DS Journal of Artificial Intelligence and Robotics
Volume 1 Issue 1, 37-43, July - September 2023
ISSN: 2583-9926/ https://doi.org/10.59232/AIR-V1I1P104

Original Article

Machine Learning-based Secure Cloud-IoT Monitoring System for Wireless Communications

P. Rajadurai

Department of Computer Science, Tamilavel Umamaheswaranar Karanthai Arts College, Thanjavur, India.

rajadurai18.panju@gmail.com

Received: 14 April 2023 Revised: 16 June 2023 Accepted: 28 June 2023 Published: 07 July 2023

Abstract - The Internet of Things (IoT) paradigm presents a number of security challenges because of the growing scale and mobility of the user base. Additionally, flexibility and connection with a cloud network are necessary for operating a central security architecture. In this paper, a novel secure IoT monitoring (Sec-IoTM) system has been proposed, which improves the security features in cloud-assisted IoT environments. The proposed system consists of three phases, namely spoof detection, trust monitoring, and authentication system. The spoof detection phase makes use of a support vector machine (SVM), which classifies the request as an attack or not. This will remove the unauthorized user at the initial stage. The trust monitoring phase contains an intrusion detection system and an intrusion prevention system that will detect and prevent the data from the attack. The authentication system will authenticate the user, and if it is an unauthenticated user, then it will be blocked. If the user is an authenticated one, then the message will be encrypted using Advanced Encryption Standard (AES) algorithm. The performance metrics of the proposed Sec-IoTM method have been evaluated in terms of parameters like performance metrics, detection times, and false positive rates. The proposed method achieves high accuracy, 96% better than existing techniques.

Keywords - Internet of Things (IoT), Machine learning, IoT monitoring system, Security, Encryption, AES algorithm

1. Introduction

Machine learning is a developing technology that allows computers to learn autonomously from prior data [1]. Machine learning employs a variety of methods to construct mathematical models and anticipates outcomes based on past data and information [2]. It is now utilized for picture recognition, speech recognition, email filtering, facebook auto-tagging, and recommendation systems [3,4].

The discipline of safeguarding IoT systems is known as IoT security. IoT security technologies aid in the prevention of attacks and breaches, the identification and monitoring of risks, and the remediation of vulnerabilities [5]. IoT security guarantees that IoT solutions are available, secure, and confidential [6]. The major cloud provider provides IoT device monitoring and security, encryption of her IoT data in transit and at rest, vulnerability assessments that IT managers may do prior to a data breach, and robust network communication security. [7].

Cellular wireless communication is via GSM/3G/4G/LTE and now 5G. This communication protocol is ideal for sensor-based IoT devices and high-speed data operating in remote locations [8, 9]. Like WLAN, wireless communication over cellular networks is easy to use and safe to use [10]. The major contribution of the work has been followed by In this paper, a novel secure IoT monitoring (Sec-IoTM) system has been proposed, which improves the security features in cloud-assisted IoT environments.

- Initially, the spoof detection phase makes use of a support vector machine (SVM), which classifies the request as an attack or not. This will remove the unauthorized user at the initial stage.
- Secondly, the trust monitoring phase contains an intrusion detection system and an intrusion prevention system that will detect and prevent the data from the attack.
- Finally, the authentication system will authenticate the user, and if it is an unauthenticated user, then it will be blocked. If the user is an authenticated one, then the message will be encrypted using Advanced Encryption Standard (AES) algorithm.
- The performance metrics of the proposed Sec-IoTM method have been calculated in terms of parameters such as performance metrics, detection times, and false positive rates.

The remaining portions of the research can be followed: Section II denotes the literature review in detail. Section III represents the suggested technique. Section IV represents the result, and section V represents the conclusion.

2. Literature Review

In 2019 Alli, A.A. and Alam, M.M., et al. [11] proposed a secure computing offload scheme (SecOFF-FCIoT) in a Fog Cloud IoT environment. Achieve efficient and safe offloading in Fog-IoT environments with the help of machine learning strategies. Simulation results show that our proposed scheme minimizes latency compared to our chosen benchmarks.

In 2023 Upreti, K. et al. [12] suggested a novel data transmission protocol based on fuzzy rule-based secure transmission with data optimization techniques utilizing deep-gain neural networks and wireless connection. The experimental findings reveal that execution time is 54%, network performance is 96%, total complexity is 71%, data optimization is 95%, and end-to-end latency is 67%.

In 2022 Vijayasekaran, G. and Duraipandian M. et al. [13] introduced the concept of edge computing, which processes data on edge devices and transfers it to the cloud, reducing latency and increasing system efficiency. Experimental results confirm that the suggested methods have lower latency and enhanced efficiency than traditional cloud IoT systems.

