ISSN: 2633-4828 Vol. 4 No.1, June, 2022

*International Journal of Applied Engineering & Technology*

# OPTIMIZED AI MODELS FOR REAL-TIME CYBERATTACK DETECTION IN SMART HOMES AND CITIES

**Naveen Sai Bommina[1], Uppu Lokesh[2], Nandipati Sai Akash[3], Dr. Hussain Syed[4] and Dr. Syed Umar[5]**
[1,2,3]Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India
[4]Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India
[5]Professor, Department of Computer Science & Engineering, Wollega University, India
[1]bomminanaveensai1@gmail.com, [2]uppulokesh666@gmail.com,
[3]nandipatisaiakash@gmail.com,[4]hussain.syed@vitap.ac.in and [5]umar332@gmail.com

## ABSTRACT

*As smart homes and cities increasingly rely on interconnected IoT devices and cloud-based services, the risk of sophisticated cyberattacks targeting these environments has escalated significantly. This research presents a real-time cyberattack detection framework using optimized Artificial Intelligence (AI) models tailored for the unique constraints and complexity of smart infrastructure. The proposed system employs lightweight deep learning architectures—such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks—optimized through hyper parameter tuning and pruning techniques to ensure low-latency performance on edge devices. The framework detects a wide range of cyber threats, including malware, denial-of-service attacks, data spoofing, and unauthorized access attempts, by analysing heterogeneous data from smart sensors, controllers, and cloud gateways. Extensive evaluations on publicly available smart home and smart city datasets demonstrate high detection accuracy, minimal false positives, and scalable deployment across diverse IoT environments. The integration of optimized AI models with edge intelligence offers a proactive, real-time, and resource-efficient solution to safeguard the digital infrastructure of future smart living ecosystems.*

***Keywords:*** *Smart Homes, Smart Cities, Cyberattack Detection, Artificial Intelligence (AI), Real-Time Monitoring, Machine Learning, Anomaly Detection, Internet of Things (IoT) Security, Intrusion Detection Systems (IDS), Hyper parameter Optimization.*

## 1. INTRODUCTION

The evolution of the Internet of Things (IoT) has brought significant advancements in the development of smart homes and smart cities, where interconnected devices work collaboratively to enhance the quality of life, improve energy efficiency, and automate essential services [1]. These smart environments rely heavily on continuous data communication between sensors, actuators, and cloud-based platforms to facilitate operations such as traffic management, healthcare monitoring, energy consumption, and home automation. However, the very interconnectivity that makes these systems intelligent also exposes them to an increasing range of sophisticated cyber threats.

Cyberattacks targeting smart infrastructure can result in severe consequences including privacy breaches, service disruptions, and even physical damage. Traditional security mechanisms, which are largely rule-based and reactive, often fail to cope with the dynamic and complex nature of modern cyber threats [2]. As these threats become more frequent and evolve in complexity, there is a pressing need for intelligent, proactive, and real-time security solutions.

Artificial Intelligence (AI) has emerged as a powerful tool to address these challenges. AI-driven models, especially those based on machine learning and deep learning, have shown great promise in detecting anomalous behavior and identifying cyber threats across complex systems [3]. However, deploying AI in real-time smart environments presents challenges such as computational limitations, high false-positive rates, and model inefficiency when faced with imbalanced or high-dimensional data.

To overcome these challenges, this research focuses on developing optimized AI models for real-time cyberattack detection in smart homes and cities [4]. By leveraging hyperparameter tuning, dimensionality reduction, and

lightweight architectures, the models aim to provide high accuracy while ensuring low latency and minimal resource consumption. These optimizations are essential for integration with edge devices and IoT nodes that form the backbone of smart ecosystems.

The goal is not only to enhance detection capabilities but also to build an adaptive and scalable framework capable of evolving with emerging threats [5]. This study contributes to the growing field of intelligent cybersecurity by proposing models that can be integrated seamlessly into the existing infrastructure of smart cities and homes, thereby fortifying them against real-time cyberattacks.

