

Autonomous Security Validation For Embedded Trust Chains In Connected Devices

Jay Bharat Mehta

Independent Researcher.

Abstract

The rapid expansion of Internet of Things (IoT) technologies has enabled large-scale connectivity among smart devices across domains such as smart homes, industrial automation, healthcare systems, and intelligent monitoring infrastructures. However, the growing number of interconnected devices also introduces significant security challenges due to heterogeneous architectures, limited computational capabilities, and increasing exposure to cyber threats. Malicious activities targeting IoT devices can disrupt communication processes, compromise embedded trust relationships, and threaten the reliability of connected systems. Therefore, effective security validation mechanisms are required to monitor device communication behavior and detect potential compromises within IoT networks. This study proposes an autonomous security validation framework designed to analyze network communication traffic generated by heterogeneous IoT devices and identify malicious activities affecting embedded trust chains. The proposed approach utilizes a data-driven experimental methodology combined with supervised machine learning techniques to learn behavioral patterns associated with both legitimate device communication and multiple cyberattack categories. The framework analyzes communication records generated by several IoT devices and performs multi-class attack classification to detect threats such as backdoor attacks, distributed denial-of-service attacks, injection attacks, password exploitation attempts, ransomware activities, scanning operations, and cross-site scripting attacks. Experimental evaluation demonstrates that the proposed model achieves strong classification performance with high accuracy, precision, recall, and F1-score, indicating reliable detection of malicious device behavior. The results highlight the effectiveness of behavioral traffic analysis and machine learning techniques for strengthening trust validation and improving security monitoring in connected IoT environments.

Keywords: Internet of Things, IoT Security, Trust Validation, Intrusion Detection, Machine Learning.

1. Introduction

The accelerated growth of the Internet of Things (IoT) has greatly changed contemporary online infrastructures in that connected devices can communicate and share information within various applications in diverse realms like smart homes, healthcare systems, industrial automation, and smart transportation. With the help of IoT, devices keep communicating with cloud services, edge infrastructures, and other existing interconnected networks to execute automated functions and establish real-time visibility options (Ammar et al., 2018; Conti et al., 2018). Irrespective of these benefits, the growing array of interconnected devices poses significant security challenges because of the heterogeneous architectures, the small amount of computing resources, and the extensive attack surfaces found in the IoT settings (Rose et al., 2015; Al-Fuqaha et al., 2015).

The security vulnerability of the IoT systems has turned out to be a critical issue because most of the devices are in open networks without effective protection systems. IoT devices with limited resources are not always able to run the conventional security models which makes them susceptible to cyber attacks such as unauthorised access, malware, distributed denial of service (DDoS) attacks, and manipulation of data. These threats are able to interfere with the work of devices and undermine the integrity of complete IoT systems (Sicari et al., 2015; Alaba et al., 2017). Besides, the penetration of IoT technologies in industrial and critical infrastructures also increases the likelihood of security breach, which underscores the necessity of credible security controls, which could safeguard interconnected systems (Boyes et al., 2018).

Another essential issue in IoT environments is trust management where a group of interconnected devices coordinates and share information over distributed networks. IoT systems are based on

embedded trust relationships where secure communication between devices and services is ensured. However, malicious activities are able to propagate through the network by interfering with these trust chains by compromised devices. Thus, to ensure safe IoT functioning, constant device activity control and authentication of the integrity of communication is required (Mosenia and Jha, 2016; Lu and Xu, 2018). Some of the works have highlighted that proper security systems should include behavioural analysis and trust verification modules to identify compromised devices and secure the IoT communication infrastructures (Sfar et al., 2018).

Most recent works have discussed machine learning and data-intensive methods to enhance intrusion detection and security surveillance in the IoT network. Machine learning algorithms can be used to analyse traffic patterns on the network and detect abnormalities that can be signs of malicious actions. The prior research proves that the traffic profiling along with the machine learning algorithms can be effective at identifying the abnormal ion of communication as produced by the compromised IoT devices (Doshi et al., 2018; Muna et al., 2018). Moreover, the deep learning models have been used to detect malware and sophisticated attack patterns in the IoT communication networks (HaddadPajouh et al., 2018).

