

Machine learning for adaptive intrusion detection system towards secure internet of things enabled healthcare systems

Omar Isam Al Mrayat¹, Malik Jawarneh², D. Vettrithangam³, Pallavi Sunil Bangare⁴, Khaled Abdulwahab Zaid Alyamani⁵, Reema Goyal⁶, Sugumar Rajendran⁷, Shubham Kumar⁸, Yuvaraj Kunnathur Periyasamy⁹, Abhishek Raghuvanshi¹⁰

¹Department of Software Engineering, Amman Arab University, Amman, Jordan

²College of Computer Science and Informatics, Amman Arab University, Amman, Jordan

³Department of Computer Science and Engineering, University Institute of Engineering, Chandigarh University, Punjab, India

⁴Department of Information Technology, Sinhgad Academy of Engineering, Pune, India

⁵Applied College, Abqaiq Branch, King Faisal University, Al-Ahsa, Saudi Arabia

⁶Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, India

⁷Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science (SIMATS), Saveetha University, Chennai, India

⁸Sharda School of Computing Science and Engineering, Sharda University, Greater Noida, India

⁹Department of Mechanical Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India

¹⁰Department of Computer Engineering, Mahakal Institute of Technology and Management, Ujjain, India

Article Info

Article history:

Received Apr 16, 2025

Revised Jul 23, 2026

Accepted Aug 20, 2026

Keywords:

Accuracy

Artificial neural network

Deep learning

Internet of things

Intrusion detection systems

Security privacy

ABSTRACT

Internet of medical things (IoMT) ties medical sensors, actuators, wearable, and communication technologies to provide an improved healthcare delivery process by means of constant patient monitoring and decision-making. The trend has resulted in an increase in its use because of the increasing prevalence of chronic diseases and aging, and the need to have cost-effective healthcare services. Nonetheless, the networks provided by the IoMT are prone to cyberattacks under the considerable threat as both process huge volumes of sensitive health data, and do not have the resources to do it. In this paper, the author suggests a new adaptive intrusion detection system (IDS) as a way to enhance the security of IoMT-enabled healthcare environments. The proposed model the pre-treats NSL-KDD dataset, filling gaps and transmitting nominal values. Particle swarm optimization (PSO) is used in the optimal selection of features and artificial neural network (ANN), K-nearest neighbors (KNN), and random forest (RF) classifiers are used in intrusion detection. Experimental performance proves that the PSO-ANN model can perform better with a high accuracy of 99.54%, sensitivity of 99.31% and specificity of 97.32% on average with high protection of intelligent healthcare systems.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Abhishek Raghuvanshi

Department of Computer Engineering, Mahakal Institute of Technology and Management

Ujjain, India

Email: abhishek14482@gmail.com

1. INTRODUCTION

Internet of medical things (IoMT) is an emerging highly technical application of the internet of things (IoT) to medicine that connects medical devices, surfaces (sensors) and healthcare systems with the use of the internet so as to offer clever tracking of both patients and care organizations. IoMT assists in ensuring the continuity of collecting, transmitting and processing of medical data and allows healthcare professionals to track patients and monitor them outside the clinic and provide them with timely clinical care.

It has already become a fundamental part of modern healthcare since it assists to resolve patient outcomes, enhance operational efficiency, and entail the application of evidence-based medical decision-making [1], [2].

One of the key applications of the IoMT is remote patient monitoring where sensors are connected to continually measure one or more vital physiological parameters (heart rate, blood pressure, body temperature, blood glucose, oxygen saturation, electrocardiogram (ECG) signal). The resulting data are transported via wireless communication networks into platform based on clouds in healthcare to enable the physicians to access the information regarding patients in real-time. The latter skill can be utilized particularly in chronic diseases such as diabetes, high blood pressure, cardiovascular diseases, and asthma where continuous monitoring can be of immense importance to identify patients at a tender age and treat them accordingly. By integrating wireless sensor networks, cloud computing and artificial intelligence, it becomes possible to provide even superior healthcare services with predictive analytics and personal recommendations on treatment [3], [4].

The increase in chronic diseases, the ageing population and the urge to make healthcare cheap have led to the increased use of networked healthcare technologies [5]. IoMT can be used with the majority of healthcare services, e.g., telemedicine, home care, aging, emergency management, and rehabilitation. IoMT enables effective information exchange and a coordinated approach to medical care due to the unhindered flow of communication with all patients and healthcare providers, hospitals, and diagnostic laboratory. Additionally, big data collection of the patient information helps in medical research, predicting diseases, and planning healthcare provision evidence-based [6], [7].

