IoT and Machine Learning Based Attacks Detection Model on Wearable Health Care Devices

Dr. F Rahman, Lalnunthari,

Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.

KEYWORDS

Network Security, Malware Detection, Machine Learning, SVM, RF

ABSTRACT

The Internet of Things (IoT) in healthcare is becoming more and more popular in the field of research aimed at improving the effectiveness of intelligent healthcare networks and applications. Nonetheless, distinct risks affect the security and privacy of data in smart health (S-Health). IoT enables healthcare professionals to engage with patients more proactively and with greater vigilance. Smart gadgets with tiny sensors attached to them that communicate with one another to track each other's performance are part of the Internet of Things. To defend S-Health from MITM attacks. The suggested method employs two layers of machine learning algorithms for attack detection and security mechanisms, including low-cost access policies for SHRs (Smart Health Records), lightweight IoT detection schemes, and timely detection of to lessen their impact on the network. According to simulation data, the suggested Hybrid ML performs better than current methods and has a higher attack detection rate overall. The main goal of this research article is to develop an attack detection technique.

1. Introduction

Because the computers are so complicated, both suppliers and customers frequently argue that they shouldn't take proper security precautions because of their heterogeneous appearance. Thanks to Internet of Things (IoT)-enabled devices, remote monitoring in the healthcare sector is now possible, opening up opportunities to keep patients safe and healthy while also enabling physicians to give superior care [1]. Patient satisfaction and engagement have increased along with the ease and efficiency of doctor-patient interactions. Despite the fact that IoT has advanced healthcare, there are certain problems with its application in this field. Security is the main problem. Every patient wants the privacy of his information; he does not want his medical records to be accessible to outside parties. Even now, the main issue with IoT use in healthcare is security. The cloud-based patient data was also used by IoT-based health diagnostic systems, which also notified the patient in the event of unusual findings. In these kinds of IoT, data transmission that is not secure results in incorrect diagnoses and may even cause patient deaths [2]. IoT security issues will lead to erratic behaviour in the smart health system. Several IoT health applications are listed below.

- Heart Monitoring and reports: Using IOT technology, the Heart Rate Monitoring system was designed to detect the patient's heartbeat and track the risk of a heart attack in addition to regular checkups [6]. Monitoring our bodies is essential to ensuring that our health is optimal. Heart rate (HR) is a crucial measure for the technology that is being discussed.
- Medical Alert System: It is recommended that patients wear pulse rhythm monitoring devices, which can detect high blood pressure [9]. When testing and inspections are necessary, healthcare providers may be able to view the reporting of patient tracking findings.
- Wireless Sensors: In labs and hospital refrigerators, wireless monitors are used to maintain the proper temperature for blood samples, cold medications, and other biological items [11].

The primary goal of this research project is to develop a safe framework for smart health care that is effective, lightweight, and capable of detecting numerous attacks while maintaining patient privacy and secure health information exchange. The following are this study's primary contributions.

- Secure communication in Smart IoT based Health System using a machine learning algorithm.
- Framework for detecting attacks by extracting features. Based on the feature value the classification is performed.

The following is the paper's outline. Some related work is provided in Section 2. Section 3 provides evidence of a thorough security and privacy system. Section 4 discusses current wearable technology,

followed by Section 5's discussion of the findings and Section 6's conclusion.

Related works

IoT-based remote patient status management system [4], which removes wait times in hospital billing systems and incorporates health-monitoring functions. The proposed system aims to integrate a creative, intelligent, and efficient health application from start to finish, which may be built using two useful building blocks [3]. But the primary job of the first building block is to gather all sensory data associated with patient monitoring; the second block's job is to store, process, and display the information that is produced on the server so that physicians can view health reports based on the cases of the patients who are being monitored. The IoT-based smart edge system for remote health monitoring described in [5] uses wearable vital sensors to send data to two innovative software engines that we have integrated into the IoT smart edge: Criticality Measure Index (CMI) alerts and Rapid Active Summarization for Effective PROgnosis (RASPRO) alerts. Massive volumes of sensor data are transformed by RASPRO into Personalised Health Motifs (PHMs), which are summaries that are therapeutically relevant. A total criticality score is produced by the CMI alerts engine. This IoT smart edge provides a risk-adjusted protocol that incorporates best-effort retrieval of detailed data-on-demand (DD-on-D) via the cloud and a rapid guaranteed push of alarms and PHMs straight to physicians. In order to determine if smart dental Health-IoT systems based on deep learning, intelligent hardware, and mobile terminals are viable for application in in-home dental healthcare, a proposal for a system is made [16]. Additionally, a smart dental device is designed and developed in this work to facilitate the gathering of tooth images [12]. An automatic diagnosis model is trained and created for the identification and categorization of seven different dental disorders, such as dental plaque, decaying teeth, and gum disease, based on a data set of 12,600 clinical photographs obtained by the proposed device from ten private dental clinics. The Internet of Things (IoT) improves the effectiveness of the healthcare system, however IoT-based smart health monitoring systems have numerous issues [7]. The Health Care Monitoring System (HCMS) includes wearable monitoring, remote control capabilities, and Internet connection at the patient's location [8]. To increase the effectiveness and security of HCMS, there are a number of challenges that must be overcome with each of these components. The primary flaw in current methods is their intricacy, which makes low power Internet of Things nodes unsuitable. The adoption of such technologies in the Internet of Things will result in increased energy usage at every node. The majority of the current techniques are ineffective for attack identities that more than one rogue node could display.