In 2020 Xiao L.et al. [14] suggested a reinforcement learning (RL) based edge central processing unit (CPU) allocation algorithm without knowing the mobile service generation model and the network model. Experimental results show that this framework suppresses selfish edge attacks, reduces response delay and saves power compared to benchmark MEC schemes.

In 2020 Khan, M.A. et al. [15] proposed a blockchain-based Deep Extreme Learning Machine (DELM) architecture. Several statistical methods were used to measure the effectiveness of the proposed solutions. The results obtained are promising, and we are currently looking at scaling them up by applying more datasets and different architectures.

According to the literature review, most approaches failed to achieve.

3. Proposed Methodology

In this paper, a novel secure IoT monitoring (Sec-IoTM) system has been proposed, which improves the security features in cloud-assisted IoT environments. The proposed system consists of three phases, namely spoof detection, trust monitoring, and authentication system. The spoof detection phase makes use of a support vector machine (SVM), which classifies the request as an attack or not. This will remove the unauthorized user at the initial stage. The trust monitoring phase contains an intrusion detection system and an intrusion prevention system that will detect and prevent the data from the attack. The authentication system will authenticate the user, and if it is an unauthenticated user, then it will be blocked. If the user is an authenticated one, then the message will be encrypted using Advanced Encryption Standard (AES) algorithm. The overall block diagram for the proposed Sec-IoTM technique is given in Figure 1.

