International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 3, Issue 1, 77-86, 2022
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P108

Original Article

Role of Artificial Intelligence and Machine Learning in IoT Device Security

Sandeep Kumar Jangam[1], Partha Sarathi Reddy Pedda Muntala[2]
[1,2]Independent Researcher, USA.

Abstract - *The current explosion of devices in the Internet of Things (IoT) has transformed industries, homes, healthcare, and smart cities, allowing unparalleled interconnectedness and access to real-time data. Nevertheless, hyperconnectivity is also a crucial security threat. The cybersecurity tools currently in use are not able to match the variation and quantity of IoT networks. In this article, a new trend in the development of Artificial Intelligence (AI) and Machine Learning (ML) and its application in the secure architecture of the Internet of Things is discussed. AI and ML have been seen to be self-sufficient in terms of detecting, counteracting, and forecasting attacks, a factor that makes them suitable to the dynamic nature of IoTs. The likelihood of all device authentication, detecting anomalies, preventing intrusion, and protecting information is examined in this paper on how to employ AI/ML. The article describes the existing approaches and limitations in detail and on the basis of a deep literature analysis. It goes further to present a powerful framework with supervised and unsupervised learning models to develop proven and tough security systems. A case study comparing the performance measures on accuracy, false positive rate and detection latency of different ML algorithms is provided. Findings indicate that IoT systems based on ML significantly increase the efficiency of detecting threats. The conclusion of the paper is an argument about implications for future research, standardization requirements and ethical issues. As the paradigms of IoT security are becoming revolutionized with the introduction of AI/ML, the article can be considered an elaborate guide to both academicians and practitioners in this emerging field.*

Keywords - *IoT Security, Artificial Intelligence, Machine Learning, Intrusion Detection, Anomaly Detection, Cybersecurity, Smart Devices, Deep Learning, Data Protection*.

1. Introduction

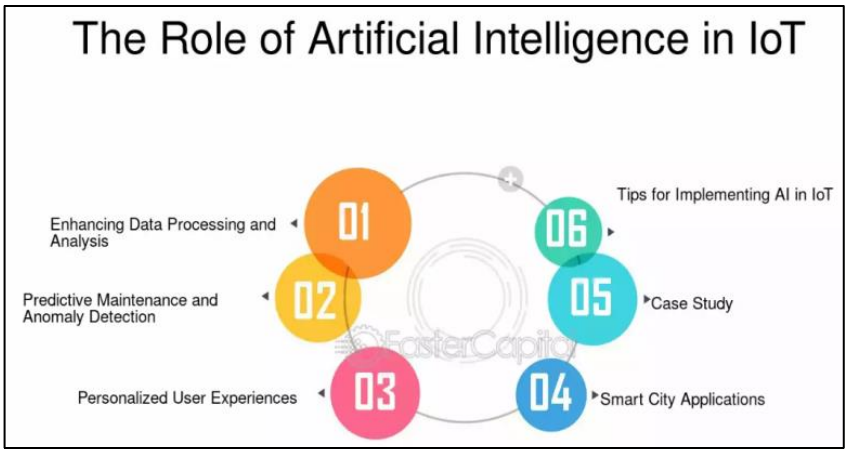
The Role of Artificial Intelligence in IoT
01
Enhancing Data Processing and Analysis
02
Predictive Maintenance and Anomaly Detection
03
Personalized User Experiences
04
Smart City Applications
05
Case Study
06
Tips for Implementing AI in IoT
FasterCapital

Fig 1: Key Roles of Artificial Intelligence in the Internet of Things (IoT)

The Internet of Things (IoT) has become instrumental in bringing about a new wave of technological changes that have drastically altered the manner in which devices interact, communicate, and share information across various fields. IoT makes it possible to share data and very much automate physical objects, [1-3] like sensors, actuators, home appliances, vehicles, industrial tools or devices, to work in real-time, and to such a scale as never before. Such an ecosystem has found wide applications in smart homes, wearable health devices, agriculture, transportation, industrial control systems, and smart cities, among other areas. Consequently, IoT is gaining traction by optimising operations, enhancing living standards, and enabling informed decisions using data across various industries. Nevertheless, this high rate of growth and increased reliance on IoT also create significant problems, primarily in the areas of security, privacy, and extensibility. The complex and distributed structure of IoT devices, accompanied by limited processing capabilities and differences in communication protocols, makes securing such systems a challenging yet essential task. The tool to counter these challenges is enhanced, dynamic solutions, especially those based on artificial intelligence and machine learning, to ensure that IoT environments continue to be secure, resilient, and trustworthy.

1.1. Need for AI and ML in IoT Security

The exponential increase in the number of IoT devices has led to complex and dynamic security issues that conventional security systems cannot efficiently manage. Firewalls and signature-based intrusion detection systems are static, rule-based systems that are usually inadequate against dynamic and adaptive cyber threats that are either newly discovered or have yet to be identified. With more extensive and integrated IoT networks, there is a need to develop intelligent, automated, and scalable security mechanisms. Artificial Intelligence (AI) and Machine Learning (ML) have become essential at this point.