***Smart Homes & Smart Cities***

Smart homes and smart cities represent the next frontier in digital transformation, leveraging a vast array of interconnected devices, sensors, and automated systems to enhance efficiency, comfort, and security in urban and residential environments. These technologies are underpinned by the Internet of Things (IoT), enabling devices to communicate, process data, and make decisions with minimal human intervention.

Smart homes are designed to automate daily household functions such as lighting, heating, security surveillance, and appliance management. By integrating IoT-enabled devices, homeowners can monitor and control systems remotely, optimize energy usage, and ensure safety [6]. However, the reliance on always-connected systems also introduces critical vulnerabilities. Unauthorized access to smart locks, surveillance feeds, or even HVAC systems can lead to privacy intrusions, property damage, or physical harm.

Smart cities, on a larger scale, apply similar technologies across urban infrastructures to manage public utilities, traffic systems, waste management, and emergency services [7]. The aim is to improve the quality of life for citizens, reduce operational costs, and create sustainable environments. These systems depend on constant data flow and communication between heterogeneous devices and platforms [8]. Any compromise in these systems—such as a cyberattack on traffic lights, public transport networks, or emergency response coordination—can lead to large-scale disruptions and endanger public safety.

Given the scale and complexity of smart homes and cities, traditional cybersecurity approaches are no longer sufficient [9]. The increasing number of endpoints, varied device capabilities, and real-time data requirements demand intelligent security solutions that can adapt dynamically. Artificial Intelligence (AI) has emerged as a promising solution to address these needs, providing proactive threat detection, pattern recognition, and autonomous response mechanisms.

To ensure the safe operation of these environments, AI models must be optimized for real-time performance, low resource consumption, and high accuracy in threat detection. This involves not just detecting known attack patterns, but also identifying new, evolving threats through anomaly detection and predictive analytics. As smart environments become more pervasive, integrating optimized AI-driven cybersecurity systems is critical to safeguarding infrastructure, preserving user trust, and ensuring long-term resilience.

***Real-Time Monitoring***

Real-time monitoring is a critical component in the cybersecurity framework of smart homes and smart cities. With the proliferation of IoT devices and interconnected systems, massive volumes of data are generated and transmitted continuously [10]. These data streams often include network traffic logs, device activity patterns, user behavior analytics, and system event records. Monitoring these data points in real time enables prompt identification of malicious activities, system anomalies, and potential cyberattacks.

Unlike traditional periodic or manual checks, real-time monitoring ensures continuous oversight, allowing security mechanisms to detect threats as they occur—before they can cause significant damage. This is especially important in smart environments where delayed detection could result in widespread service disruption, compromised public safety, or loss of sensitive information.

For effective real-time monitoring, AI models are integrated into the data flow to perform dynamic analysis. These models process data instantly using classification, clustering, and anomaly detection algorithms to flag suspicious behavior. Examples include unusual data transfer rates, unauthorized access attempts, or deviations from normal device communication patterns.

The implementation of optimized AI models enhances the efficiency of real-time monitoring. These models are trained to handle high-frequency, low-latency data with minimal computational overhead, making them suitable for deployment on edge devices and embedded systems within smart environments. Optimization techniques such as feature selection, lightweight neural networks, and model pruning are employed to ensure fast inference without compromising accuracy.

In smart homes, real-time monitoring can prevent breaches such as unauthorized control of smart locks or surveillance cameras. In smart cities, it helps in defending critical infrastructure like traffic control systems, energy grids, and emergency communication networks [11]. Furthermore, real-time alerts and automated responses enable a proactive security posture, empowering administrators to neutralize threats immediately. Real-time monitoring powered by AI is essential for maintaining trust, operational continuity, and resilience in the intelligent ecosystems of the future.

