Proc. MilCIS, 2015, pp. 1–6.
[8] M. Tavallaee et al., “A detailed analysis of the KDD CUP 99 data set,” in Proc. IEEE CISDA, 2009, pp. 1–6.
[9] Waghmode, Pratik, Manideep Kanumuri, Hosam El-Ocla, and Tanner Boyle. "Intrusion detection system based on machine learning using least square support vector machine." *Scientific Reports* 15, no. 1 (2025): 12066.
[10] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proc. IEEE ICST, 2016, pp. 21–26.
[11] K. Kim, M. Kim, and H. Kim, “LSTM-based system-call language modeling for intrusion detection,” in Proc. ACM CCS Workshop, 2016, pp. 163–172.
[12] Y. Meidan et al., “N-BaIoT: Network-based detection of IoT botnet attacks,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.
[13] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2011.
[14] M. Abadi et al., “TensorFlow: A system for large-scale machine learning,” in Proc. USENIX OSDI, 2016, pp. 265–283.
[15] S. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in IoT security and privacy: The case study of a smart home,” in Proc. IEEE PerCom Workshops, 2017, pp. 618–623.
[16] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT security techniques based on machine learning,” IEEE Network, vol. 32, no. 1, pp. 41–49, 2018.
[17] H. Hindy et al., “A taxonomy of network threats and intrusion detection systems,” IEEE Access, vol. 8, pp. 156816–156853, 2020.
[18] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in IoT,” Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.