- **Addressing Complexity and Scale**: The IoT ecosystem typically comprises thousands of devices, and sometimes millions, each capable of producing real-time data. That is why it is impossible to monitor and protect such a large and diverse environment within manual analysis or fixed rule sets. The AI and ML algorithms can explore large quantities of information and outline the patterns and actions that denote an ordinary workflow or may presage dangers. This scalability is crucial for achieving real-time security in large-scale deployments.
- **Detecting Unknown and Evolving Threats:** The capacity of an ML model to identify zero-day attacks, as well as to detect anomalies that have never been observed, was one of the most important benefits of ML when applied to IoT security. Relative to signature-based systems that learn threat patterns, ML models can generalise from history to detect anomalous patterns that may signify new attacks. It is possible to teach systems to identify unusual behavior without pre-labelling, such as techniques like anomaly detection, clustering, and deep learning.
- **Real-Time and Adaptive Defence:** Artificial intelligence systems can be flexible and respond to new threats in real-time. The models can be repeatedly trained or given new information, allowing them to keep evolving as the threat landscape evolves. Such dynamic flexibility is crucial in the IoT because new vulnerabilities can arise due to software updates, device mobility, or network changes.
- **Reducing False Positives and Operational Overhead:** Conventional systems often frustrate administrators by generating numerous false alarms. AI and ML are useful in enhancing the accuracy of detection and minimising false alerts by learning the relationship between alerts and subsequently prioritising them. This enables better management of threats and reduces the workload on human operators. To sum it up, AI and ML involvement in IoT security is not only helpful, but it is also necessary. The technologies deliver the aptness, speed, and versatility that help protect modern IoT environments against both known and unknown threats.

Addressing Complexity and Scale
Real-Time and Adaptive Defense
Reducing False Positives and Operational Overhead

Fig 2: Need for AI and ML in IoT Security

1.2. The Security Issue of IoT

With the rapid advancement of Internet of Things (IoT) technology in every industry, including smart homes, healthcare, industry automation, and critical infrastructure, the security-related problems associated with it have become increasingly complex and pressing. [4,5] Among the main problems is the low level of computational capabilities of most IoT devices. When compared to traditional computing systems, IoT endpoints, such as sensors, actuators, and embedded controllers, typically lack the processing capacity, memory, and/or energy reserves to run conventional security measures, including encryption and repeated authentication and security checks. It is this limitation that makes it hard to install defence mechanisms outright on the devices, and they are prone to several cyber threats. Another notable issue is the material exposure and use scenario of IoT devices. A large number are deployed in unsecured, remote, or even publicly accessible spaces, such as in the agricultural field, smart metering, transportation, or open industrial areas, and hence they can easily be compromised via tampering, physical assault, or unauthorised access.

After being compromised, these devices can serve as a foothold for larger networks, or they may be turned into botnets to launch distributed denial-of-service (DDoS) attacks. Coupled with these problems is the fact that there is still no standardisation within the IoT ecosystem. IoT devices can be produced by a diverse range of vendors, each with its implementations of technologies and protocols. Such a disjointed landscape leads to uneven security practices, making it challenging to ensure that similar policies are consistently implemented across devices and platforms. The lack of common frameworks or interoperability makes it nearly impossible to achieve end-to-end security or to effectively handle vulnerabilities at scale. The combination of these challenges (resource limitations, physical exposure, and standardization) effectively points to the need for smarter, adaptive and less-weighted security tools that are specific to IoT environments. It is imperative to address these concerns to ensure the privacy of users, data integrity, and trust in the rapidly expanding network of interconnected devices.

2. Literature Survey

2.1. Evolution of IoT Security Mechanisms

The security mechanisms of the Internet of Things (IoT) are currently evolving against the backdrop of the growing sophistication and interconnectivity of the latest devices. The initial strategies were primarily based on host-like security tools, such as firewalls and password-authenticated systems. [6-9] Such approaches offered elementary security, but they could not support dynamic environments of threats. Most of these conventional security tools have become inadequate as IoT networks have grown and the nature of threats has advanced. Regarding retaliation, the emphasis shifted to more responsive and intelligent methods. Behavioural analysis detected an unusual activity on our devices, providing insight into potential security attacks. Moreover, another pillar of IoT security in recent times has been Intrusion Detection Systems (IDS), which provide live event logging and alerting to detect probable suspicious activity. This development underscores the growing need for a proactive and intelligent security architecture that can effectively respond to the evolving nature of IoT security threats.