Besides the intrusion detection mechanisms, other security frameworks have been established to enhance authentication, access control, and secure communication between the IoT devices (Amanullah et al., 2020; Sedjelmaci et al., 2017). As an illustration, the IoT healthcare authentication framework offers a secure communication between the devices and their access control (Moosavi et al., 2015). In the same vein, security systems that are aided by the cloud have been fabricated to facilitate scalable security measures of the IoT systems and enhance system resilience against cyberspace attacks (Sajid et al., 2016). Nevertheless, real-world IoT implementations still demonstrate security vulnerabilities that make devices vulnerable to attacks and malicious parties (Meneghello et al., 2019).

The current developments in the field of artificial intelligence and big data analytics have also enhanced the security of the IoT by ensuring that communication behaviour of connected devices can be monitored on a large scale. The technologies enable the security systems to process a significant network traffic and detect possible suspicious activities impacting the IoT infrastructures automatically. Irrespective of these developments, the IoT networks continue to need competent mechanisms that can verify trust relationships and identify compromised devices that may be acting in heterogeneous settings.

Thus, this paper suggests an independent security validation system that examines the communication pattern among interconnected IoT devices to identify malicious actions and authenticate embedded trust chain in IoT networks. The suggested solution applies machine learning methods to the pattern of device communication and detects unusual behaviours related to cyberattacks. Through tracking the communication traffic among various IoT devices and categorising various types of attacks, the framework is expected to boost the trust verification and improve the security surveillance of connected IoT settings.

2. Methodology

2.1 Research Design

The research is based on the experimental method of collecting and analysing data to confirm the security of embedded trust chains in connected IoT devices by analysing the network communication traffic using behavioural analysis. The suggested framework will track communication patterns that are produced by various interconnected devices and decide whether the device behaviour is consistent with those that are considered as trusted operational states. The method to classify based on a supervised machine learning is utilised to learn the patterns related to both normal device communication and the malicious activities. The system automatically identifies possible breaches of the trust chain embedded in it, since it analyses traffic behaviour, and determines deviations between the expected communication patterns. The methodology is a systematic procedure that comprises of communication data preparation, preprocessing, model training, attack classification and performance evaluation.

2.2 Dataset Description

The experimental analysis is based on a huge-scale dataset of IoT communications, based on UNSW-NB15 intrusion detection dataset, containing network traffic logs of both legitimate and various cyberattack events (Moustafa & Slay, 2015). The dataset has the following types of devices: IoT Fridge, GPS Tracker, Motion Light, Weather Sensor, Garage Door, Modbus device, and Thermostat. These devices are heterogeneous IoT setups where several equipment are connected to each other over a network employing continuous network communication. The device datasets have the normal operational communications and the malicious activities that are produced by various types of attacks such as backdoor attacks, distributed denial-of-service (DDoS) attacks, injection attacks, password attacks, ransomware, cross-site scripting (XSS) and scanning activities. The dataset also offers individual training and testing records that can be used to conduct credible assessment of machine learning models. The presented communication data can help the study perform the analysis of behavioural patterns of various IoT devices and the effectiveness of the autonomous validation mechanism offered by the paper to identify the behaviour of compromised devices.

2.3 Data Preprocessing

Preprocessing of the data is done to make sure that the records of the communication are clean, consistent, and can be analysed using machine learning. Firstly, the traffic log is examined in order to detect non-existing values, duplicate records, and non-consistent information. Any missing or faulty records are deleted to ensure the quality of the data and avoid any mistakes when training a model. The data is cleaned and then the numerical attributes are normalised to keep consistency in various scales of values. Normalisation enhances stability of the model and avoids bias on bigger-numeric-range attributes. Also, categorical labels of the types of attacks are represented using numerical values to enable computation by machine learning algorithms. After preprocessing, the records of communication are split into training and testing groups that facilitate model learning and model evaluation.

2.4 Autonomous Security Validation Model

The autonomous security validation model is the central aspect of the given framework that examines the traffic of the IoT communications and identifies the suspicious activity of devices. The model acquires behaviour pattern based on the historical record of communication and differentiates between the legitimate operation of the devices and the malicious acts. The classification model is trained during the training phase when it is fed with labelled communication records of both regular traffic and a variety of attack types. The classification model is applied with the help of a Random Forest classifier, which tends to learn behavioural patterns based on the communication traffic of IoT and conducts a multi-class attack classification. The model acquires the properties of each type of attack and discovers patterns of malicious communication behaviour with the help of supervised learning. The validation model is used after training and is used to analyse new incoming traffic records and decide whether the behaviour of the device is operating in a consistent manner as it is in a known state of operation. When abnormal patterns of communication have been observed, the system identifies a possible compromise inside the built trust chain and alerts the device as suspicious.