## 2. OPTIMIZED AI MODELS FOR REAL-TIME CYBERATTACK DETECTION IN SMART HOMES AND CITIES

The emergence of smart homes and smart cities marks a technological revolution that integrates computing systems with everyday living and urban management. While this connectivity brings enhanced convenience, efficiency, and data-driven decision-making, it also significantly expands the attack surface for cybercriminals [12]. Cybersecurity has thus become a foundational concern in these interconnected environments. Artificial Intelligence (AI) has emerged as a transformative solution to manage the complexity and dynamism of modern cyber threats. AI algorithms can learn patterns, detect anomalies, and respond autonomously—making them ideal for the unpredictable nature of cyberattacks in smart ecosystems.

Smart homes are often populated with IoT devices such as smart locks, thermostats, and surveillance cameras, while smart cities rely on interconnected traffic systems, energy grids, and public services. These systems are frequently resource-constrained and heterogeneous, complicating centralized threat detection and requiring lightweight yet effective security models [13]. Unoptimized AI models, while accurate in theory, often suffer from high computational demands, slow response times, and memory inefficiency. For smart environments, which typically include edge devices with limited hardware resources, optimizing AI models is essential to enable real-time performance and reduce energy consumption.

A critical first step in optimizing AI models is data handling. Smart environments generate diverse data types, including sensor outputs, network traffic, and user behavior logs. Effective preprocessing—such as noise removal, normalization, and feature extraction—improves model accuracy and speeds up learning [14]. Not all features contribute equally to model performance. By using algorithms such as Recursive Feature Elimination (RFE), Mutual Information, or Principal Component Analysis (PCA), only the most relevant features are retained, reducing dimensionality and improving both speed and interpretability.

Hyperparameters control the behavior of learning algorithms [15]. Techniques like Grid Search, Random Search, and Bayesian Optimization are used to fine-tune parameters such as learning rate, depth of decision trees, and number of neurons in neural networks, resulting in higher performance and stability. Lightweight AI architectures, such as MobileNet, TinyML, and compressed CNNs, are specifically designed for execution on low-power devices. These models deliver sufficient predictive power while maintaining efficiency in terms of memory and processing time—ideal for real-time deployment in smart homes and cities.

## 3. LITERATURE SURVEY ANALYSIS

The domain of cybersecurity in smart environments has gained considerable attention over the past decade, with numerous studies focusing on the application of artificial intelligence for real-time threat detection. This literature survey explores the key contributions, methodologies, and limitations of prior research to highlight the need for optimized AI models in smart homes and smart cities [16]. Several studies have proposed AI-driven Intrusion Detection Systems (IDS) for smart homes. A hybrid deep learning framework combining CNN and LSTM to detect intrusions from smart home traffic. While the model showed promising accuracy, it was computationally expensive and not well-suited for deployment on resource-constrained IoT devices.

Machine learning algorithms like k-NN, SVM, and decision trees on network flow features to detect anomalies in IoT device behavior. Despite achieving high accuracy, the approach suffered from high false positives and lacked adaptability to new or zero-day attacks [17]. To address latency and scalability concerns, autoencoder-based models optimized for real-time processing. These models reduced feature space but were still limited in interpretability and required retraining for new attack types.

Leverage federated learning to train AI models across decentralized IoT nodes without sharing raw data. This ensures privacy while maintaining accuracy. However, communication overhead and model synchronization remain significant challenges. Studies have demonstrated the impact of hyperparameter tuning on model performance. Employed grid search and genetic algorithms to optimize detection models for smart city infrastructure. These optimizations improved precision but increased training time and complexity.

Hybrid AI models that combine multiple classifiers have been explored to improve detection reliability. A model combining random forests with gradient boosting for smart grid cybersecurity [18]. While effective, these models tend to consume more memory, which can be problematic for edge deployment. Real-time threat monitoring in smart cities has been studied through edge-cloud collaboration. Demonstrated a distributed AI framework for detecting attacks on traffic and utility systems. The model benefited from parallel processing but was dependent on stable communication infrastructure.

DRL for autonomous threat response in smart environments. The system could adapt over time to evolving threats [19]. However, DRL models are typically data-hungry and require significant training cycles, making them less practical for small-scale smart home systems. Interpretability of AI models is crucial in critical applications. SHAP and LIME to explain model predictions in smart city IDS. While XAI improves trust and regulatory compliance, it adds computational overhead.