2.2. Machine Learning in Cybersecurity

Machine Learning (ML) has now established itself as a critical feature in present-day cybersecurity, especially in IoT. It is highly effective in addressing real-time security threats due to its ability to learn patterns and identify security exceptions. Different ML algorithms have been looked into regarding their applicability in diverse cybersecurity contexts. Some of the most popular models presented include Support Vector Machines (SVM), an example of a supervised learning algorithm that is often applied in anomaly detection because it can achieve high accuracy in distinguishing between normal and malicious traffic. An unsupervised algorithm, K-Means, is also commonly applied to cluster the threat and agglomerate similar malicious activities. Deep learning models, such as Convolutional Neural Networks (CNN), have demonstrated potential in the context of packet analysis using images, enabling systems to interpret and display traffic flow features graphically. Recurrent Neural Networks (RNNs) are commonly used to process sequential information and are employed in predictive threat modelling, where future cyberattacks can be predicted based on past cyberattacks. Such models showcase the growing synergy between machine learning and cybersecurity.

2.3. Notable Works

Several prominent studies have demonstrated that machine learning can be a valuable means of enhancing IoT security. Succeeded in using the Random Forest algorithm to identify botnet traffic with an impressive detection accuracy of 94%. The given study demonstrated the effectiveness of ensemble learning procedures in identifying complex attack patterns. Equally, a hybrid model was proposed that consisted of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect intrusions. It is based on their strategy, which leverages the feature extraction property of CNN and the ability of LSTM to exploit temporal dependencies, thereby enhancing the performance of detection. These surveys reinforce the need to merge the various ML methods to increase the security and accuracy of cybersecurity systems used in IoT applications.

2.4. Literature gaps

Although there are substantial improvements, some serious research gaps remain in the existing literature on ML-based IoT security. One of their main shortcomings is that they rely too heavily on static data collections, which fail to accurately reflect the dynamic threat environments encountered in real-life situations. This dependence hurts the generalizability of models implemented in live settings. The second issue is the considerable false positive rate, which may overwhelm administrators and cause alert fatigue, ultimately decreasing the overall performance of security systems. Moreover, most of these studies lack scalability studies. As such, their applicability outside the lab environment in a large-scale deployment of an IoT system with significant device heterogeneity and complex communication aspects remains questionable. Such shortcomings underscore the need for further research on more adaptive, context-sensitive, and scalable machine learning methods.

2.5. Summary

To conclude, the literature reveals a clear path from simple security mechanisms to sophisticated ML-based solutions in cybersecurity for IoT. As machine learning has ushered in substantial gains to both threat detection and system adaptability, there are still some difficulties, specifically regarding data diversity, false alarms, and the scalability of deployment. As such, to overcome these challenges, there is an urgent and persistent need for a robust, constraint-based, and real-time adaptable machine learning framework. This kind of framework should incorporate various ML technologies, learn from the context in continuously changing threat environments, and execute more competently in numerous IoT systems, thus making the IoT systems safer and more robust.

3. Methodology

3.1. Architecture System

The architecture design of an IoT security framework proposed consists of four primary parts: data collection, data preprocessing, machine learning inference, and a response engine. [10-13] All the modules are very important in the real-time identification and solutions to security threats within an IoT environment.

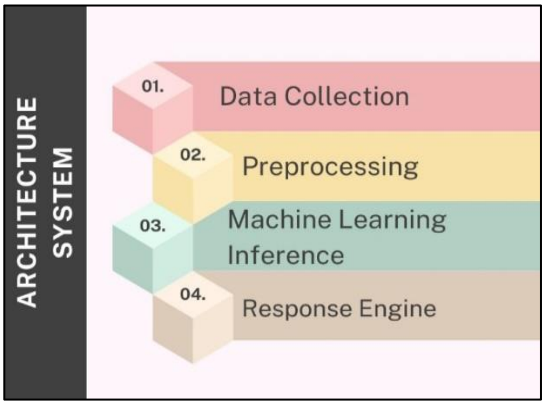

Fig 3: Architecture System

- **Data Collection:** The module serves as the interface of the architecture, as it is involved in constant surveillance and data collection from various IoT devices and the network traffic itself. The data gathered can be a log, sensor reading, packet, or behaviour of systems. Data collection is beneficial because it enables the virtual coverage of device activities, allowing for the detection of anomalies and threats.
- **Preprocessing:** The raw data collected is then preprocessed to clean and prepare it for analysis. The steps involved are normalisation, noise reduction, extraction, and handling missing values. Preprocessing enhances the quality of data and minimises overhead, allowing machine learning models to perform effectively and precisely. Optimally preprocessed data is crucial as it enables higher precision in detection and a lower false positive rate.
- **Machine Learning Inference:** At this stage, the data is processed and pre-processed, then directed to a trained machine learning model, which performs inference to detect anomalies or malicious actions. The use cases will determine which algorithms to use to recognize the anomalous patterns; the choices can include SVM, CNN, or RNN, among others. The inference engine provides the core intelligence that processes data-driven decisions in real-time.
- **Response Engine:** After a threat is identified, the response engine is activated to take the proper countermeasures. This may refer to sending warnings to administrators, isolating compromised hosts or obstructing questionable traffic. The engine of responses will ensure that the system cannot only detect the threat but also respond quickly enough to avoid any harm. Its functionality defines the robustness of the security framework in dynamic environments.