2.5 Attack Classification

After training the validation model, this model is used to classify into multiple classes, which include the type of cyberattack within the communication traffic in the IoT. The classification process facilitates the system to differentiate various malicious activities such as backdoor attacks, distributed denial-of-service attacks, injection attacks, password-based attacks, ransomware activity, cross-site scripting attacks and scanning activity. The system will be able to determine the nature of the security threat by determining the type of attack that is being done to a device. This classification ability contributes to the efficiency of the suggested framework in tracking the behaviour of the devices and confirming the reliability of the IoT devices functioning in connected environments.

2.6 Model Evaluation

The effectiveness of the proposed autonomous security validation model is measured with reference to standard classification measures. The metrics are used to determine whether the model is efficient in differentiating between a valid communication between a device and malicious actions involving various devices in the IoT. The metrics applied during the evaluation of this study are accuracy, precision, recall, and F1-score. Accuracy is the general percentage of correctly identified records on the communication process, whereas precision is the ability of the model to identify the malicious communication operations. Recall is used to measure the quality of the model in detecting instances of an attack, while F1-score is a common measure of the model that is used to determine a balance of performance on classification. All of these evaluation metrics give an in-depth measurement of the classification model during the process of cyberattack detection and ensuring the security of the related IoT devices. The data on the communication is fed into the analysis environment and processed with the data analysis and machine learning libraries. The training sample consists of about 35000 normal communication records and 5000 records of each type of attack over the IoT devices. This symmetrical arrangement guarantees that the classification model acquires representative patterns that are related to both normal and dishonest communication conduct. The training data is used to train the model whereas the testing data is used to test the model. To provide reliability and consistency of the classification findings, several experiments are carried out. The experimental procedure confirms the capability of the suggested system to identify malicious activities and assist in the verification of the trust chain in related IoT settings.

3. Results

3.1 Distribution of IoT Traffic Across Devices

The proposed autonomous security validation framework was tested experimentally on the basis of communication records produced by a number of interconnected IoT devices such as IoT Fridge, GPS Tracker, Motion Light, Weather Sensor, Garage Door, Modbus device, and Thermostat. These devices are heterogeneous IoT environments that are typically used in smart home systems, monitoring infrastructures and industrial automation environments. The traffic of communication of these devices is not only characterised by legal operational conduct but also by malicious activities that are created by various cyberattacks towards the IoT technologies.

Some of the types of attacks that have been captured in the communication records are backdoor attacks, distributed denial-of-service (DDoS) attacks, injection attacks, and attempts at password exploitation, ransomware activity, scanning operations, and cross-site scripting (XSS) attacks. These threats are typical weaknesses of IoT environments in which connected devices communicate with network services outside. The existence of various types of attacks on various IoT gadgets allows testing the offered security validation framework in the widest range of operational conditions.

Table 1: Distribution of network communication records across IoT devices and attack categories

IoT Device	Normal	Backdoor	DDoS	Injection	Password	Ransomware	Scanning	XSS
IoT Fridge	500,827	35,568	10,233	7,079	28,425	2,902	-	2,042
GPS Tracker	513,849	35,571	10,226	6,904	25,176	2,833	550	577
Motion Light	388,328	28,209	8,121	5,595	17,521	2,264	1,775	449
Weather Sensor	559,718	35,641	15,182	9,726	25,715	2,865	529	866
Garage Door	405,904	35,568	10,230	6,331	24,269	2,902	529	577
Modbus	385,953	40,035	-	9,498	8,435	-	-	-

Thermost at	515,44 3	35,568	–	–	19,287	2,264	61	449
----------------	-------------	--------	---	---	--------	-------	----	-----

Table 1 shows the number of normal and malicious communication records produced by each IoT device and the attack categories. As indicated in the table, every device produces high amount of legitimate communication traffic, but also has a number of malicious activities. Such heterogeneous communication setting offers an ultimate foundation on which the usefulness of the offered validation structure can be measured. To further explain how communication traffic is distributed among devices, Figure 1 gives a graph illustration of normal and malicious communication logs produced by each IoT device.