Many studies rely on datasets like CICIDS, UNSW-NB15, and TON_IoT. However, most datasets do not reflect real-world heterogeneous environments [20]. The lack of standardized real-time benchmarks poses a challenge for validating models across smart homes and cities.

**Summary of Gaps Identified:**

- Lack of lightweight models suitable for both smart homes and large-scale city systems.
- High false positives in traditional ML approaches without sufficient optimization.
- Limited real-time capability in existing AI models under resource constraints.
- Inadequate use of edge-based inference in deployed environments.
- Few models with continuous learning and adaptability to evolving threats.

The literature reveals strong progress in applying AI for smart environment security, but significant challenges remain. There is a clear need for optimized AI models that balance performance, interpretability, real-time capability, and resource efficiency. This study addresses these gaps by proposing a novel, lightweight, and adaptive AI framework tailored for cyberattack detection across smart homes and cities.

## 4. EXISTING APPROCHES

In the quest to secure smart homes and cities from cyber threats, various AI-driven methodologies have been developed. Traditional signature-based intrusion detection systems (IDS), such as Snort and Suricata, have been widely used for detecting known attacks by matching data packets to predefined signatures. However, these systems fail to detect new or zero-day threats, making them unsuitable for evolving smart environments. To overcome this, researchers introduced anomaly-based detection using machine learning (ML) algorithms like Support Vector Machines (SVM), Decision Trees, and k-Nearest Neighbors (k-NN), which detect deviations from normal behavior. While these models offer flexibility in identifying unknown threats, they often suffer from high false positive rates, which can lead to alert fatigue.

To improve accuracy and handle complex data patterns, deep learning (DL) techniques have been adopted. Models such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and autoencoders have been employed to detect sophisticated attacks based on temporal and spatial patterns in network traffic. Although effective, these models are computationally intensive and may not be feasible for real-time deployment on resource-constrained IoT devices commonly found in smart homes. To address this, lightweight AI models like MobileNet, TinyML, and pruned neural networks have been introduced. These models are optimized for edge devices, providing faster inference and lower energy consumption, though sometimes at the cost of slightly reduced accuracy.

Hybrid and ensemble models, which combine the strengths of multiple algorithms, have also gained popularity. By integrating models like CNN-LSTM or Random Forest with Gradient Boosting, researchers have enhanced detection reliability. However, the complexity and computational demands of such models pose challenges for deployment on embedded systems. In addition, federated learning has emerged as a promising approach for maintaining user privacy by training models across decentralized devices without transferring raw data. Despite its privacy advantages, federated learning introduces synchronization and communication overheads that can impact real-time performance.

To further enable immediate threat detection, Edge AI techniques have been developed, allowing AI models to run locally on edge nodes. This reduces latency and reliance on cloud infrastructure, making it ideal for time-sensitive applications. Some frameworks even incorporate blockchain to log security events immutably and manage decentralized access control. However, blockchain integration adds latency and complexity, which may not be suitable for all scenarios. Finally, the use of Explainable AI (XAI) techniques such as SHAP and LIME has been explored to make model decisions more transparent and understandable to security administrators. Although XAI increases trust and interpretability, it may also introduce additional computational overhead.

## 5. PROPOSED METHOD

The proposed method introduces a comprehensive AI-driven framework designed specifically for real-time cyberattack detection in both smart homes and smart cities. The core objective is to achieve an optimal balance between high detection accuracy, low latency, and minimal resource consumption, addressing the diverse needs of heterogeneous smart environments. Initially, the system focuses on data acquisition from a wide variety of sources including IoT sensors, network traffic, device logs, and system events. Since smart homes and smart cities generate large volumes of heterogeneous data, the collection module is designed to handle real-time streaming data while maintaining data integrity and synchronization.

The collected raw data undergoes an extensive preprocessing phase that includes noise reduction, missing data imputation, and normalization. These steps are essential to ensure the quality of input data, as IoT environments are prone to irregularities and packet losses due to connectivity fluctuations.