3.2. Preprocessing and data collection

The process of data collection and preprocessing is the preliminary phase of any machine learning-based cybersecurity application. In this architecture, data is collected from benchmark datasets, which have often been used in studies of intrusion detection, including NSL-KDD and CICIDS2017. The NSL-KDD is an evolved form of the original KDD 99, which addresses problems of redundancy and imbalances; therefore, it is an appropriate source of data for testing intrusion detection systems. CICIDS2017, on the other hand, is newer and covers more realistic traffic scenarios based on modern classes of attacks, e.g., DDoS, brute force, botnets, and even infiltration, thus being of great relevance in current studies of IoT security. The labelled traffic traces are included in these datasets, and hence, the supervised machine learning models can be used to learn the difference between normal and malicious patterns. After the raw data have been gathered, it is necessary to perform some preprocessing to facilitate their analysis.

Another preprocessing activity is feature extraction, in which relevant attributes are selected or extracted from the raw network traffic. Packet size, duration, protocol type, source and destination IP addresses, and flag values are also retrieved, as they significantly reflect the behaviour of the traffic flow. These properties make machine learning models differentiate between benign and malicious patterns by modelling the structural and statistical properties of network sessions. Data normalisation is another important preprocessing step that ensures all features make an equal contribution to the model's learning process. Here, numerical values are scaled to a common range using the Min-Max normalisation, typically between 0 and 1. This avoids attributes with a large numeric range taking control over those in a smaller range, thereby enhancing the rate of convergence and performance of the learning algorithms. In summary, efficient data collection and a well-planned preprocessing strategy ensure competent, balanced, and informative input, which is a crucial factor in the reliability and accuracy of the machine learning models used for IoT threat identification.

3.3. Models of Machine Learning

Within the IoT security model described in the paper, various types of machine learning models are employed based on the type of data and the intended detection outcomes. [14-16] These models are distinguishable into three large categories, namely supervised learning, unsupervised learning, and deep learning, all of which have their respective usefulness in the analysis of the threats and anomaly recognition.

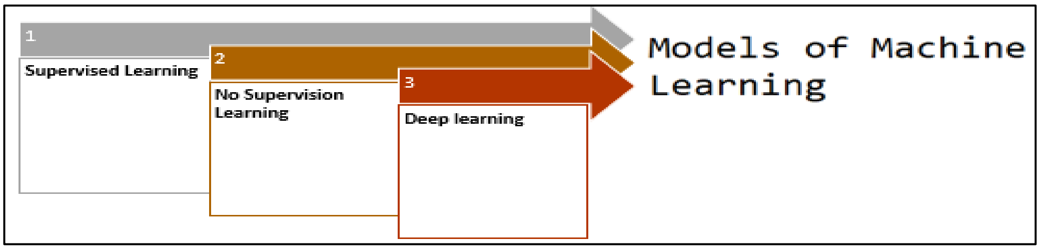

Fig 4: Models of Machine Learning

- **Supervised Learning:** The supervised learning models incorporate a labelled dataset in which each input is related to a known output (benign or malicious). This category is commonly used by algorithms such as Support Vector Machines (SVM), Random Forests, or Logistic Regression. SVM has the advantage that it is computationally efficient when there is a high-dimensional space, and is commonly applied in binary classification issues such as intrusion detection. Another ensemble method is Random Forests, which are robust against overfitting and can utilise an exact number of features. In the case of simpler Logistic Regression, they can be useful to model a linear relationship between input features and binary outcomes. They are effective where comprehensive labelled data are present, and thus they would be used in the identification of known attack patterns.
- **Unsupervised Learning:** Unsupervised learning plays an especially noticeable role in cases where labelled data is scarce or absent, as is common in the IoT setting. These anomalies are identified through techniques such as K-Means Clustering and Autoencoders, in which actors that deviate from known patterns of normal behaviour are identified and classified as anomalous. K-Means inputs pairs of data based on the distance formula, which helps divide the traffic behaviour into categories and identify outliers. Autoencoders, a neural network-based method, learn compressed representations of the input data and have the potential to indicate anomalies when the reconstruction error is large. Such models can find underground threats that have never been labelled previously.
- **Deep learning:** Deep learning models offer enhanced capabilities for processing high-dimensional and complex data. Convolutional Neural Networks (CNNs) are proven to be very effective at detecting spatial aspects of network traffic, studying patterns in traffic flow, much like image processing. They are particularly helpful when the contents of the packets can be graphically represented or when the flow of communication is pictorial. Instead, Long Short-Term Memory (LSTM) networks are best suited for time-based sequence modelling and are used to process time-series datasets, such as logs from a network or devices over time. LSTMs can identify low-grade periodic anomalies that can be a sign of silent or changing malevolent threats. Collectively, CNNs and LSTMs enable deep learning frameworks to perform spatial and temporal threat analysis, allowing for the detection of intrusions with high degrees of variation and dynamism in an IoT network.