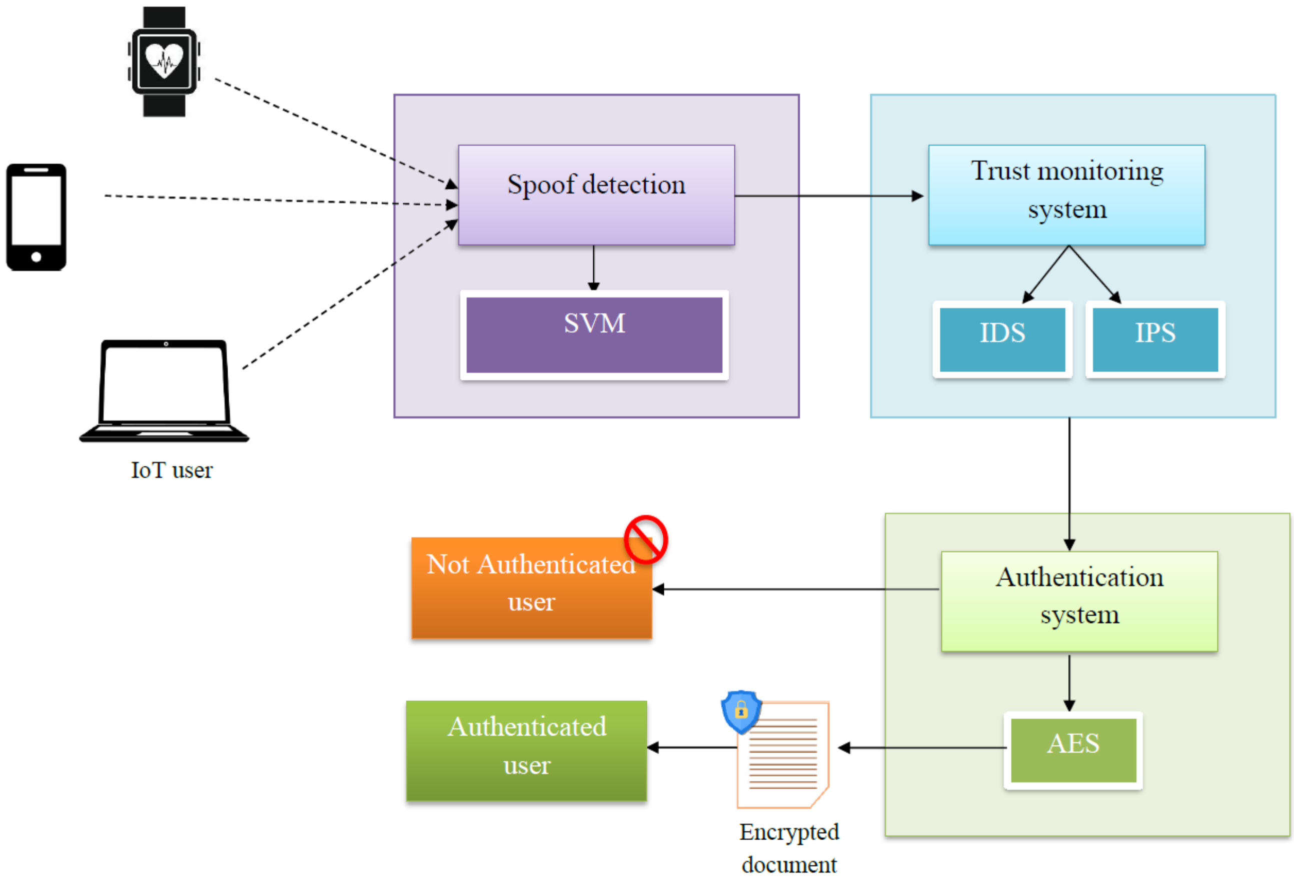

Fig. 1 Overall block diagram for the proposed Sec-IoTM method

4. Spoof Detection in SVM

Spoofing attempts can be detected by algorithms that detect non-living sample artifacts and may use "active" means such as secondary modalities. Spoofing and other presentation assaults are considerably reduced in efficacy by liveness detection technologies. SVM is a very effective supervised technique that performs best on small yet complicated datasets. SVMs, or support vector machines, may be used for both regression and classification tasks but are often better suited for classification challenges. Typically, SVMs are used to categorize high-dimensional data that may be separated by a kernel function. When training data is scarce, SVM performs better in classification. The natural human voice and synthetic speech are used to train SVM-based binary classifiers. As illustrated in (1) and (2), while training an SVM, natural languages are allocated class +1, and synthetic languages are assigned class -1. (x,y) denotes the training data set, x the MFCC function set, and y the class label. The normal vector is w, and the bias value is bo.

$$< v.y > +co \geq 1, \forall x = 1 \tag{1}$$

$$< v.y > +co \geq -1, \forall x = 1 \tag{2}$$

Separating the training data used linear and nonlinear radial basis function (RBF) kernels to separate the natural and synthetic fake hyperplanes. The linear kernel function and the RBF kernel function with small positive σ are given by (1) and (2).

5. Authentication System

Authentication technologies manage system access by checking that a user's credentials match those on a database or data authentication server owned by an authorized user. Authentication maintains the security of organizational systems, procedures, and information.

6. Result and Discussion

The experimental arrangement of the proposed technique-based smart appliances was implemented using MATLAB. Accuracy, specificity, precision, and recall are the different metrics used to evaluate it. The performance of the proposed Sec-IoTM method has been evaluated in terms of parameters such as Performance metrics, detection times, and false positive rates.

7. Performance Metrics:

The effectiveness of the categorization strategy is assessed using the following statistical parameters as Precision, Recall, Accuracy, Specificity and sensitivity.

7.1. Accuracy

Accuracy is defined as the number of corrected predictions for all of the input samples. It is evaluated by,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

7.2. Specificity

Specificity measures when the real condition is absent and an attack is classified negatively. It is evaluated by,

$$Specificity = \frac{TN}{TN + FP}$$

7.3. Precision

Precision, when the rate of false positives is large, offers an accurate assessment, and it is evaluated by,

$$Precision = \frac{TP}{TP + FP}$$

7.4. Recall

A model that produces no false negatives has a recall, and it is calculated by,

$$Recall = \frac{TP}{TP + TN}$$

Where TN, FN represents the true and false negatives and TP, FP denotes the true and false of the sample.