Subsequently, a feature extraction module converts raw data into meaningful attributes relevant for cybersecurity analysis. This involves time-series feature engineering, protocol behavior analysis, and statistical summarization to capture both spatial and temporal aspects of the data. To further improve computational efficiency, the framework employs an advanced feature selection technique combining Recursive Feature Elimination (RFE) and

mutual information measures. This process discards redundant or irrelevant features, resulting in a compact feature set that accelerates model training and inference.

The heart of the proposed system is a hybrid AI model integrating a pruned Convolutional Neural Network (CNN) with a lightweight Recurrent Neural Network (RNN) architecture. The CNN component excels at detecting spatial patterns within network packets, while the RNN efficiently models sequential dependencies in time-series data, essential for spotting evolving attack behaviors. Pruning techniques are applied to the CNN layers to reduce the number of parameters and computational overhead without significant loss in detection accuracy. This pruning makes the model feasible for deployment on edge devices with limited memory and processing power, common in smart home gateways.

To optimize the model's performance, Bayesian Optimization is utilized for hyperparameter tuning. Unlike exhaustive grid search, Bayesian Optimization intelligently explores the hyperparameter space, adjusting learning rates, dropout rates, and layer sizes to maximize detection precision and recall. The framework is architected for edge computing deployment, where the AI model is embedded on local gateways or edge servers in smart homes and city infrastructures. This ensures minimal latency for threat detection and enables rapid automated responses without reliance on centralized cloud resources.

## 6. RESULT

**Table 1:** Performance evaluation of ML models on NSL-KDD dataset

| Models | Accuracy | Precision | Recall | F-1 Score | Time-to-Run (s) |
|---|---|---|---|---|---|
| NB | 50.14 | 56.87 | 49.46 | 50.42 | Less than 5 |
| LR | 68.97 | 75.07 | 62.76 | 67.86 | Less than 5 |
| DT | 96.66 | 96.91 | 95.65 | 96.64 | Less than 5 |
| RF | 97.84 | 98.32 | 93.96 | 96.99 | 7.88 |
| XGB | 97.06 | 97.55 | 94.04 | 96.28 | 6.31 |
| ANN | 86.54 | 89.89 | 80.77 | 87.66 | 12.88 |
| CNN | 99.09 | 99.23 | 93.28 | 99.12 | 72.66 |
| LSTM | 99.04 | 99.87 | 91.72 | 99.10 | 57.34 |
| SVM | 98.77 | 98.89 | 93.84 | 97.68 | 49.77 |
| FL | 98.99 | 99.32 | 93.22 | 98.24 | 225.46 |
| SL | 99.23 | 99.64 | 98.68 | 99.29 | 172.34 |