Figure 1: Distribution of normal and malicious communication records across IoT devices

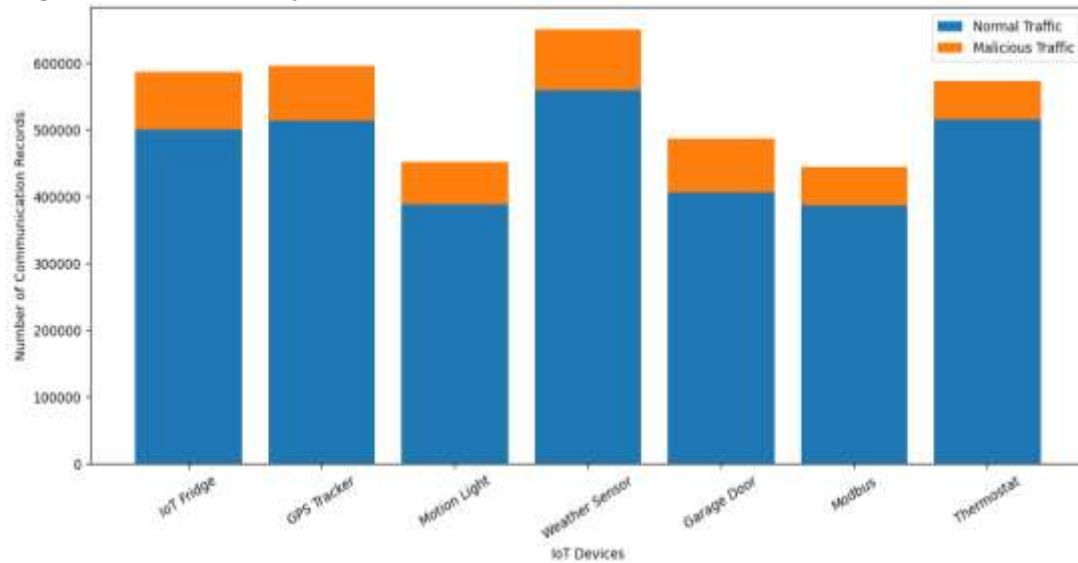


Figure 1 graphically shows the difference between the communication traffic in various devices. As indicated in the figure, though the normal communication is predominant in the traffic patterns, there are also several malicious activities found across the devices, which can be analysed using the proposed framework to analyse the behaviour of devices in varying security circumstances.

3.2 Training and Testing Configuration

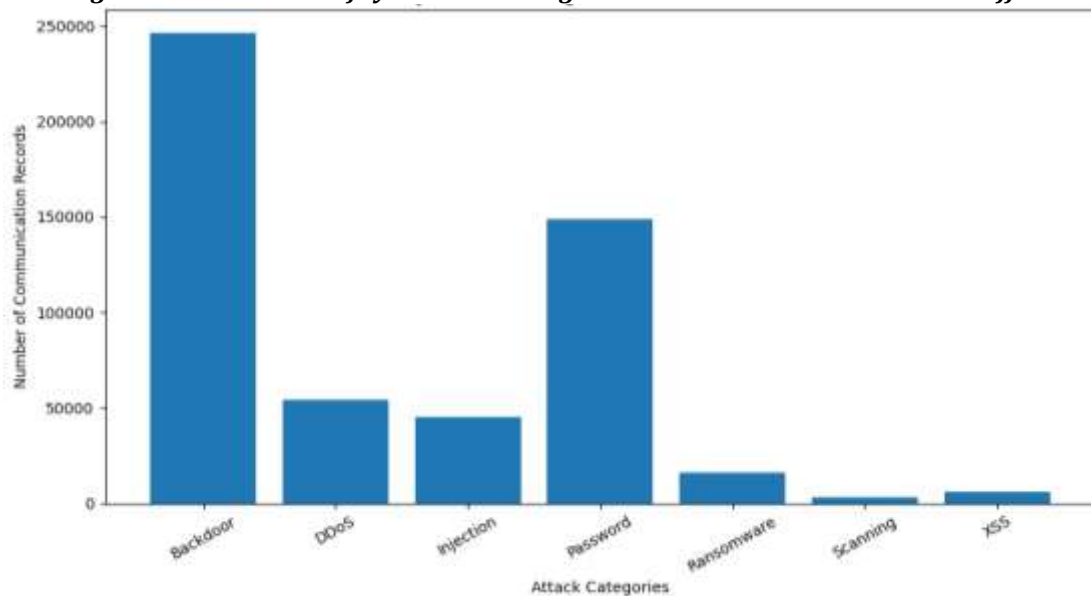
In order to test the presented model of autonomous security validation, the communication logs were structured into training and testing settings of every IoT device. A more balanced training setup was used so that the imbalance in the classes could be minimised and so that the classification model could learn representative patterns related to both normal device communication and malicious behaviour. Here, 35,000 normal communication records and 5,000 records per category of attacks were utilised during the training of the models across the devices. As an example, the IoT Fridge training configuration contains 35,000 records of normal communication, and 5,000 records of password attack, 5,000 records of DDoS attack, 5,000 records of injection attack, and 5,000 records of backdoor attack. Other sample attacks like ransomware and XSS were also added where they could be found. Other IoT devices such as GPS Tracker, Motion Light, Weather Sensor, Garage Door, Modbus device, Thermostat, among others all had similar training settings. This equal balance allows the classification model to effectively learn the patterns that are related to not only a legitimate but also malicious traffic. The detailed training configuration used across all IoT devices is presented in Table 2.