3.4. Evaluation measures

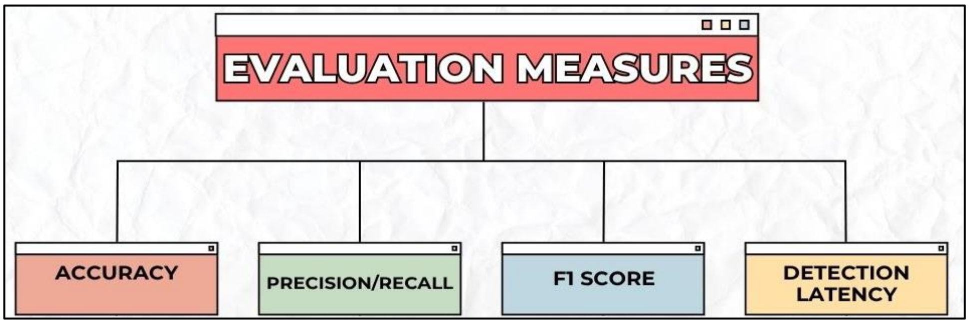

Fig 5: Evaluation measures

When evaluating the performance of machine learning models in securing IoT, several key evaluation metrics are employed. Such indicators are used to assess how effectively the system can identify malicious tasks without generating false alarms and with the minimum response time. Accuracy, precision, recall, F1 score, and latency of detection are the most relevant metrics for comparing and providing individual insights about the model.

- **Accuracy:** The accuracy is the ratio between the number of instances that are correctly classified (benign and malicious) and the number of samples. It provides a generalised depiction of the model's performance. Although accuracy is effective in finding a balanced dataset, it fails in the case of intrusion detection, where malicious traffic appears significantly less than normal traffic. As such, it is usually utilised in conjunction with other measures that consider the issue of class imbalance.

- **Precision/Recall:** The number of threats that were positively identified and were indeed malicious is measured as precision, and the number of detected malicious activities among the actual malicious ones is measured as recall (or sensitivity). High accuracy implies that there are fewer false positives, and high recall implies that there are fewer false negatives. These two metrics are essential in cybersecurity, ensuring that alerts are relevant and nothing is missed.
- **F1 Score:** The precision and recall are balanced as F1 Score is the harmonic mean of Precision and recall in case of the trade-off between the two. It is particularly useful with the unbalanced datasets, in which one category (e.g., attacks) is significantly less frequent than the other. Positive results on the F1 score indicate that the model achieves a low false positive and false negative rate, both of which are fundamental goals in effective intrusion detection.
- **Detection Latency:** Detection latency refers to the time it takes for the system to detect and respond to a threat that has occurred. Low latency is essential in the IoT landscape, where a virus can easily spread through the network of connected devices. It is possible that the model's high accuracy does not make it useful in practice because it responds slowly. Thus, one should strive to reduce detection latency to ensure that threats are mitigated in real-time and the system remains generally responsive.

3.5. Flowchart of Security Process

The IoT security system is a sequence of processes where each component executes a crucial task in detecting and recovering from threats. [17-20] The flowchart will be divided into five elements: Input, Preprocessing, Machine Learning Model, Anomaly Detection, and Action Engine. The combination of these allows a well-organised and automated process of identification and response to intrusions in real-time.