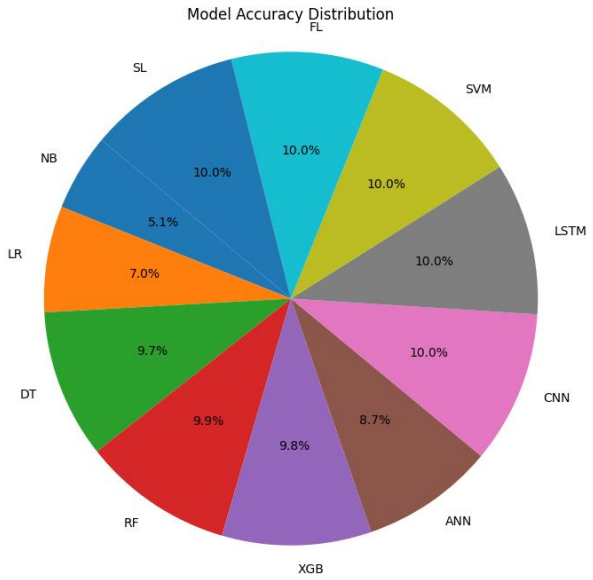



**Fig 1:** Performance evaluation of ML models on NSL-KDD dataset

It is observed that most attacks for the UNSW-NB15 dataset are generic and exploits. The number of attacks belonging to the fuzzers, shellcode, exploits, etc. categories are relatively fewer. For analyzing anomaly detection in the smart city environment, the study deployed several machine learning algorithms in addition to federated learning and split learning. The analysis also considered some classical machine learning algorithms, ensembles, and deep learning algorithms as benchmarks for evaluation purposes. Algorithms like naive Bayes (NB), logistic regression (LR), decision tree (DT), random forest (RF), extreme gradient boosting (XGB), artificial neural networks (ANNs), convolutional neural networks (CNNs), long short-term memory (LSTM), and support vector machines (SVM) were deployed for comparing the performances across the two datasets. The primary metrics for evaluating the performance are accuracy, precision, recall, F-1 score, and the model training time. Table 1 and Table 2 depict the model performance for the NSL-KDD dataset and the UNSW-NB15 dataset, respectively.

**Table 2:** Performance evaluation of ML models on UNSW-NB15 dataset

| Models | Accuracy | Precision | Recall | F-1 Score | Time-to-Run (s) |
|---|---|---|---|---|---|
| NB | 88.98 | 88.87 | 88.80 | 88.83 | Less than 5 |
| LR | 92.80 | 92.97 | 92.80 | 92.09 | Less than 5 |
| DT | 96.38 | 96.38 | 96.32 | 96.44 | Less than 5 |
| RF | 97.68 | 97.69 | 97.68 | 97.68 | 5.68 |
| XGB | 95.85 | 95.86 | 95.85 | 95.85 | 46.95 |
| ANN | 96.25 | 96.66 | 96.32 | 96.03 | 43.94 |
| CNN | 95.09 | 95.03 | 95.01 | 95.03 | 178.77 |
| LSTM | 96.48 | 96.32 | 96.44 | 96.46 | 127.56 |
| SVM | 93.08 | 92.77 | 93.55 | 92.79 | 88.76 |
| FL | 97.78 | 97.64 | 97.56 | 97.89 | 232.56 |
| SL | 98.02 | 98.12 | 98.02 | 98.11 | 222.33 |

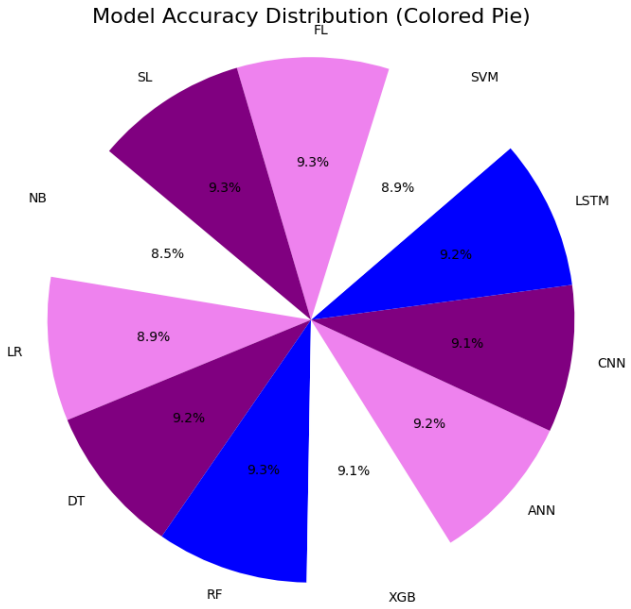
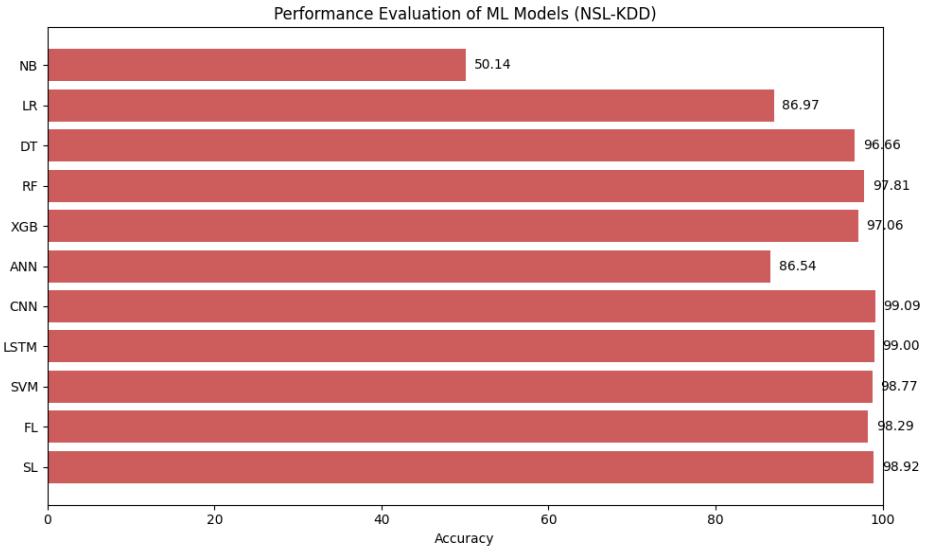