Roposed Work

IoT integration in smart health poses security issues with regard to privacy, integrity, authentication, and other issues. IoT-based smart health care systems are vulnerable to numerous assaults. The main objective of this project is to safeguard Smart-Health apps from different types of threats by implementing a secure architecture. To defend S-Health against three distinct threats, a framework known as the Multi Attack Detection Framework (MADF) based Multi class Support Vector Machine classifier based Random Forest algorithm [13][10][14] is created.

In this work, the polynomial component supplied by is mapped to information,

$$F_{x,x} = (x.x + 1)\,k \qquad (1)$$

where k is the kernel parameter and x and x are the training vectors. The amount of information, processing vector is $250 * 6$.

Assume a "n" dimensional pattern (object) x with "n" coordinates by using a relaxed classification error bound.

$$X\{X_1, X_2 \dots \dots \dots X_N\}$$

Bringing the training set T of "m" patterns to class,

$$T = \{(X_1.Y_1), (X_2.Y_2) \dots \dots \dots . . (X_m.Y_m)\} \qquad (2)$$

The patterns are integrated into a dot product space 'S',$X_1, X_2 \dots \dots \dots X_m \in S$. Any hyper plane in the space can be labeled as

$T = \{(X_1.Y_1), (X_2.Y_2) \dots \dots \dots (X_n.Y_n)\}$ (3)

Once a certain number of trees have been fitted, the training and test errors often level off.

$(X_1, Y_1), (X_2, Y_2), \dots (X_n, Y_n)$ (4)

In the case of probability (and probability distributions), Y is the class label of X. Let the training data be rearranged so that, given a norm on a point,

$\|X_{(1)} - x\| \leq \cdots \|X_{(n)} - x\|$ (5)

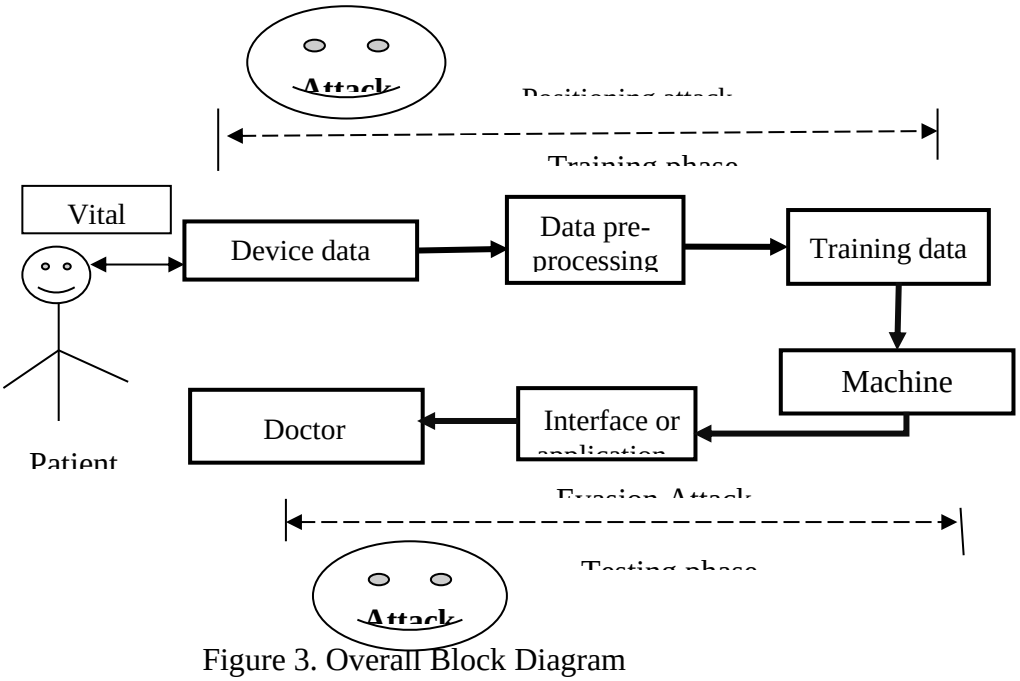

Figure 3. Overall Block Diagram

After training, predictions for unseen samples x' can be made by averaging the predictions from all the individual regression trees on x'

$\hat{f} = \frac{1}{B}\sum_{b=1}^{B} f_b(x')$ (6)

The SVM with RF classification is carried out using the Python programming language and Tensor Flow.