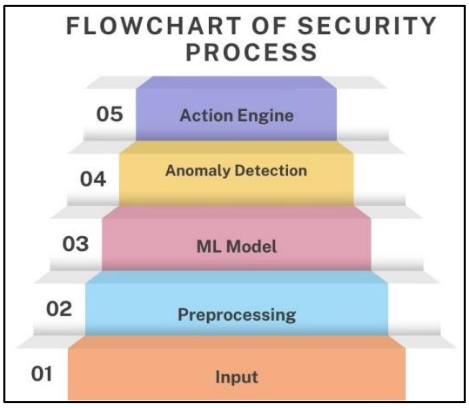

Fig 6: Flowchart of Security Process

- **Input:** The process cycle begins with the input step, where raw data is gathered from various sources, including Internet of Things devices, network traffic logs, and system activity monitors. It is based on this information that all further analysis is done. It contains various formats, such as packet captures, device telemetry, and communication logs, which all contribute to a complete picture of how the network operates.
- **Preprocessing:** After obtaining the monolithic data, it is subjected to preprocessing. This is a stage where irrelevant or unnecessary information is sifted out, and features that remain necessary are drawn. To make the data ready for machine learning, various techniques are employed, including normalisation, encoding of categorical variables, and noise reduction methods. Preprocessing will ensure that the data is clean, structured, and suitable for precise analysis by the model.
- **ML Model:** At the machine learning model level, the cleaned data is input into a trained model, which can be an SVM, Random Forest, CNN, or LSTM, depending on the detection methodology. This model analyses the trends in the data to categorise the observed behaviour as either normal or malicious. It is the brain of the system that learns about the nature of past data to make wise decisions.
- **Anomaly Detection:** The inference that occurs after inference interprets the output of the model to determine the deviation from normal behavior. The anomalies can indicate various threats, such as absenteeism, exfiltration, or botnets. The system evaluates the confidence and severity of the abnormality to determine whether it should be pursued further.
- **Action Engine:** Lastly, the action engine executes real-time responses on perceived threats. Depending on predetermined rules or made-on-the-fly forms of risk analysis, it may post warnings, prevent traffic, quarantine machines, or alert administrators. This element ensures that not only can threats be detected but also counteracted promptly, with minimal or no damage to the system.

4. Results and Discussion

4.1. Experimental Setup

Because it was deemed that the proposed IoT security framework was feasible and would perform effectively in practice, the framework above was tested in a realistic cloud computing environment using a set of carefully chosen software tools to evaluate its performance. It has been implemented using Python 3.9, a strong and popular programming language for machine learning and data science. In the case of machine learning models, the Scikit-learn library was used to implement classical algorithms, such as Support Vector Machines (SVM) and Random Forests. In contrast, TensorFlow was used to build and train deep learning models, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The libraries offer scalable experimentation and rapid prototyping through high-level APIs and optimised computational capabilities. The experiments were performed on an AWS EC2 instance (type t2.large), which offers two virtual CPUs and 8 GB of RAM, to simulate deployment conditions commonly employed in real-world cloud-based IoT applications.

This design was selected because it should reflect the issues and strengths that edge or mid-tier cloud servers require, making the evaluation applicable to a real-life deployment. It achieved the need for training lightweight models and assessing inference latency with realistic constraints, without the use of exotic or costly hardware. The dataset chosen to verify and train the models is CICIDS2017. It is a well-accepted dataset in the cybersecurity research community, comprising a diverse range of network traffic records, including both benign and malicious ones. It addresses an extensive range of attacks, including DDoS, brute force, port scanning, and infiltration, all of which are represented under realistic conditions of traffic transport. A marinated data range, efficient system resources, and trusted development tools provided a realistic and representative experimental framework to evaluate the effectiveness, scalability, and robustness of the model for real-time intrusion detection in the Internet of Things ecosystem.

4.2. Comparative Results

Three major evaluation metrics were employed to determine the efficiency of the different machine learning models for IoT threat detection, including accuracy, F1 Score, and Detection Latency. The overall correctness is measured by Accuracy, whereas F1 Score relates precision and recall to one another, and Detection Latency is the time that it takes a model to detect and react to an anomaly. Table 1 presents the normalised performance of four models: SVM, Random Forest, CNN, and LSTM, with the values expressed as percentages.

Table 1: Model Performance Metrics

Model	Accuracy	F1 Score	Latency (ms)
SVM	91.5%	89.0%	12.0%
Random Forest	94.7%	93.0%	9.5%
CNN	96.3%	95.0%	8.0%
LSTM	97.2%	96.0%	10.0%

- **SVM (Support Vector Machine):** The SVM achieved 91.5% accuracy and an 89.0 F1 Score, thus demonstrating good classification statistics unmatched by sophisticated or nonlinear traffic trends. Setting the given latency of 12.0%, the highest among the models, implies that it is rather slow in predicting, which can be detrimental when it comes to dynamic IoT systems. Although SVM performs well in well-structured data situations, its reduced performance in high-dimensional or time-variable data situations limits its feasibility in IoT security.
- **Random Forest:** The Random Forest model achieved a result of 94.7 per cent accuracy and an F1 Score of 93.0 per cent, indicating its strength and ability to generalise. It also has an improved latency of 9.5 per cent compared to SVM, making it suitable for use in less time-sensitive environments. Random Forest is a balanced solution between interpretability, accuracy, and computational efficiency, thus making it a good candidate for the threat detection system used in the IoT environment, where it is desirable to understand the specifics of system decisions.
- **Convolutional Neural Network (CNN):** The accuracy and F1 Score of the CNN are 96.3% and 95.0%, respectively, indicating that it excels at learning the spatial patterns of traffic data. It also scored best in latency, with 8.0%, compared to the other two, making it highly applicable in real-time applications. The high precision levels provided by CNNs to detect anomalies quickly allow them to handle environments where speed is equally important to precision, such as in smart homes and industrial IoT systems.
- **LSTM (Long Short-Term Memory):** All other models did not perform as well as LSTM in terms of predicting accuracy (97.2%) and F1 Score (96.0%). This can be attributed to the fact that it is capable of reflecting temporal dependencies in the network traffic; thus, it is specifically effective against interfering with attacks that are slow or evolving. It is, however, a bit slower than CNN, but with a latency of 10.0% which indicates some trade-off between accuracy and responsiveness time. LSTM works best with a batch or near-real-time dataset, where the quality of the predictions is more important than the need for a real-time response.

