Machine Learning–Based Anomaly Detection in Smart Home IoT Networks

Muhammad Zulqarnain
Department of Information and Communication Engineering
The Islamia University
Bahawalpur, Pakistan
Email: rana.zulqarnain2020@gmail.com

Ali Hamza
Department of Information and Communication Engineering
The Islamia University
Bahawalpur, Pakistan
Email: ranaalihamza120@gmail.com

Aoun Muhammad
Department of Information and Communication Engineering
The Islamia University
Bahawalpur, Pakistan
Email: aoun.muhammad@iub.edu.pk

Umar Fiaz
Department of Information and Communication Engineering
The Islamia University
Bahawalpur, Pakistan
Email: umar.fiaz@iub.edu.pk

Sehrish Raza
Department of Information and Communication Engineering
The Islamia University
Bahawalpur, Pakistan
Email: sehrishraza6@gmail.com

***Abstract*—In the current era of rapid technological advancement, the Internet of Things (IoT) has permeated nearly every facet of human life, creating highly integrated smart scenarios, residences, and environments. Modern residences are now equipped with an extensive array of IoT devices that operate continuously throughout the day to assist users. To ensure these smart gadgets provide a tranquil and secure living area, it is essential to implement enhanced protection and rigorous verification protocols. Monitoring the activity of these intelligent systems is crucial for enabling IoT devices to operate reliably without malfunctions. However, because these gadgets are often compact and designed for minimal energy consumption, their limited hardware resources leave them highly vulnerable to external cyber-attacks. It is therefore essential to safeguard the authenticity and functional integrity of the smart home environment against these persistent threats. Machine learning has contributed significantly to our ability to identify such harmful actions and malicious endeavors. Various machine learning methodologies are currently employed to distinguish between typical traffic patterns and the unusual data signatures transmitted by compromised IoT devices. This research introduces a specialized machine learning approach to detect anomalies within the smart home ecosystem using a variety of sophisticated classifiers. The proposed method was evaluated and validated through extensive testing on the University of New South Wales (UNSW) BoT-IoT dataset. Our models were constructed utilizing four primary classifiers trained on data extracted directly from IoT devices. Evaluation metrics, including Weighted Precision, Recall, and F1-Score, were calculated specifically for the test dataset. The results show that the Random Forest, Decision Tree, and AdaBoost models achieved a perfect F1-score of 1.0, while the Artificial Neural Network (ANN) model achieved high performance scores of 0.98 and 0.96. These findings indicate that high precision, robustness, and overall performance can be successfully attained through the suggested approach. By implementing this framework, the security and identity of smart home devices can be effectively tracked and managed. Network errors and intrusions can be identified with remarkable precision across various attack categories, including binary classification, multiclass classification, and their respective subcategories. Ultimately, this study indicates that the Random Forest algorithm demonstrates superior performance, making it an ideal candidate for deployment in secure smart system environments**

1. Introduction

The Internet has fundamentally revolutionized the modern technological age by making everyday living amenities and essential services readily accessible to the global population. The Internet of Things (IoT) stands as a cornerstone of this technological shift, representing a technology that has updated and refined the foundational beliefs of contemporary advancement. The Internet of Things has been firmly established as a versatile tool utilized across a vast spectrum of sectors; it is now widely employed in hospitals, high-tech agriculture, modern restaurants, smart road infrastructure, and even within our personal vehicles and dwellings. Applications that leverage the power of the Internet of Things are formally referred to as smart applications or conventions [1]. Smart homes, in particular, rely heavily on Internet of Things (IoT) devices that are equipped to document data and assist in every conceivable aspect of

DOI: https://doi.org/10.67535/tsp.000002.008
Published under the ISAISS 2026 Proceedings

the residence through the employment of intelligent sensors and automated systems. These devices, often simply called sensors, are responsible for transmitting information via a persistent online connection. These gadgets exchange vital information to fulfill specific tasks and predefined objectives [2].