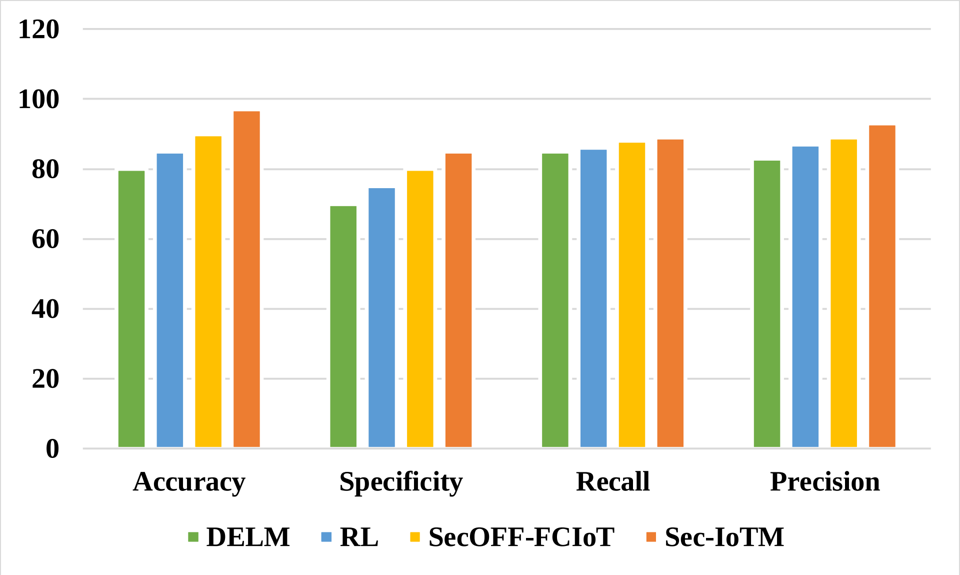

Fig. 2 Comparison via performance analysis

Fig. 2 shows a comparative result analysis of the proposed model. With respect to accuracy, Specificity, Precision and Recall while the DELM, RL, and SecOFF-FCIoT systems have accomplished. In the proposed method achieves high accuracy, 96% better than existing techniques.

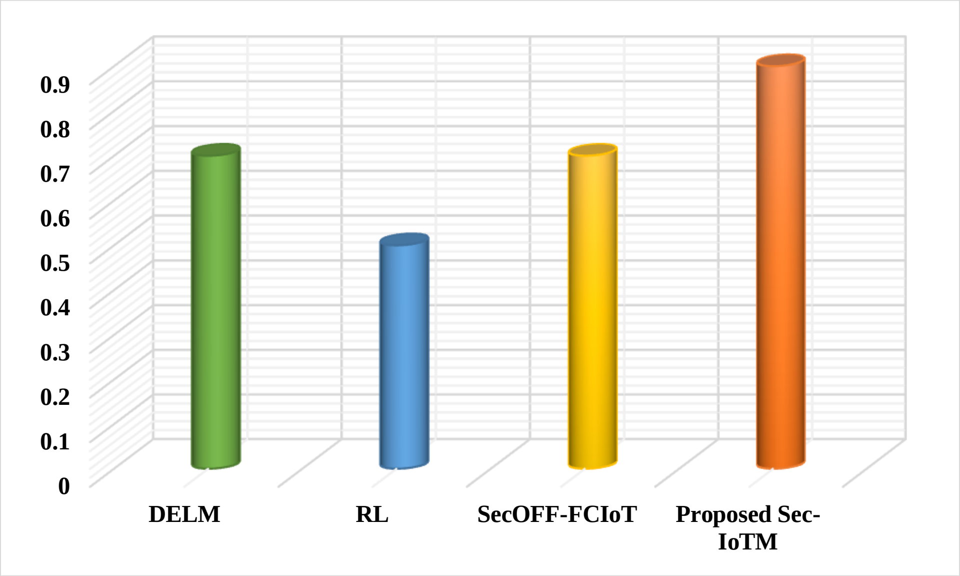

Fig. 3 Detection time

Attack detection time is the total amount of time needed to identify the attacker's IP address, identify susceptible behaviour, and contact the coordinator to validate other properties. Fig. 3 displays the average amount of time needed to identify a single attack. When compared to existing approaches, the proposed Sec-IoTM has the quickest attack detection time and is more effective than the DELM, RL, and SecOFF-FCIoT.