Results of Performance Experiments

Table 1 and 2 displays the findings of the examination of performance indicators for various attacks. From the table, it's important to note that the hybrid model produced the best performance results out of all the attacks taken into consideration.

Table 1. Performance metrics of attack detection

Models	**Accuracy (%)**	**Specificity (%)**	**Sensitivity (%)**	**F1-Score**	**Computational Time (sec)**	**Memory Utilization (%)**
SVM [8]	82.15	93	75	0.91	576.38	75.21

RF [9]	95	95.16	95.15	0.97	193.39	45.25
Proposed (SVM with RF)	97.7	98.05	97	0.96	95.92	47.90

Table 2. Performance metrics of attack detection

Models	Precision (%)	Recall (%)	Algorithm Complexity
SVM [8]	88.88	68.25	12.02
RF [9]	97	89.85	6.10
Proposed (SVM with RF)	99.15	91.05	4.22

The effectiveness of our suggested models was assessed using accuracy metrics. Our suggested model's accuracy was really satisfactory. Our Hybrid ML technique achieves 98.7% accuracy when compared to existing algorithms.

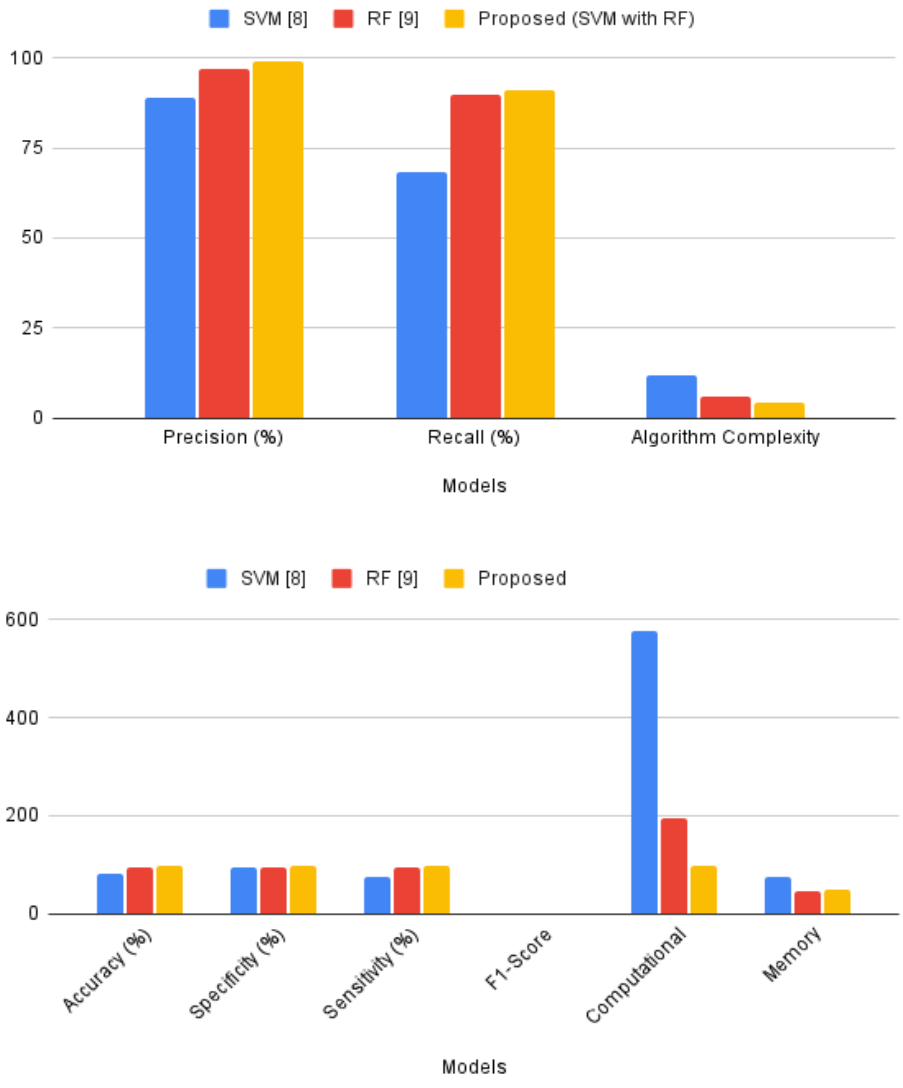

Figure 2. Performance plot

2. Conclusion and future scope

Technology is being used more and more every day. The need for technology in health has been apparent throughout this pandemic. The utilisation of medical services has increased as a result of the application of new technologies like the Internet of Things. IoT is protected by our architecture from the most frequent threats. The suggested approach employs two levels of machine learning algorithms for attack detection and securing mechanisms, security and privacy, low-cost access policies for SHRs (Smart Health Records), a lightweight detection scheme for the Internet of Things, and timely attack detection to lessen its impact on the network in order to protect S-Health from MITM attacks. According to simulation data, the suggested Hybrid ML performs better than current methods and has a higher attack detection rate overall

Reference

[1] Sabry, Farida, Tamer Eltaras, Wadha Labda, Khawla Alzoubi, and Qutaibah Malluhi. "Machine learning for healthcare wearable devices: the big picture." *Journal of Healthcare Engineering* 2022, no. 1 (2022): 4653923.

[2] Newaz, AKM Iqtidar, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A. Selcuk Uluagac. "Healthguard: A machine learning-based security framework for smart healthcare systems." In *2019 sixth international conference on social networks analysis, management and security (SNAMS)*, pp. 389-396. IEEE, 2019.

[3] Srinivasa Rao, M., Praveen Kumar, S., & Srinivasa Rao, K. (2023). Classification of Medical Plants Based on Hybridization of Machine Learning Algorithms. Indian Journal of Information Sources and Services, 13(2), 14–21.