The common intrusion detection model in the context of the IoMT healthcare systems includes the process of network traffic and malware data gathering, then, data processing and feature extraction to enhance the model. These common components are shown in Figure 1. The artificial data are analyzed by applying machine learning and deep learning algorithms to categorize normal and malicious activities. The trained models continue to observe the network traffic, detect anomalies on-the-fly and issue security alerts thereby enhancing the maximum confidentiality, integrity, and availability of healthcare information. Smart intrusion-detection systems are hence crucial to well-run, resilient, and secure IoMT-based healthcare settings [8], [9].

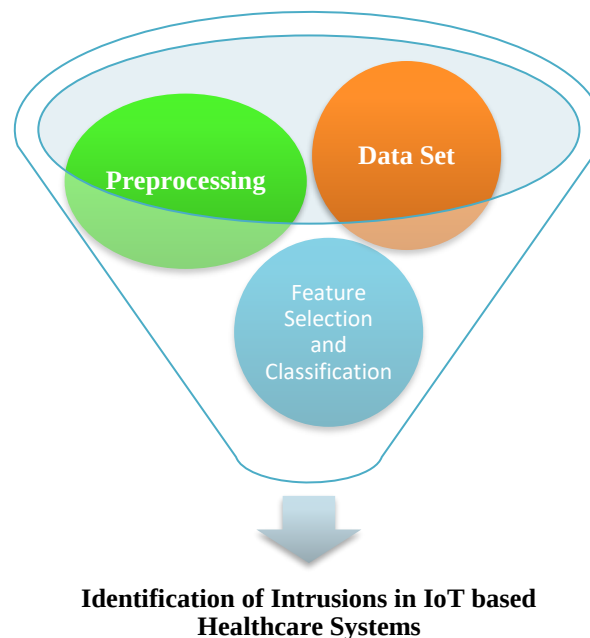


Figure 1. Intrusion detection in IoT based healthcare systems

2. LITERATURE SURVEY

Intrusion detection systems (IDSs) the signature based IDS seeks to alert when malicious activity is detected by comparing traffic across a network to signature of attacks that have been defined and are stored as attack signatures in a database of well known attacks. Such systems are quite efficient in detecting a low false alarm rate and threats, but are indeed unable to detect new attacks or attacks that have never been

observed before [10]. The other popular signature-based IDS is a program named Snort by Roesch whose Snort program is a network IDS in a lightweight that fits well in a resource constrained environment. Snort applies a matching algorithm known as pattern matching algorithm suggested by Boyer-Moore as a technique of matching the incoming traffic with known attack signature. The algorithm works well especially when the attack patterns are different and non-overlapping. The major deficiency of signature-based methods however is that it often needs the metadata to be updated with a new cyber threat by updating the signature database. To enhance the computational efficiency of attack-detection in IoT devices, scholars have suggested optimized pattern-matching engines with auxiliary tool of shifting and early decision that decrease unnecessary matching procedures and decrease the amount of computing overhead [11].

Concrete IoT-specific IDS frameworks have been sped up due to the special security considerations of resource limited devices and heterogeneous network structures. An IDS architecture has also been presented in 6 low-power wireless personal area networks (6LoWPAN) to thwart a host of cyberattacks of the low-power IoT networks [12]. Updates to the existing IDS systems such as the popular Suricata to allow them to be more efficient in detecting attacks deployed in IoT applications have also been undertaken by other researchers [13]. The performance of supervised intrusion detection models however, is highly dependent on the quality and diversity of the training data. False alarms risks will be enormous [14] in case the normal operation of the network is not adequately represented by the training data. Moreover, some protocols like the constrained application protocol (CoAP) which are heavily used in IoT speak need specific security mechanisms due to their lightweight structure and large-scale implementations of the protocol.