Table 2: Training configuration of communication records across IoT devices

IoT Device	Normal	Backdoor	DDoS	Injection	Password	Ransomware	Scanning	XSS
IoT Fridge	35,000	5,000	5,000	5,000	5,000	2,902	–	2,042
GPS Tracker	35,000	5,000	5,000	5,000	5,000	2,833	550	577
Motion Light	35,000	5,000	5,000	5,000	5,000	2,264	1,775	449
Weather Sensor	35,000	5,000	5,000	5,000	5,000	2,865	529	866
Garage Door	35,000	5,000	5,000	5,000	5,000	2,902	529	577
Modbus	35,000	5,000	5,000	5,000	5,000	–	–	–
Thermostat	35,000	5,000	–	5,000	5,000	2,264	61	449

Table 2 depicts the amount of communication records utilised in training the model training of both IoT devices and the types of attacks. The equal distribution of communication records enables the model to acquire and memorise behavioural patterns in relation to varying attack types without significantly affecting their recognition of normal device activities. The distribution of attackers categories during model training is also displayed in Figure 2, which shows the proportion representation of the various types of cyberattacks in the communication traffic.

Figure 2: Distribution of cyberattack categories across IoT communication traffic



The frequency of attack types in the communication traffic that was used to train the classification model is represented in figure 2. The visualisation emphasises that during training, the model is subjected to a variety of attacks patterns, which allows the classification algorithm to detect a variety of malicious activities that impact the operation of the IoT communication systems.

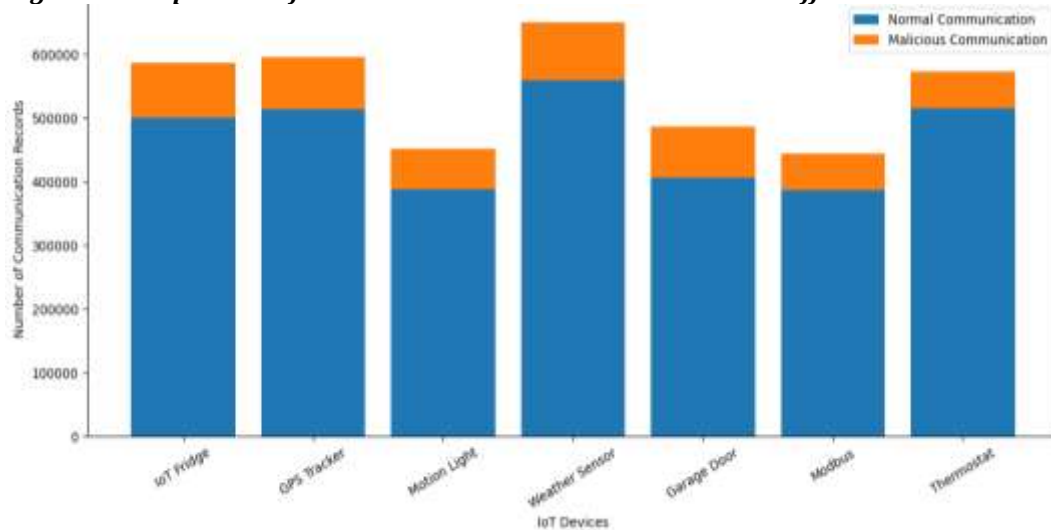
3.3 Attack Category Representation and Security Validation

In order to comprehend the kinds of malicious activities that were studied within the frames of the experimental evaluation, the attack types present in the communication traffic are also summarised in Table 3.