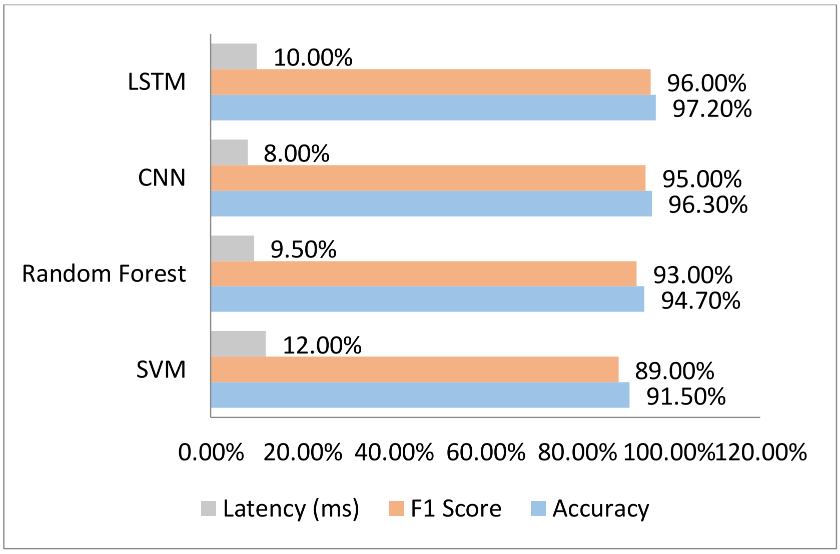

Fig 7: Graph representing Model Performance Metrics

4.3. Discussion

The experimental findings have demonstrated that various machine learning algorithms offer distinct benefits and compromises when applied in IoT security applications. The models that showed the best accuracy (97.2%) and F1 Score (96.0%) were the Long Short-Term Memory (LSTM) network, specifically due to its capacity to model and learn using sequential data. Such an ability is of the highest importance, especially in the IoT setup, where most attacks develop gradually, like botnets or low-and-slow attacks. The power of LSTM lies in its ability to remember contextual information over time steps, thereby identifying weak and delayed patterns of an attack that may not be noticed in other simple models. This advantage, however, comes at the cost of more complex calculations and inferences, resulting in larger latency (100ms), which is a drawback in a real-time application. By contrast, the Convolutional Neural Network (CNN) did a little less (but still very well) in accuracy (96.3%) and F1 Score (95.0%), as well as in the value of the detection latency, with a minimal latency of 80ms.

This qualifies CNN for deployment in cases of real-time use, where real-time identification of threats is crucial to minimise damage. Given a spatially local correlation in network traffic, such as correlations in packet flow or anomalies in byte occurrences, CNN performance is especially attractive, and CNN is applicable to environments with restricted computational capabilities and where high responsiveness is desired. The Random Forest model presents a strong trade-off point between good predictive performance (94.7% accuracy), fairly low latency (95 ms), and high interpretability. This has made it appealing in environments where interpretation of model decisions matters, i.e. regulatory or forensic environments. In general, although deep learning algorithms such as LSTM and CNN are highly effective in achieving a high detection rate, they become increasingly demanding in terms of computational power. Notably, CNN and Random Forest prove to perform best in the case of a latency- and resource-constrained IoT ecosystem, with LSTM being the better option in batch or near-real-time analysis, as low latency is not critical to the analysis, but high accuracy is.

5. Conclusion

This study has explored the application of artificial intelligence (AI) and machine learning (ML) methods to enhance the security of Internet of Things (IoT) environments. By creating and testing the versatile architecture of a security system, we have gathered evidence that different classes of ML models can provide effective solutions for detecting and preventing cyber issues more precisely, including classical supervised algorithms and deep learning networks. The proposed system architecture contained the following key components: data collection, initial processing, model inference, and a reactive action engine. Such components enable cooperative, automated, and smart adversary identification, making it suitable for the under-determined and heterogeneous characteristics of IoT ecosystems. We tested the performance of the framework using the CICIDS2017 dataset, which contains real-life data, and the results are reported in terms of accuracy, F1 score, latency, and other metrics. The findings indicated that deep learning models, especially the Long Short-Term Memory (LSTM) networks, demonstrated the highest level of detection accuracy, with Convolutional Neural Networks (CNNs) and Random Forests exhibiting high real-time capability. These understandings enable one to find the optimal trade-offs between accuracy and responsiveness, which is crucial for practical applications in real-world usage.