Anomaly based, in contrast, to signature based systems, IDSs that work on the basis of an anomaly will build an example of normal network behavior, and compare any abnormality with that example. These systems are able to detect the unknown attacks but are more prone to have false positives. In a number of studies some methods of anomaly detection have been suggested to detect botnet attacks in 6LoWPAN gateways using network traffic behavior [15], [16]. Other researchers have proposed sinkhole authentication methods to routing protocol for low-power and lossy networks (RPL) but the methods generally consume a lot of power, and there are lots of false alarms [17]. There are also statistical methods that have been used to detect network traffic entropy based and fuzzy logic model based DDoS attacks using the entropic method with better accuracy [18], [19]. This kind of hybrid intrusion detection framework has been more recently suggested as being based fundamentally on game theory and security information and event management, as well as machine learning techniques, to provide efficient, adaptive, and intelligent security solutions to resource-constrained, resource based IoT environments at an acceptable computational cost [20]–[24].

3. METHOD

This section presents a machine learning based methodology for intrusions detection in IoT based healthcare systems. It is shown in Figure 2. In this framework, input data set is preprocessed to handle missing values and encode categorical elements. Features are extracted by particle swarm optimization (PSO) technique. Classification is performed by artificial neural network (ANN), K-nearest neighbors (KNN) classifier, and random forest (RF) decision tree classifier.

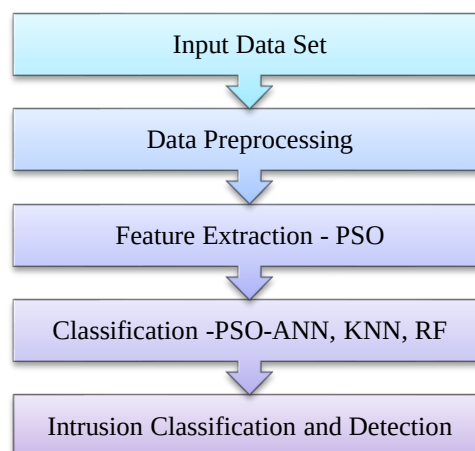


Figure 2. A machine learning framework for intrusion detection in IoT based healthcare systems

The illustration in the framework indicates a methodical procedure in searching intrusion in healthcare systems on the IoT with the use of machine learning. The IoT-based healthcare systems are dependent on devices and sensors that are interconnected to collect and share real-time information. These systems, as much as they offer several advantages in health monitoring, also pose chances of vulnerability and security risks owing to their enormous levels of interconnectivity and sharing of data among themselves. This framework is an attempt to safeguard such systems through machine learning that is capable of detecting and identifying intrusions. We are going to go through each of the steps one by one.

3.1. Input data set

The initial step in the framework is to get the input data set. The quality and relevancy of input data is the most important in the functioning of any machine learning model, and IDS are not an exception. When it comes to healthcare systems based on the IoT, the dataset usually includes the information received by different sensors, actuators, and communication devices, which are a part of the network. They might contain the following information:

- Network traffic data: the packets exchanged on the IoT network, which have the potential to hold sensitive information regarding health.
- Sensor readings: sensor data refers to the readings of medical devices like heart rate monitors, glucose meters or smart thermometers.
- System logs: the records of the IoT devices or servers that document which operations and interactions take place between system components.
- Health data: information revolving around the health conditions of the patients, including blood pressure levels, ECG, and other vital statistics that can be compromised by cyberattacks.

This data is normally raw and it may contain noise, missing values as well as inconsistencies which can influence the output of IDSs. As such, it has to undergo preprocessing to make sure that only the information that is relevant is utilized in the subsequent steps.

3.2. Data preprocessing

The data preprocessing is an important process through which the raw input data is prepared to be processed into features and classified. Preprocessing stage solves the problem of universal data in the real world and pre-processes it before the machine learning algorithms. Data preprocessing in the context of intrusion detection in the IoT-based healthcare systems is aimed at achieving the following key objectives:

- Handling missing values: most real-world data contains missing or partial values. Losses of values may occur due to sensor failures, dropped network packets, or not all the activities may be logged. Imputation (replacing missing values with statistical estimates, e.g., mean, median, and mode) techniques or data deletion (eliminating rows that have missing values) techniques are used.
- Data normalization: IoT sensor data can be highly scaled, and such high variability might result in some features dominating in the model training process. Normalization is done to bring the features to a certain range (normally 0 to 1) to make certain that all the features are given equal contribution to the learning process of the model.
- Categorical encoding: there are lots of IoT datasets, which have categorical data (e.g., the type of device and user ID) that must be converted to numerical values prior to being inputted into machine learning models. Categorical variables are processed by common encoding methods, such as one-hot encoding or label encoding.
- Noise reduction: IoT data can be noisy because of the environmental condition or sensor error. To reduce noise and preserve meaningful data trends, filtering and smoothing methods, e.g., moving averages or signal processing methods, are frequently used.