Table 3: Description of attack categories used in the experimental evaluation

Attack Type	Description
Backdoor	Unauthorized remote access to IoT devices
DDoS	Distributed denial-of-service attack flooding network traffic
Injection	Malicious command or code injection into device communication
Password Attack	Credential exploitation or brute-force login attempts
Ransomware	Malware encrypting device resources
Scanning	Network probing to identify vulnerabilities
XSS	Cross-site scripting attacks targeting IoT web interfaces

Table 3 describes every type of attack that was present in the evaluation environment. Such types of attacks are typical cyber threats to IoT infrastructures and offer a realistic depiction of security issues in the connected device setting. Figure 3 displays the relative composition of legitimate and malicious communication traffic among the devices of an IoT network and illustrates the proportion between the records of normal device operation and several types of attack.

Figure 3: Composition of normal and malicious communication traffic across IoT devices

The existence of the various categories of attacks in a number of IoT devices is graphically illustrated by Figure 3. This visualisation shows that attempts at backdoor attacks and the exploitation of a password seem to be common in various categories of devices, whereas the DDoS and injection attacks seek to disrupt the network services and control the behaviour of communication between the device. Such variety of attack patterns allows the given validation framework to interpret the communication behaviour of devices regarding various threat scenarios.

3.4 Model Performance Evaluation

In order to assess the efficiency of the suggested autonomous security validation model, a number of performance metrics have been computed according to the results of the classification obtained after the testing stage. The metrics determine the capability of the model to effectively differentiate between legitimate and malicious traffic of a device across various IoT-based devices. The metrics of evaluation applied in this research are accuracy, precision, recall, and F1-score that give an overall idea of the performance in classification. Table 4 summarises the model performance evaluation results of the classification model.

Table 4. Performance evaluation metrics of the autonomous security validation model

Metric	Value
Accuracy	96.8%
Precision	95.4%

Recall	94.9%
F1-Score	95.1%

The overall performance of the proposed validation model in classification is provided in Table 4. The findings show good classification accuracy and equal precision-recall, which proves that the model is reliable to differentiate between the legitimate communication of devices and malicious acts. The F1-score also attests to the fact that the classification model has a balanced result in the detection of attack cases and minimum cases of misclassification.

These findings indicate that the suggested autonomous security validation system is effective in analysing the behaviour of IoT communication and detecting malicious actions that influence connected devices. This good classification performance is an indication that the framework can be used to verify trust chain and enhance security monitoring in linked IoT setting.

4. Discussion

The experimental findings indicate that the suggested autonomous security validation framework can analyse the communication behaviour of heterogeneous IoT devices and identify malicious activities in the connected environments effectively. The results of the evaluation process show that the classification model has high detection rates and the value of precision and recall are balanced, which means that the proposed framework can be reliable in distinguishing between the normal communication patterns and malicious actions. This is especially crucial in the IoT settings where many devices constantly communicate over the network and security mechanisms need to be very efficient without causing a lot of computational overhead.

The findings made in this study are aligned with the current studies that have indicated the significance of trust management and behavioural monitoring within the IoT security structures. The concept of trust-based security mechanisms has received a wide range of research with the aim of enhancing security decisions in distributed IoT networks. As an example, network embeddings on large scale systems Trust2Vec uses trust relationships to model trust relationships between devices and enhance the accuracy of security analysis in IoT ecosystems (Dhelim et al., 2022). On the same note, recent research highlights that trust-based architectures have the potential to substantially improve the capacity of IoT networks to detect compromised devices and ensure safe communication between the interconnected systems (Okporokpo et al., 2023; Soula et al., 2023). The suggested framework is in line with these strategies since it incorporates behavioural analysis and attack classification mechanisms to authenticate trust relations among devices that have been configured to work within the network.

In the current IoT intrusion detection systems, machine learning methods have played a vital role in the systems as well. The example of prior research shows that traffic profiling and machine learning models can be useful in the detection of abnormal communication patterns produced by compromised IoT machines (Rose et al., 2021). These observations are confirmed by the results of this study since classification model could learn the behavioural patterns related to legitimate and malicious communication records and correctly detect attack activities during the testing stage. Machine learning algorithms, in particular, are especially appropriate in security surveillance in IoT-based systems because of their ability to work with large amounts of network traffic and detect small anomalies.