**Fig 2:** Performance evaluation of ML models on UNSW-NB15 dataset

The "time to run" values in Table 1 and Table 2 represent an average over multiple runs and indicate a commitment to capture the algorithm's consistency in terms of performance and stability. Encouraging multiple runs provides a more robust assessment, accounting for potential variations in execution times due to factors like dataset nuances or algorithmic randomness. This approach also enhances the reliability of the results and ensures that the time metrics reflect a representative measure of the algorithm's efficiency in real-world scenarios. This practice also aligns with best practices in machine learning research, fostering transparency and enabling a more nuanced understanding of the algorithm's computational behavior.



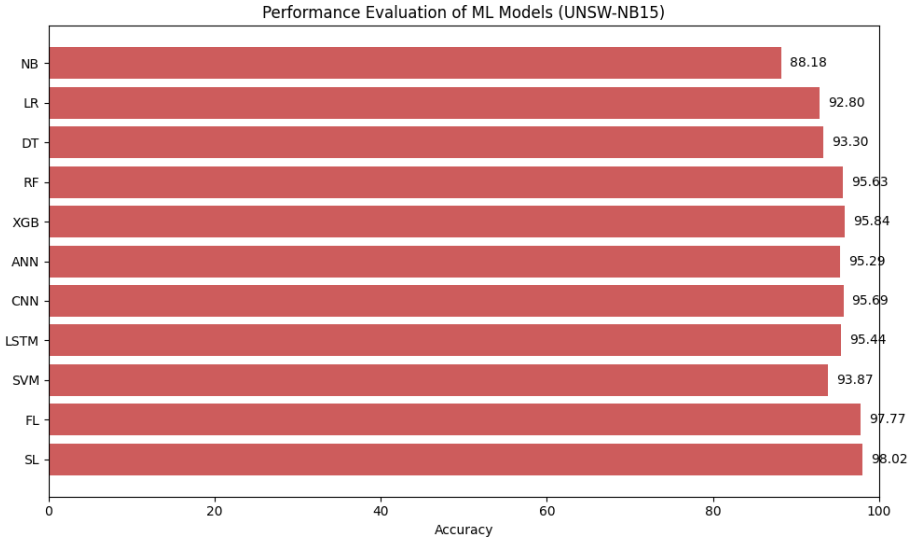



**Fig 3:** Performance evaluation of ML models for both the datasets.

Based on the evaluation metrics, it is observed that naive Bayes, logistic regression, and support vector machine exhibit the most unsatisfactory performance, while random forests, LSTM, federated learning, and split learning exhibit the best performance in terms of accuracy, precision, recall, and F-1 scores. The accuracy scores for random forest (RF), LSTM, federated learning, and split learning are 97.68, 96.48, 97.78, and 98.02, respectively. It is also observed that the training time for federated learning (232.56) is higher compared to split learning (222.33), which is higher compared to random forest (5.68) and LSTM (127.56). Regarding training time, RF performs the best, and in terms of accuracy, split learning performs the best. Figure 3 show the performance evaluation of both the datasets concerning accuracy using the Ml models and federated and split learning.