Through preprocessing, the dataset is tidied and standardized, meaning that the next processing phases in the framework will be done on a trustworthy and consistent data.

3.3. Feature extraction-particle swarm optimization

The process of feature extraction is done by PSO after preprocessing. In machine learning, feature extraction refers to a process of converting raw data to a collection of useful features that have the potential to enhance the performance of the model. The relevance of different features can vary in the intrusion detection case, and it is necessary to select the most appropriate features to detect possible threats [23].

PSO is one of the optimization algorithms that use social behavior of a flock of birds, or school of fish. PSO is a method applied to find the best combination of features through the simulation of a population of candidate solutions (particles) which traverse the feature space. Individual particles consider the quality of the solution (i.e., the chosen features) of the chosen particle and reevaluates position based on its previous best position and the global best position of any particle in the swarm. PSO helps in:

- Reducing dimensionality: discovering a few important features (including features that are not necessarily the most important) in the data.
- Improving efficiency: overall, as the PSO chooses only the most important features, it minimizes the complexity of the computation involved in the classification models.
- Enhancing model accuracy: the model becomes more accurate and the chances of overfitting are minimized by concentrating on the pertinent features.

A set of features which can be used to effectively classify the input data to detect intrusions is the output of this stage.

3.4. Classification-PSO-ANN, KNN, and RF

The second step is classification wherein the obtained features are subjected to machine learning classifiers to determine possible intrusions. There are three classification algorithms applied in this framework:

- PSO with ANNs

PSO-ANN is a superior hybrid algorithm, which incorporates the optimization capability of PSO and the learning ability of ANN. PSO is an optimization algorithm based on nature which simulates the social process of birds or fish to search the solution space. In PSO-ANN, the weights and biases of the ANN are optimized by the use of PSO which improves the capability of the network in making correct predictions.

The main purpose of such combination is to enhance the training of ANN. The training of ANNs is usually performed by means of such methods as backpropagation, which can also have such drawbacks as they can lead to local minimum. This is overcome by PSO which directs the neural network to an optimal solution on weight optimization across the globe. PSO particles (or candidate solutions) will either change their positions sequentially depending on personal experiences and also depending on the best solutions of the swarm resulting in more effective weight convergence.

This optimization increases the overall performance of the ANN, which is also highly effective in identification of elaborate patterns, including intrusions in IoT-based healthcare systems [25]. PSO-ANN not only improves the accuracy but improves sensitivity (the ability to be able to detect positive cases correctly) and specificity (the ability to detect negative cases correctly). Consequently, PSO-ANN is better suited to the task when high accuracy and the potential to deal with complex patterns of data are essential, like those of intrusion detection and cybersecurity.

The network in ANN network structure usually has three layers:

- Input layer: the input layer is where the input features are received by the data set. In the example of intrusion detection, they may be such features as network traffic information, sensor measurements or system logs.
- Hidden layers: hidden layers are the layers that are used to carry out calculations on the input data with the help of weighted connections. Several layers (deep learning) are employed to represent non-linear relationships that are of complex nature. The amount of the hidden layers and the number of neurons in each layer is typically determined by experiment.
- Output layer: this is the final output layer that will give the result or prediction as to whether the data is an intrusion or not.
- KNN is a simple classification algorithm which is effective. The principle of it is the label of a data point, which depends on the majority vote of its closest neighbors in the feature space. KNN comes in handy specifically when it is required to detect the known forms of intrusion with similar patterns to similar ones that have been previously observed [26]. In KNN, K is a parameter that is used to give the number of nearest neighbors to use in the making of a classification decision. Given a particular data point, KNN forms the difference distance of the data point with the rest of the data points in the feature space and makes a classification, based on the majority class of the KNN. The smaller K value results in a sensitive model to noise whereas the higher the K value, the more results are generalized. In most cases, the optimum K value is determined through a cross-validation technique.
- RF is a type of ensemble learning that is based on numerous decision trees and integrates the results of those trees. It works well with large datasets with high-dimensionality and offers a robust performance even in the event of noise or overfitting [27]. RF has very many trees in the forest, and the performance of the model greatly depends on this number. A RF is trained on a random subset of the data, and the end result is the classification decision is made by combining the predictions of all the trees (e.g., with majority ruling in classification tasks). This is because, increasing number of trees usually increases the accuracy of the models as it decreases the overfitting and variance creating stronger and generalized forecast. Nevertheless, excessively large trees may not bring about any meaningful performance benefits as they may rise in computation complexity.