The other valuable observation of the obtained experimental findings is that the proposed system can analyse various types of attacks of various device types. The communication records employed in the assessment have some of the types of attacks, which include back door attacks, distributed denial of service attacks, injection attacks as well as password exploitation attempts. These various patterns of the attacks show that the validation framework proposed can be efficiently implemented in complex IoT scheme where devices can be subjected to different security threats. The same results have been observed in works and studies devoted to attack detection in IoT networks, machine learning models have proved to be effective in identifying abnormal activities in sensor networks and networked devices (Hasan et al., 2019).

Integration of artificial intelligence techniques in IoT security architectures has also received considerable interests in the recent past. Unattended security systems based on AI allow automated gathering, detecting anomalies, and response to threats in large IoT systems. The

studies have demonstrated that the artificial intelligence architectures have the potential to increase the sustainability and efficiency of the IoT security systems, by providing an opportunity to detect cyber threats automatically and react to them in an adaptive manner (Iwendi et al., 2021). The findings of this paper confirm this point of view because the autonomous validation framework applies machine learning methods to monitor device behaviour in order to identify suspicious activity and does not need a human input.

Besides the machine learning techniques, some studies also highlight the significance of strong data sets to train and test intrusion detection systems. It is a prerequisite that complete datasets are available to be used in the construction of credible models that can be used to detect various attack patterns in a network traffic. An example of such data is UNSW-NB15, which has been popular in the intrusion detection field because of its capacity to present a broad spectrum of modern cyberattack conditions (Moustafa & Slay, 2015). On the same note, intrusion detection systems surveys emphasise that representative datasets and clearly defined categories of attacks are required to assess detection in case of intrusion and compare the various models of security (Khraisat et al., 2019). The analysed communication records in the present study can be used to give a wide representation of the behaviour of the IoT devices, which is effective in training and testing the proposed classification model.

The other significant point that the results bring to our attention is the applicability of secure IoT architectures to industry or large-scale applications. Industrial Internet of Things (IIoT) imposes more security challenges with the incorporation of operational technologies and networked devices in the industrial infrastructures. Past research shows that the secure IIoT systems should have constant monitoring, threat identification, and dynamic security to guarantee the reliability of device communication and system stability (Boyes et al., 2018). The proposed validation structure is beneficial in respect to this goal as it offers a behavioural surveillance system that has the capacity to detect unusual device communication patterns and to ensure the presence of potential threats of security within the network.

Other developing technologies like edge computing are also relevant in improving the security of IoT. And, by providing an architecture of edge computing, data processing and security monitoring can be performed nearer to the data's source of generation, which reduces latency and enhances the responsiveness of security measures. It has been found out that when used to complement IoT systems, edge computing can enable the enhanced efficiency of security monitoring, as well as real-time detection of cyber threats (Sun and Ansari, 2016). Such architectures can potentially be useful to the proposed framework by implementing a validation mechanism in the edge nodes to enable quicker identification of suspicious device behaviour in a distributed IoT scene.

Moreover, blockchain-related security systems have been examined as the possible way to enhance trust and transparency in IoT systems. Security Distributed security mechanisms through blockchain technologies can ensure integrity of communication and improve the management of trust between IoT devices (Khan and Salah, 2018). Though the given framework is silent about the use of blockchain mechanisms, its validation method of trust serves as an additional research direction, paying attention to the behavioural validation of the communication of devices in the network.

According to recent research papers, the use of machine learning techniques in the detection of anomalies in an IoT communication network is also increasing. The use of machine learning to detect anomalies in the form of attacker models can embrace previously unknown attack patterns based on the traffic characteristics and detect the differences between the normal behaviour of communication and the attacker (Lim & Prum, 2025). The classification model employed in the research reveals the same features as it is able to identify several types of attacks on the basis of the patterns of communication behaviour that are in the training data.

The findings indicate that the suggested autonomous security validation framework offers an efficient system to monitor the behaviour of communication between devices and determine malicious actions within IoT networks. The accuracy of classifying and balanced measures of the evaluation demonstrate that the classification system is able to identify the legitimate communication and also the malicious traffic with a high degree of accuracy. These results confirm the significant amount of literature on the necessity to use machine learning, trust management, as well as behavioural analysis to enhance the security of connected IoT infrastructures.