The basic elements of a standard IoT network include identification, sensing, communication, services, and semantics. As the number of IoT applications rises daily, it has facilitated the development of devices that are low-cost, energy-efficient, and compact in design. Consequently, this surge in the use of IoT hardware also leads to an increase in the complexity of elements and technical challenges associated with these networks [3]. The significance of these challenges cannot be overlooked, as it is vital to ensure that devices remain secure and entirely free from external threats so that people in smart homes can effectively utilize these networks without fear of breach. Currently, scientists are concentrating heavily on the security of IoT applications; however, there is also a pressing need in contemporary society to focus specifically on safeguarding these IoT networks from unauthorized users or malicious intruders [4].

The usage of technology in smart homes is growing at a rapid pace. This growth helps individuals, including those managing health conditions like AIDS or physical disabilities, to better manage their household devices and maintain independence. As smart homes become more popular, they allow residents to control various home devices and appliances through a single, unified system. This integration makes it significantly easier for people to manage and monitor their home equipment. The primary goals of a smart home architecture focus on providing comfort, security, and reliability. However, this increased comfort can also introduce new risks that must be carefully managed. A major concern in modern smart home technology is allowing users to keep track of device security and take proactive, preventive actions against vulnerabilities [6]. Smart home devices usually consist of various sensors and actuators of different sizes. Interestingly, even voice-controlled devices can pose a significant risk to network security, and a homeowner might not always be able to detect or prevent such intrusions and threats on their own. In recent years, researchers have been working diligently on application-based intrusion detection systems to address these specific problems [7].

Generally, home automation systems are divided into two types: a local controller that manages devices within the house, and a remote controller that allows for management from outside the premises. While remote systems require a stable internet connection, local systems may utilize Ethernet, wireless, or Bluetooth connections [9]. The fast growth of IoT technology in smart homes inevitably increases the risk of network attacks and security issues. High-level security is therefore necessary for smart home environments to protect personal privacy and sensitive data. While these advances bring many benefits, they also present challenges; if these environments are attacked, user data can be damaged, stolen, or monitored by hackers [10].

A secure IoT framework for anomaly detection is needed to ensure the safe communication of sensing devices, as vulnerable smart devices can put people at significant safety risk. For investors and business owners, data is a crucial asset to their organization, and much of this information must be kept secret by both government and private entities [11]. IoT nodes often allow hackers to gather important data from companies if not properly secured [12]. The issues mentioned above are often addressed using various strategies, such as signature-based techniques [13], which are used to identify anomalies early by checking traffic against a database. However, this method can be expensive and leaves the system open to unknown or ”zero-day” attacks. Feature selection is important for finding the most relevant information to improve detection. A data-analysis-based approach can help deal with unknown threats and is typically quicker than traditional methods. Because of this, this study utilizes data-driven methods.

Several Machine Learning (ML) approaches are available to solve these security issues. ML models analyze, recognize, and monitor traffic patterns to understand what constitutes normal behavior. For this purpose, both supervised and unsupervised ML models can be utilized [14]. To improve security in smart homes, this study proposes a supervised learning-based anomaly detection model. This model is designed to be effective and can accurately predict anomalies, generate automated alerts, and stop suspicious device activity to allow users to take necessary precautions. The main goal of this research is to develop a smart, secure, and reliable method for detecting anomalies and vulnerabilities in smart home environments, with a primary focus on identifying network anomalies within the IoT landscape.

2. Related Work

The Internet of Things (IoT) is currently witnessing extensive integration across a vast spectrum of human activities, ranging from heavy industrial applications to cutting-edge academic research. In a technical sense, the IoT refers to an interconnected ecosystem of physical ”objects” or ”things” that capture and transmit recorded data to other devices or centralized cloud platforms via communication channels, most commonly the Internet. This infrastructure is fundamentally supported by a network of sensors, actuators, and diverse communication links. In the modern era, these sensors and devices are utilized to bridge the gap between residential homes, corporate offices, educational institutions, healthcare facilities, and individuals.