These classifiers are all trained and evaluated with the features obtained above and their performances are checked in terms of accuracy, sensitivity and specificity.

3.5. Intrusion classification and detection

The last phase is intrusion classification and detection whereby the classified data is applied to determine whether an intrusion has taken place. According to the outcomes of the classification phase, the system will show whether the ongoing activity or data stream can be considered evidence of an intrusion attempt, including illegal access, suspicious data patterns, or possible attacks against IoT devices.

This step typically involves:

- Alert generation: once an intrusion is spotted, then an alert is generated to alert the system administrators of the suspicious activity.
- Response actions: response measures may be undertaken, including blocking out intrusion or secluding compromised offenses, depending on the severity of the intrusion.

The IDS is constantly watching the IoT healthcare network and adjusts the detection mechanisms according to the new information, thus making the system robust and resilient to new threats.

4. RESULTS AND DISCUSSION

NSL KDD data set [28] is used as an input data set. This data set consists of 125973 instances and 41 features. 80% records are used to train the deep learning model and rest 20% is used to test and validate the model. In this framework, input data set is preprocessed to handle missing values and encode categorical elements. Features are extracted by PSO technique. Classification is performed by ANN, KNN classifier, and RF decision tree classifier. For instance, a study applying PSO for feature selection on the NSL-KDD dataset identified 10 features that significantly reduced the false alarm rate and enhanced detection accuracy. These features include: protocol type, service, flag, duration, source bytes, destination bytes, hot, num failed logins, logged in, and num compromised.

Sensitivity:

$$\text{Sensitivity} = \frac{TP}{(TP+FN)}$$

where TP stands for true positive and FN stands for false negative.

Specificity:

$$\text{Specificity} = \frac{TN}{(TN+FP)}$$

where TN stands for true negative and FP stands for false positive.

Accuracy:

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

From Figure 3, it is clear that ANN clearly outperforms both KNN and RF across all evaluation metrics, making it the most effective model for intrusion detection in this comparison. RF offers a solid balance and is a good alternative if computational simplicity or interpretability is a concern. KNN, while decent, is the least effective among the three and may be more suited for simpler or smaller-scale problems.

Table 1 illustrates the performance of three machine learning models of KNN, RF and PSO-ANN with regard to three performance metrics, that is, accuracy, sensitivity, and specificity. KNN has an accuracy of 91.32%, a sensitivity value of 95.25% and specificity value of 92.13%. This implies that KNN is effective in identifying positive cases (high sensitivity), but the sensitivity and specificity of the model are relatively low compared to the rest.

An accuracy of 94.73% represents an improvement of RF. Both its sensitivity 95.75% and specificity 96.12% values are large indicating that the model is not only effective in correctly categorizing positive instances, but also effective in correctly categorizing negative instances.

PSO-ANN performs better than KNN as well as RF with an accuracy of 99.54%, sensitivity and specificity of 99.31% and 97.32% respectively. The PSO-ANN model has proven to be more effective in all metrics, especially the accuracy and sensitivity, which means that it is quite strong in the aspect of ranking in the right direction, both positive and negative cases. To conclude, the three models have high level of performance, but PSO-ANN has higher accuracy and balanced sensitivity and specificity.