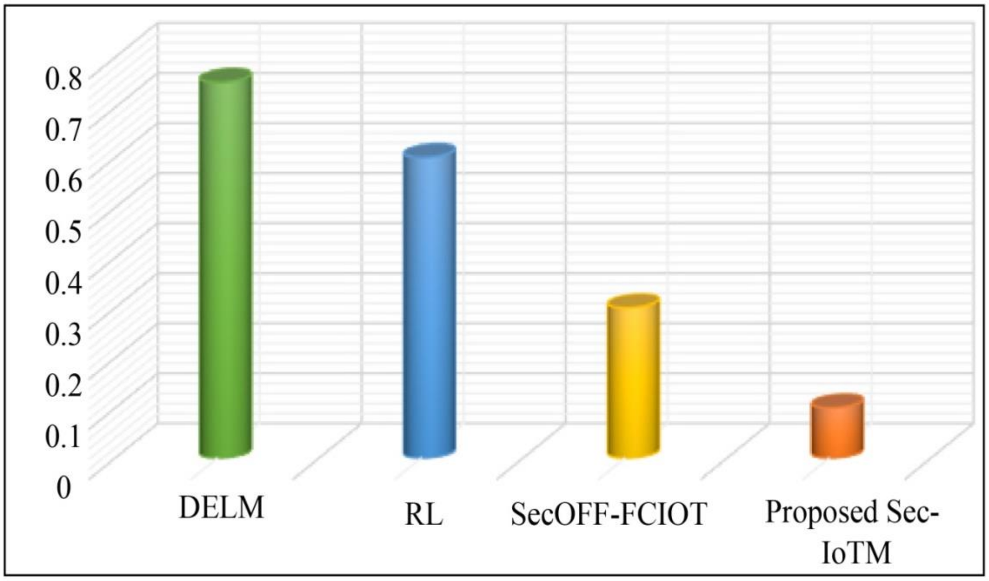

Fig. 4 False positive rate

Fig. 4 illustrates the proposed Sec-IoTM technique achieves the 10% lowest false positive rate compared with DELM, RL, and SecOFF-FCIoT.

8. Conclusion

This paper proposes a novel secure IoT monitoring (Sec-IoTM) system which improves the security features in cloud-assisted IoT environments. The proposed system consists of three phases, namely spoof detection, trust monitoring, and authentication system. The spoof detection phase makes use of a support vector machine (SVM), which classifies the request as an attack or not. This will remove the unauthorized user at the initial stage. The trust monitoring phase contains an intrusion detection system and an intrusion prevention system that will detect and prevent the data from the attack. The authentication system will authenticate the user, and if it is an unauthenticated user, then it will be blocked. If the user is an authenticated one, then the message will be encrypted using Advanced Encryption Standard (AES) algorithm. The performance of the proposed Sec-IoTM method has been evaluated in terms of parameters such as performance metrics, detection times, and false positive rates. In the proposed method achieves high accuracy, 96% better than existing techniques.

References

[1] Gagandeep Kaur et al., "Face Mask Recognition System using CNN Model," *Neuroscience Informatics*, vol. 2, no. 3, p. 100035, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] P. Yogendra Prasad et al., "Implementation of Machine Learning Based Google Teachable Machine in Early Childhood Education," *International Journal of Early Childhood*, vol. 14, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Gunes Gürsoy, Asaf Varol, and Serkan Varol, "Impact of Machine Learning in Digital Marketing Applications," *3rd International Informatics and Software Engineering Conference*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Philip Tovstogan, Xavier Serra, and Dmitry Bogdanov, "Similarity of Nearest-Neighbor Query Results in Deep Latent Spaces," *Proceedings of the Sound and Music Computing 2022 Music Technology and Design*, pp. 287-294, 2022. [Google Scholar] [Publsisher Link]

[5] Muhammad Shafiq et al., "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-based Security Attacks," *Wireless Communications and Mobile Computing*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Abid Ali et al., "Advanced Security Framework for Internet of Things (IoT)," *Technologies*, vol. 10, no. 3, p. 60, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Giancarlo Fortino et al., “Iot Platforms and Security: An Analysis of the Leading Industrial/Commercial Solutions,” *Sensors*, vol. 22, no. 6, p. 2196, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Caroline Omoanatse Alenoghena et al., "Telemedicine: A Survey of Telecommunication Technologies, Developments, and Challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, p. 20, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Muhammad Naeem Tahir, Pekka Leviäkangas, and Marcos Katz, "Connected Vehicles: V2V and V2I Road Weather and Traffic Communication using Cellular Technologies," *Sensors*, vol. 22, no. 3, p. 1142, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Chetna Monga et al., "Secure Techniques for Channel Encryption in Wireless Body Area Network without the Certificate," *Wireless Communications and Mobile Computing*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Adam A. Alli, and Muhammad Mahbub Alam, "SecOFF-FCIoT: Machine Learning based Secure Offloading in Fog-Cloud of Things for Smart City Applications," *Internet of Things*, vol. 7, p. 100070, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Kamal Upreti et al., "Enhanced Algorithmic Modelling and Architecture in Deep Reinforcement Learning based on Wireless Communication Fintech Technology," *Optik*, vol. 272, p. 170309, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] G. Vijayasekaran, and M. Duraipandian, "An Efficient Clustering and Deep Learning-based Resource Scheduling for Edge Computing to Integrate Cloud-IoT," *Wireless Personal Communications*, vol. 124, pp. 2029-2044, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Liang Xiao et al., "A Reinforcement Learning and Blockchain-based Trust Mechanism for Edge Networks," IEEE Transactions on Communications, vol. 68, no. 9, pp. 5460-5470, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Muhammad Adnan Khan et al., "A Machine Learning Approach for Blockchain-based Smart Home Networks Security," *IEEE Network*, vol. 35, no. 3, pp. 223-229, 2020. [CrossRef] [Google Scholar] [Publisher Link]