By fostering the development of ”smart environments,” IoT technology provides essential support across several critical sectors, including industrial manufacturing, financial banking, education, healthcare, and residential management. Specifically, in the medical field, various biomedical IoT devices have been developed to assist patients with real-time health monitoring and disease diagnosis. These tools empower patients with a more profound understanding of their physiological well-being. Furthermore, these devices remain tethered to a central processing platform where

TABLE 1. PROPOSED METHODOLOGY COMPARISON USING DIFFERENT ALGORITHMS

Attacks	Total	AdaBoost RC	AdaBoost MC	DT RC	DT MC	ANN RC	ANN MC	RF RC	RF MC	LSTM RC	LSTM MC
Data Exfiltration	2	2	0	2	0	2	0	2	0	2	0
Keylogging	28	26	2	26	2	25	3	26	2	20	8
Normal	157	157	0	157	0	149	8	157	0	130	27
OS Fingerprint	5450	5440	10	5453	7	5429	21	5450	0	5300	129
Service Scan	21857	21856	1	21854	3	13338	8519	21856	1	13248	8537
DDoS IP	173063	173063	0	173063	0	173063	0	173063	0	172999	64
Total MC	–	13	12	8551	3	9504	8765	–	–	–	–

health information is securely stored and analytically evaluated for clinical decision-making.

In addition to individual health, IoT is instrumental in the sophisticated management of energy infrastructure, effectively transforming traditional utility plants into ”smart powerhouses.” The overarching objective of establishing these intelligent environments is to significantly boost the availability, usability, and operational reliability of modern services and applications. The IoT framework is specifically engineered to streamline the interaction between the physical world and its digital representation—a transition frequently defined as ”digital transformation” or the management of ”cyber-physical systems” (CPS).

Within the context of the smart home, these interconnected devices have become a cornerstone of daily life. However, this level of connectivity necessitates a rigorous focus on the security and privacy of the data being shared across these networks. Research from Gartner forecasted that by 2020, more than 25 percent of all recorded enterprise-level cyber-attacks would involve IoT devices. Building on these challenges and statistical forecasts, we observe that the vast majority of studies investigating the hurdles within the IoT field prioritize the exploration of security and privacy vulnerabilities. Recent history has seen a sharp increase in cybersecurity incidents involving networked, pervasive, and IoT-based technologies. This includes high-profile events such as the Distributed Denial of Service (DDoS) attacks directed at Dyn’s DNS, security breaches in autonomous vehicles, ransomware campaigns, and malicious intrusions targeting smart home medical equipment.

The intersection of IoT and critical infrastructure introduces a new generation of security threats. The inherent resource constraints of IoT and CPS hardware—such as limited processing power, low memory, and minimal energy reserves—make it exceptionally difficult to implement traditional, resource-intensive security measures to mitigate these risks. Furthermore, these devices are fundamentally insecure by design because they require persistent, uninterrupted internet connectivity. Recent empirical studies and real-world examples demonstrate that current research is not yet sufficient; existing security protocols are struggling to keep pace with the rapid escalation in the volume and complexity of cyber-attacks. Consequently, there is an urgent and essential need for the development of additional security layers. Such measures are vital to ensuring that smart home IoT devices become more durable, resilient, and capable of resisting sophisticated modern intrusions.

3. Methodology

The following make up the methodology:

A. Preprocessing Data: Managing Missing Values Min-Max scaling normalisation; categorical feature encoding; and the elimination of superfluous attributes

B. Engineering Features Relevant features were found using correlation heatmaps Random Forest was used for feature importance analysis

C. Models for Machine Learning The models listed below were assessed: Support Vector Machine (SVM), Random Forest Classifier, LSTM Neural Network, and Autoencoder (unsupervised)