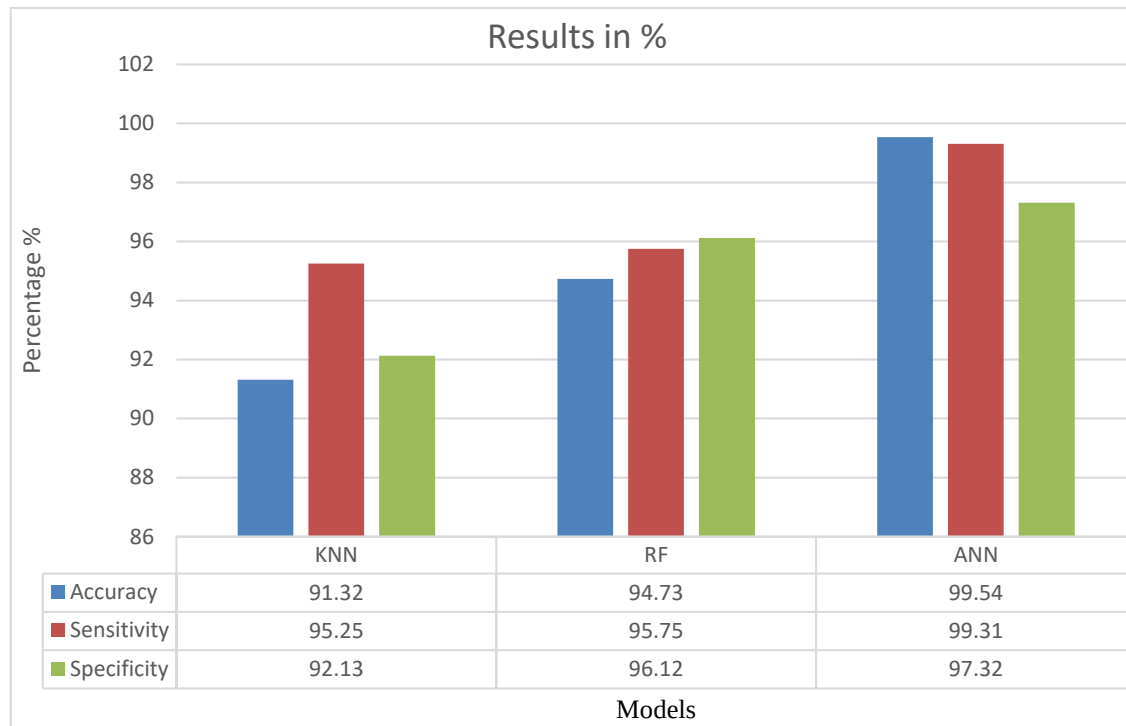


Figure 3. Result comparison of classifiers for intrusion detection in IoTs based healthcare systems

Table 1. Result comparison of machine learning models

Model	Accuracy	Sensitivity	Specificity
KNN	91.32	95.25	92.13
RF	94.73	95.75	96.12
PSO-ANN	99.54	99.31	97.32

5. CONCLUSION

The dependability and safety of the functioning of IoT-enabled applications is paramount, particularly in the context of large networks. As the links between IoT devices increase, the security of communications between the two is of the highest priority. One of the major problems of the IoT systems is the guarantee of safe data transmission which is critical towards preserving the integrity and secrecy of the information. This paper introduces an adaptive IDS that is targeted to secure the IoT-enabled smart healthcare systems. The suggested methodology will involve input datasets and deep learning algorithms in which NSL KDD dataset will be used as an input dataset in training. The model uses three machine learning algorithms namely, ANN, KNN, and RF, all of which aid in the detection of possible intrusions. The testing has revealed that ANN model is much better than the other algorithms with greater accuracy, sensitivity, and specificity to detect intrusion, which improves the security of the IoT-enabled healthcare applications.

It is the contribution of this paper that has led to the creation of a strong IDS of IoT healthcare systems, feature extraction using PSO, and a comparative analysis of the various classification algorithms. This work can be further developed as a future direction with the addition of real-time data streams, further research of more sophisticated deep learning methods, and the application of the system in a variety of healthcare settings to further consider its scalability and efficacy in the practical implementation.

ACKNOWLEDGMENTS

We are deeply thankful to our institutions for providing the necessary resources and facilities that enabled the successful completion of this research.