## 7. CONCLUSION

The increasing interconnectivity of devices in smart homes and smart cities has introduced significant cybersecurity challenges that demand robust, efficient, and real-time threat detection mechanisms. This study presents an optimized AI-driven framework that addresses these challenges by combining lightweight yet powerful hybrid AI models with advanced feature selection, edge computing, and federated learning techniques. By focusing on real-time data processing and low-latency inference, the proposed system effectively detects a wide range of cyberattacks, including novel and evolving threats, while operating within the resource constraints of diverse smart environments. The integration of online incremental learning enables continuous adaptation, ensuring the model remains relevant against emerging attack vectors without frequent retraining. Additionally, the incorporation of explainable AI components fosters transparency, enabling security professionals to interpret and trust the system's decisions. This holistic approach not only improves detection accuracy and efficiency but also enhances privacy, scalability, and practical deployability. The proposed optimized AI framework represents a significant advancement toward securing smart homes and smart cities against cyber threats. Its flexible design supports deployment across heterogeneous devices and infrastructures, promising a safer and more resilient future for increasingly connected urban and domestic spaces. Future work will focus on extensive real-world validation, integration with automated response systems, and expanding the framework to encompass broader aspects of smart environment security.

## REFERENCES

**[1]** Suryotrisongko, H., & Musaddiq, A. (2018). Evaluating machine learning algorithms for intrusion detection system. 2018 International Conference on Cybernetics and Intelligent Systems (ICORIS).

**[2]** Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

**[3]** Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

**[4]** Stiawan, D., Idris, M. Y. I. B., & Anuar, N. B. (2017). Cyber-attack penetration testing and system security assessment of smart home infrastructure. Computers & Electrical Engineering, 66, 58–75.

**[5]** Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. 2018 IEEE Security and Privacy Workshops (SPW), 29–35.

**[6]** Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118–137.

**[7]** Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.

**[8]** Yang, H., Zhao, L., & Su, J. (2019). A smart IDS for IoT-based smart homes. IEEE Access, 7, 83206–83217.

**[9]** Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.

**[10]** Amaral, A., et al. (2018). A hybrid artificial intelligence intrusion detection system for smart home environments. Sensors, 18(11), 3781.

**[11]** Sikder, A. K., Petracca, G., & Aksu, H. (2019). A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys & Tutorials, 21(2), 1309–1343.

**[12]** Chhetri, L. R., Rashid, A., & Vasilakos, A. V. (2019). Smart city security and privacy: A review. IEEE Internet of Things Journal, 6(5), 8856–8871.

**[13]** Moustafa, N., & Slay, J. (2016). UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference (MilCIS), 1–6.

**[14]** Mohammadi, M., Al-Fuqaha, A., Guizani, M., & Oh, J. (2018). Semi-supervised deep reinforcement learning in support of IoT and smart city services. IEEE Internet of Things Journal, 5(2), 624–635.

**[15]** Zhang, C., Wang, H., & Zhang, Y. (2018). A distributed intrusion detection system for smart cities using ensemble learning. Journal of Ambient Intelligence and Humanized Computing, 9, 459–468.

**[16]** Xie, J., Tang, B., Huang, T., Jin, X., Chen, L., & Kim, H. J. (2019). A survey of machine learning techniques applied to cybersecurity. Journal of Information Security and Applications, 46, 90–106.

**[17]** Cheng, Y., Chen, K., & Lai, Y. (2018). Intelligent intrusion detection system for smart home environment using CNN and RNN. Sensors, 18(7), 2536.

**[18]** Ferrag, M. A., Maglaras, L., Janicke, H., & Jiang, J. (2019). A survey on privacy-preserving schemes for smart grid communications. Computer Communications, 91, 17–33.

**[19]** Gendreau, A. A., & Moorman, M. (2016). Survey of intrusion detection systems towards an end to end secure Internet of Things. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 84–90.

**[20]** Franco, J., & Macedo, D. F. (2018). A real-time DDoS detection system based on machine learning for software-defined networks. International Journal of Network Management, 28(5), e2039.