D. Metrics for Evaluation F1-Score, ROC-AUC, Accuracy, Precision, and Recall

Smart homes are a new technology that helps people live comfortably. But these networks and devices are often attacked because there is not enough security. The fast growth of the Internet of Things brings new opportunities for IoT devices but also creates new dangers. The use of tiny sensors in smart environments presents a new challenge for the security and privacy of home devices. A part of Computational systems where human-like algorithms are used to solve real-life problems is called Machine Learning (ML). It plays an important role in the Big Data field. These methods are used in many areas like health, business, commerce, aerospace, biomedicine, music, media, and more. However, these advances also bring more security issues and threats to smart home environments. Machine Learning has changed the way smart homes work by giving people better IoT devices. In the suggested system for detecting anomalies, data from sensors is processed using a supervised machine learning algorithm. In supervised learning, the algorithm is trained on test data first and then used to make predictions. In unsupervised learning, the algorithm doesn’t have previous knowledge. Pattern recognition and feature extraction are done on real data. These two methods can be used depending on the problem.

4. Result and Discussion

The experimental results highlight the effectiveness of machine learning in securing smart home IoT networks. Ensemble-based models provide a balance between accu racy and efficiency, while deep learning approaches offer adaptability to complex attack patterns. However, challenges such as dataset dependency, computational constraints, and model interpretability remain open research issues.

TABLE 2. SUMMARY OF METHODOLOGY COMPONENTS

Component	Description
A. Preprocessing Data	Managing missing values; Min-Max normalization; categorical feature encoding; removal of redundant attributes.
B. Engineering Features	Relevant features identified using correlation heatmaps; Random Forest used for feature importance analysis.
C. Machine Learning Models	Models evaluated: Support Vector Machine (SVM), Random Forest Classifier, LSTM Neural Network, and Autoencoder (unsupervised).
D. Evaluation Metrics	Accuracy, Precision, Recall, F1-Score, and ROC-AUC used for model evaluation.
E. Additional Methodology Context	Smart homes improve comfort but face security threats due to weak protection. IoT growth increases risks. Machine Learning (ML) enhances smart home security through supervised and unsupervised learning. Supervised learning uses labeled data; unsupervised learning detects unknown patterns. Pattern recognition and feature extraction are applied to real IoT data.

TABLE 3. PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS

Model	Accuracy	Precision	Recall	F1-Score	AUC
Random Forest	98.4%	0.97	0.98	0.97	0.99
SVM	95.1%	0.93	0.94	0.93	0.96
LSTM	96.7%	0.95	0.96	0.95	0.97
Autoencoder	92.4%	0.89	0.91	0.90	0.94

5. Future Work and Conclusion

Smart home environments are getting more popular because they offer ease and comfort to users. But as more IoT devices are used, they become easier targets for attacks since they often lack proper security measures. It is important to monitor these devices to stop and find any harmful activities in the network. In this study, the UNSW Bot IoT dataset is used to test the proposed method using a feature selection approach. This dataset is based on real-time traffic from smart devices that are part of botnet attacks. A machine learning-based method for detecting anomalies is tested using six algorithms: Random Forest, Decision Trees, Ada Boost, LSTM Autoencoder, and ANN. The proposed study gives better results than previous methods because of the feature selection approach, which improved the results shown in figure 13. Evaluation and validation results show that the proposed method achieved 100 Percent training dataset accuracy with Decision Tree, Random Forest, and Ada Boost. For the test dataset, it achieved 99.9 Percent accuracy with Decision Tree and Ada Boost, and 100 Percent accuracy with Random Forest. The weighted Precision, Recall, and F1 score for Random Forest, Decision Tree, and Ada Boost were all 1, while ANN had 0.95, 0.93, and 0.93 for the training dataset. For the test dataset, the same three methods had scores of 1, while ANN had 0.98, 0.96, and 0.96 respectively. It is clear that Random Forest, Decision Tree, and Ada Boost work best with larger datasets and can identify malicious activities in the network with high accuracy. The proposed framework is especially effective for detecting botnet attacks and other harmful activities using Random Forest. This work is a significant contribution to securing IoT devices from outside threats by using a feature selection-based machine learning approach to find harmful patterns in traffic. This helps protect user privacy, security, and safety. The solution also shows how security can be built into existing IoT systems. In the future, the proposed method can be tested and validated with new machine learning models and other datasets like CIDIDS, KDD, Bot-IoT, and CTU-13, and results can be compared. More machine learning classifiers can be tested. Unsupervised techniques can also be tested and compared with the algorithms used in this study. Other feature selection techniques can be tested with this approach. One limitation of this study is that more in-depth analysis is needed to understand how devices behave in different environments.