FUNDING INFORMATION

No funding received for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Omar Isam Al Mrayat	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	
Malik Jawarneh		✓				✓		✓	✓	✓	✓	✓		
D. Vetrithangam	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	
Pallavi Sunil Bangare	✓	✓		✓		✓		✓	✓	✓			✓	
Khaled Abdulwahab		✓				✓		✓	✓	✓	✓	✓		
Zaid Alyamani														
Reema Goyal	✓	✓	✓	✓		✓	✓			✓	✓		✓	✓
Sugumar Rajendran	✓		✓	✓	✓	✓		✓	✓	✓			✓	
Shubham Kumar	✓		✓	✓	✓	✓	✓		✓	✓	✓		✓	
Yuvaraj Kunnathur	✓			✓		✓		✓	✓	✓			✓	
Periyasamy														
Abhishek Raghuvanshi		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : **O**riginal Draft

E : **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

- [1] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, and M. El Bakkali, "An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system," *Results in Engineering*, vol. 23, pp. 1–17, Sep. 2024, doi: 10.1016/j.rineng.2024.102659.
- [2] A. Al Abdulwahid, "Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models," *Computational Intelligence and Neuroscience*, pp. 1–15, Nov. 2022, doi: 10.1155/2022/2037954.
- [3] A. Raghuvanshi, U. K. Singh, and C. Joshi, "A review of various security and privacy innovations for IoT applications in healthcare," in *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*, Wiley, 2022, pp. 43–58, doi: 10.1002/9781119769293.ch4.
- [4] W. Meng, W. Li, and L. Zhu, "Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management against Insider Attacks," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1377–1386, Nov. 2020, doi: 10.1109/TEM.2019.2921736.
- [5] Y. K. Saheed and M. O. 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*, vol. 9, pp. 161546–161554, 2021, doi: 10.1109/ACCESS.2021.3128837.
- [6] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020, doi: 10.1109/ACCESS.2020.3026260.
- [7] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services against External Attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/TII.2020.3011444.
- [8] M. K. Hasan *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Communications*, vol. 16, no. 5, pp. 421–432, Mar. 2022, doi: 10.1049/cmu2.12301.
- [9] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.
- [10] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, Jan. 2013, doi: 10.1016/j.jnca.2012.09.004.
- [11] D. Oh, D. Kim, and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the internet of things," *Sensors*, vol. 14, no. 12, pp. 24188–24211, Dec. 2014, doi: 10.3390/s141224188.
- [12] S. F. Aghili, M. Ashouri-Talouki, and H. Mala, "DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT," *Journal of Supercomputing*, vol. 74, no. 1, pp. 509–525, Jan. 2018, doi: 10.1007/s11227-017-2139-y.
- [13] A. Merlo, E. Spadacini, and M. Migliardi, "IPS-based reduction of network energy consumption," *Logic Journal of the IGPL*, vol. 24, no. 6, pp. 982–995, Dec. 2016, doi: 10.1093/jigpal/jzw053.

Machine learning for adaptive intrusion detection system towards secure internet ... (Omar Isam Al Mrayat)

- [14] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013, doi: 10.1016/j.adhoc.2013.04.014.
- [15] D. Zhao *et al.*, "Botnet detection based on traffic behavior analysis and flow intervals," *Computers and Security*, vol. 39, pp. 2–16, Nov. 2013, doi: 10.1016/j.cose.2013.04.007.
- [16] J. Kim, R. Haw, E. J. Cho, C. S. Hong, and S. Lee, "A 6LoWPAN sensor node mobility scheme based on proxy mobile IPv6," *IEEE Transactions on Mobile Computing*, vol. 11, no. 12, pp. 2060–2072, Dec. 2012, doi: 10.1109/TMC.2011.240.
- [17] M. Y. Tabari and Z. Mataji, "Detecting Sinkhole Attack in RPL-based Internet of Things Routing Protocol," *Journal of AI and Data Mining*, vol. 9, no. 1, pp. 73–85, 2020, doi: 10.22044/jadm.2020.9253.2060.
- [18] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement*, New York, New York, USA: ACM Press, 2005, pp. 345–350, doi: 10.1145/1330107.1330148.
- [19] S. Ramakrishnan and S. Devaraju, "Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language," *International Journal of Fuzzy Systems*, vol. 19, no. 2, pp. 316–328, Apr. 2017, doi: 10.1007/s40815-016-0160-6.
- [20] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, vol. 32, pp. 228–241, Jun. 2014, doi: 10.1016/j.engappai.2014.02.001.
- [21] D. Lavrova and A. Pechenkin, "Applying correlation and regression analysis to detect security incidents in the internet of things," *International Journal of Communication Networks and Information Security*, vol. 7, no. 3, pp. 131–137, Apr. 2015, doi: 10.17762/ijcnis.v7i3.1375.
- [22] B. Agarwal and N. Mittal, "Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques," *Procedia Technology*, vol. 6, pp. 996–1003, 2012, doi: 10.1016/j.protcy.2012.10.121.
- [23] N. N. P. Mkuzangwe and F. V. Nelwamondo, "A fuzzy logic based network intrusion detection system for predicting the TCP SYN flooding attack," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10192, pp. 14–22, 2017, doi: 10.1007/978-3-319-54430-4_2.
- [24] L. Santos, C. Rabadao, and R. Goncalves, "Intrusion detection systems in Internet of Things: A literature review," in *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, Caceres, Spain: IEEE, Jun. 2018, pp. 1–7, doi: 10.23919/CISTI.2018.8399291.
- [25] L. Mahmoud and R. Praveen, "Artificial Neural Networks for detecting Intrusions: A survey," in *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Bangalore, India: IEEE, Nov. 2020, pp. 41–48, doi: 10.1109/ICRCICN50933.2020.9296181.
- [26] K. Taunk, S. De, S. Verma, and A. Swetapadma, "A brief review of nearest neighbor algorithm for learning and classification," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India: IEEE, May 2019, pp. 1255–1260, doi: 10.1109/ICCS45141.2019.9065747.
- [27] Z. Bingzhen, Q. Xiaoming, Y. Hemeng, and Z. Zhuho, "A random forest classification model for transmission line image processing," in *2020 15th International Conference on Computer Science & Education (ICCSE)*, Delft, Netherlands: IEEE, Aug. 2020, pp. 613–617, doi: 10.1109/ICCSE49874.2020.9201900.
- [28] M. H. Zaib, "NSL-KDD," [www.kaggle.com](https://www.kaggle.com/datasets/hassan06/nslkdd), [Online]. Available: <https://www.kaggle.com/datasets/hassan06/nslkdd>, (Accessed: Apr. 09, 2025).