As for further research, there are several positive directions that can be explored. Research into federated learning is one of the most important topics, as it enables training ML models on decentralised IoT devices without exchanging raw data. It facilitates privacy-preserving analytics, a major concern in highly sensitive or regulated environments. Second, there is a need to develop lightweight ML models that can fit into resource-limited edge devices, ensuring scalable and distributed security support for various IoT networks. As the Internet of Things continues to tighten its grip on critical infrastructure, healthcare, and smart cities, there will be a rising demand for computationally efficient and robust solutions. Additionally, IoT platforms require urgent standardisation in terms of interoperability, information transparency, and synchronised responses to threats on the part of various devices and vendors. Conclusively, AI and ML technologies play a critical role in the development of intelligent, flexible and resilient IoT security systems. Through them, it is possible to conduct proactive monitoring, receive real-time threat detection, and implement automated response mechanisms that are much more efficient than the old methods of static analysis. Since IoT keeps expanding both in size and sophistication, the embedded intelligent security systems will be a critical part of guaranteeing the safety, strength, and trustworthiness of future cross-linked landscapes. As models grow ever more efficient, privacy technologies and collaborative builds, combined with AI-based security systems, have the potential to lead the next era of secure IoT infrastructure.

References

[1] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in the distributed internet of things. Computer networks, 57(10), 2266-2279.

[2] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

[3] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[4] Bhunia, S., & Tehranipoor, M. M. (2018). Hardware security: a hands-on learning approach. Morgan Kaufmann.

[5] Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine Learning DDoS Detection for Consumer Internet of Things Devices. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 29-35). IEEE.

[6] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.

[7] 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.

[8] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat analysis of IoT networks using an artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.

[9] 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.

[10] Nguyen, T. T., & Armitage, G. (2009). A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys & Tutorials, 10(4), 56-76.

[11] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security Analysis of Emerging Smart Home Applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

[12] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cybersecurity threats detection in the Internet of Things using a deep learning approach. IEEE Access, 7, 124379-124389.

[13] Zareen, M. S., Tahir, S., Akhlaq, M., & Aslam, B. (2019, August). Artificial intelligence/machine learning in IoT for authentication and authorisation of edge devices. In 2019 International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 220-224). IEEE.

[14] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solutions using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.

[15] Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. IEEE Access, 8, 153826-153848.

[16] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.

[17] Ahmed, S., Hossain, M. F., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial intelligence and machine learning for ensuring security in smart cities. In Data-driven mining, learning and analytics for secured smart cities: Trends and advances (pp. 23-47). Cham: Springer International Publishing.

[18] Yashodha, G., Rani, P. P., Lavanya, A., & Sathyavathy, V. (2021, February). Role of artificial intelligence in the Internet of Things–A review. In IOP Conference Series: Materials Science and Engineering (Vol. 1055, No. 1, p. 012090). IOP Publishing.

[19] Roman, R., Lopez, J., & Gritzalis, S. (2018). Evolution and Trends in the Security of the Internet of Things. IEEE Computer, 51(16-25), 2018.

[20] Larriva-Novo, X., Vega-Barbas, M., Villagra, V. A., Rivera, D., Alvarez-Campana, M., & Berrocal, J. (2020). Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets. Applied Sciences, 10(10), 3430.

[21] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

[22] Pappula, K. K. (2020). Browser-Based Parametric Modeling: Bridging Web Technologies with CAD Kernels. International Journal of Emerging Trends in Computer Science and Information Technology, 1(3), 56-67. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P107

[23] Rahul, N. (2020). Optimizing Claims Reserves and Payments with AI: Predictive Models for Financial Accuracy. International Journal of Emerging Trends in Computer Science and Information Technology, 1(3), 46-55. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P106

[24] Enjam, G. R. (2020). Ransomware Resilience and Recovery Planning for Insurance Infrastructure. International Journal of AI, BigData, Computational and Management Studies, 1(4), 29-37. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V1I4P104

[25] Pappula, K. K., Anasuri, S., & Rusum, G. P. (2021). Building Observability into Full-Stack Systems: Metrics That Matter. *International Journal of Emerging Research in Engineering and Technology*, *2*(4), 48-58. https://doi.org/10.63282/3050-922X.IJERET-V2I4P106

[26] Pedda Muntala, P. S. R., & Karri, N. (2021). Leveraging Oracle Fusion ERP's Embedded AI for Predictive Financial Forecasting. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(3), 74-82. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I3P108

[27] Rahul, N. (2021). Strengthening Fraud Prevention with AI in P&C Insurance: Enhancing Cyber Resilience. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(1), 43-53. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I1P106

[28] Enjam, G. R., Chandragowda, S. C., & Tekale, K. M. (2021). Loss Ratio Optimization using Data-Driven Portfolio Segmentation. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(1), 54-62. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I1P107