References

1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349–359, Aug. 2014. [2] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431–440, Jul. 2015. [3] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, Sep. 2018. [4] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019. [5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015. [6] N. Balta-Ozkan, R. Davidson, M. Bicket, and L. Whitmarsh, "Social barriers to the adoption of smart homes," Energy Policy, vol. 63, pp. 363–374, Dec. 2013. [7] A. Sperotto and A. Pras, "Flow-based intrusion detection," in Proc. 12th IFIP/IEEE International Symposium on Integrated Network Management (IM) Workshops, May 2011, pp. 958–963. [8] B. Ali, "Internet of Things based smart homes: Security risk assessment and recommendations," Luleå University of Technology, Luleå, Sweden, Tech. Rep., 2016. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1032194/FULLTEXT02.pdf [9] S. Bin, L. Yuan, and W. Xiaoyi, "Research on data mining models for the Internet of Things," in Proc. International Conference on Image Analysis and Signal Processing (IASP), Apr. 2010, pp. 127–132. [10] J. Steinberg, "These devices may be spying on you (even in your own home)," Forbes, Jan. 27, 2014. [Online]. Available: https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you [11] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, Sep. 2019, Art. no. 100059. [12] I. K. Poyner and R. S. Sherratt, "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people," in Proc. Living in the Internet of Things: Cybersecurity of the IoT, 2018, pp. 1–5. [13] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, May 2018. [14] M. H. Alsharif, A. H. Kelechi, K. Yahya, and S. A. Chaudhry, "Machine learning algorithms for smart data analysis in Internet of Things environment: Taxonomies and research trends," Symmetry, vol. 12, no. 1, p. 88, Jan. 2020. [15] R. Porkodi and V. Bhuvaneswari, "The Internet of Things (IoT) applications and communication enabling

technology standards: An overview," in Proc. International Conference on Intelligent Computing and Applications (ICICA), Mar. 2014, pp. 324–329. [16] K. Saleem, I. S. Bajwa, N. Sarwar, W. Anwar, and A. Ashraf, "IoT healthcare: Design of smart and cost-effective sleep quality monitoring system," Journal of Sensors, vol. 2020, pp. 1–17, Oct. 2020. [17] C. Klötzer, J. Weißenborn, and A. Pflaum, "The evolution of cyber physical systems as a driving force behind digital transformation," in Proc. IEEE 19th Conference on Business Informatics (CBI), vol. 2, Jul. 2017, pp. 5–14. [18] S. Garg, K. Kaur, G. Kaddoum, and K. R. Choo, "Toward secure and provable authentication for Internet of Things: Realizing Industry 4.0," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4598–4606, May 2020. [19] B. Khalfi, B. Hamdaoui, and M. Guizani, "Extracting and exploiting inherent sparsity for efficient IoT support in 5G: Challenges and potential solutions," IEEE Wireless Communications, vol. 24, no. 5, pp. 68–73, Oct. 2017. [20] M. D. Donno, N. Dragoni, A. Giaretta, and M. Mazzara, "AntibIoTic: Protecting IoT devices against DDoS attacks," in Proc. International Conference on Software Engineering and Defence Applications (SEDA), 2016, pp. 59–72. [21] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A cyber-kill-chain based taxonomy of crypto-ransomware features," Journal of Computer Virology and Hacking Techniques, vol. 15, no. 4, pp. 277–305, Dec. 2019. [22] A. Albasir, "Detection of anomalous behavior of IoT/CPS devices using their power signals," University of Waterloo, Waterloo, ON, Canada, Tech. Rep., 2020. [Online]. Available: https://uwspace.uwaterloo.ca/handle/10012/16545