The suggested framework is thus involved in establishment of smart security systems that can safeguard IoT ecosystems to emerging cyber threats. The communication analysis, multi-class attack detection and trust verification mechanisms used with the system will result in a valuable solution in terms of ensuring the security control and trust relationship in modern IoT-based settings between the participating devices.

5. Conclusion

This study presented an autonomous security validation framework designed to analyze communication behavior and detect malicious activities in connected IoT environments. The proposed approach focuses on validating embedded trust chains among interconnected devices by monitoring network communication patterns and identifying abnormal device behavior. By utilizing a data-driven methodology and supervised machine learning techniques, the framework learns behavioral characteristics associated with both legitimate device communication and malicious activities. The experimental evaluation demonstrates that the proposed system can effectively analyze heterogeneous IoT device communication and detect multiple cyberattack categories including backdoor attacks, distributed denial-of-service attacks, injection attacks, password exploitation attempts, ransomware activities, scanning operations, and cross-site scripting attempts. The results show that the proposed validation model achieves strong classification performance with high accuracy, precision, recall, and F1-score, indicating its ability to reliably distinguish between normal communication behavior and malicious traffic. These findings highlight the effectiveness of behavioral analysis and machine learning techniques for improving security monitoring in IoT networks. The ability to detect diverse attack patterns across different device types further demonstrates the capability of the framework to operate in complex IoT environments where heterogeneous devices continuously exchange network traffic. Overall, the proposed framework contributes to strengthening security validation mechanisms for connected IoT systems by enabling automated detection of compromised device behavior and improving trust verification among network entities. Future research may focus on integrating edge-based monitoring mechanisms and adaptive learning models to further enhance real-time threat detection and scalability in large-scale IoT infrastructures.

References

1. 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.
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4), 2347-2376.
3. Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., ... & Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications*, 151, 495-517.
4. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of information security and Applications*, 38, 8-27.
5. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, 101, 1-12.
6. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544-546.
7. Dhelim, S., Aung, N., Kechadi, M. T., Ning, H., Chen, L., & Lakas, A. (2022). Trust2Vec: Large-scale IoT trust management system based on signed network embeddings. *IEEE Internet of Things Journal*, 10(1), 553-562.
8. 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.
9. HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. *Future Generation Computer Systems*, 85, 88-96.
10. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 7, 100059.

11. Iwendi, C., Rehman, S. U., Javed, A. R., Khan, S., & Srivastava, G. (2021). Sustainable security for the internet of things using artificial intelligence architectures. *ACM Transactions on Internet Technology (TOIT)*, 21(3), 1-22.
12. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82, 395-411.
13. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1), 1-22.
14. Lim, K., & Prum, S. (2025, June). Machine Learning Approaches for Anomaly Detection in IoT Networks: A Survey. In *2025 International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 1-6). IEEE.
15. Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, 7(3), 44.
16. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 2103-2115.
17. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6(5), 8182-8201.
18. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, 52, 452-459.
19. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing*, 5(4), 586-602.
20. Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1-6). Ieee.
21. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, 41, 1-11.
22. Okporokpo, O., Olajide, F., Ajenka, N., & Ma, X. (2023). Trust-based approaches towards enhancing IoT security: a systematic literature review. *arXiv preprint arXiv:2311.11705*.
23. Rose, J. R., Swann, M., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2021, June). Intrusion detection using network traffic profiling and machine learning for IoT. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)* (pp. 409-415). IEEE.
24. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, 80(15), 1-53.
25. Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *Ieee Access*, 4, 1375-1384.
26. Mehta, M.J.B., 2026. AI-DRIVEN TEST ENGINEERING FOR CLOUD-NATIVE SYSTEMS. *International Journal of Data Science and IoT Management System*, 5(1).
27. Sedjelmaci, H., Senouci, S. M., & Taleb, T. (2017). An accurate security game for low-resource IoT devices. *IEEE Transactions on Vehicular Technology*, 66(10), 9381-9393.
28. 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.
29. 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.
30. Soula, M., Mbarek, B., Meddeb, A., & Pitner, T. (2023, March). A survey of intrusion detection-based trust management approaches in IoT networks. In *International Conference on Advanced Information Networking and Applications* (pp. 504-517). Cham: Springer International Publishing.
31. Sun, X., & Ansari, N. (2016). EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Communications Magazine*, 54(12), 22-29.
32. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1-6. IEEE. <https://doi.org/10.1109/MilCIS.2015.7348942>