[4] Pirbhulal, Sandeep, Nuno Pombo, Virginie Felizardo, Nuno Garcia, Ali Hassan Sodhro, and Subhas Chandra Mukhopadhyay. "Towards machine learning enabled security framework for IoT-based healthcare." In *2019 13th international conference on sensing technology (ICST)*, pp. 1-6. IEEE, 2019.

[5] AlZubi, Ahmad Ali, Mohammed Al-Maitah, and Abdulaziz Alarifi. "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques." *Soft Computing* 25, no. 18 (2021): 12319-12332.

[6] Stephen, K. V. K., Mathivanan, V., Manalang, A. R., Udinookkaran, P., De Vera, R. P. N., Shaikh, M. T., & Al-Harthy, F. R. A. (2023). IOT-Based Generic Health Monitoring with Cardiac Classification Using Edge Computing. Journal of Internet Services and Information Security, 13(2), 128-145.

[7] Chidambaranathan, S., and R. Geetha. "Deep learning enabled blockchain based electronic heathcare data attack detection for smart health systems." *Measurement: Sensors* (2023): 100959.

[8] Mohamed, K.N.R., Nijaguna, G.S., Pushpa, Dayanand, L.N., Naga, R.M., & Zameer, AA. (2024). A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 94-108. https://doi.org/10.58346/JOWUA.2024.I2.007

[9] Bahalul Haque, A. K. M., Bharat Bhushan, Afra Nawar, Khalid Raihan Talha, and Sadia Jeesan Ayesha. "Attacks and countermeasures in IoT based smart healthcare applications." In *Recent Advances in Internet of Things and Machine Learning: Real-World Applications*, pp. 67-90. Cham: Springer International Publishing, 2022.

[10] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. Archives for Technical Sciences, 2(29), 11-22.

[11] Newaz, AKM Iqtidar, Nur Imtiazul Haque, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A. Selcuk Uluagac. "Adversarial attacks to machine learning-based smart healthcare systems." In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2020.

[12] Kavitha R., et.al Stabilizing preserve and confidentiality in mobile cloud computing, Eurasian Journal of Analytical Chemistry, V-13, I-3, PP:982-988, 2018.

[13] Manimaran, M., Murali Dhar, Roger Norabuena-Figueroa, R. Mahaveerakannan, S. Saraswathi, and K. Selvakumarasamy. "Implementing Machine Learning-based Autonomic Cyber Defense for IoT-enabled Healthcare Devices." *Journal of Artificial Intelligence and Technology* 3, no. 4 (2023): 162-172.

[14] Thilagam, K., A. Beno, M. Vanitha Lakshmi, C. Bazil Wilfred, Santhi M. George, M. Karthikeyan, Vijayakumar Peroumal, C. Ramesh, and Prabakaran Karunakaran. "Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System." *Journal of Nanomaterials* 2022, no. 1 (2022): 2638613.

[15] Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.

[16] Saheed, Yakub Kayode, and Micheal Olaolu Arowolo. "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms." *IEEE Access* 9 (2021): 161546-161554.