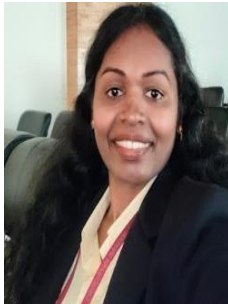
BIOGRAPHIES OF AUTHORS



Dr. Omar Isam Al Mrayat     is a faculty in the Department of Software Engineering, Amman Arab University, Amman, Jordan. His research interests are machine learning and educational data mining. He can be contacted at email: o.mrayat@aau.edu.jo.



Malik Jawarneh     is associate professor in College of Computer Science and Informatics, Amman Arab University, Amman, Jordan. He has a large number of research publications in reputed journals. His research areas are machine learning, healthcare analytics, and deep learning. He can be contacted at email: M.jawarneh@aau.edu.jo.



D. Vettrithangam    is working as a professor in the Department of Computer Science and Engineering at Chandigarh University, Punjab, India. She has more than 17+ years of experience in teaching and research, and has published more than 90 research papers in various Scopus- and SCI-indexed journals and conferences and edited books, chapters. She is currently working in image processing, deep learning, machine learning, the internet of things, and remote sensing for various applications, including medical imaging, disease detection and prediction, cancer detection, soil moisture, and climate change. She has published books and book chapters, holds 12 published patents and 1 grant patent, and has more than 5 design granted patents. She also guides Ph.D. and M.E. research scholars working in machine learning, deep learning, explainable AI, and wireless sensor networks. She can be contacted at email: vetrigold@gmail.com.



Dr. Pallavi Sunil Bangare    is faculty in Department of Information Technology, Sinhgad Academy of Engineering, Pune, India. She is having a vast experience in teaching, research and administration. Her research areas are machine learning, deep learning in educational, and health care data analytics. She can be contacted at email: pallavi.bangare@gmail.com.



Khaled Abdulwahab Zaid Alyamani    is faculty in Applied College, Abqaiq Branch, King Faisal University, Al-Ahsa, Saudi Arabia. He is having a versatile profile in academia and research. Research areas are AI and machine learning applicability in educational mining, and business management. He can be contacted at email: kalyamani@kfu.edu.sa.



Reema Goyal    is associate professor in Department of Computer Science Engineering in Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, India. She can be contacted at email: reemagoyal01@gmail.com.



Dr. Sugumar Rajendran    is professor in Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science (SIMATS), Saveetha University, Chennai, India. He can be contacted at email: sugu16@gmail.com.



Dr. Shubham Kumar    is faculty in Department of Computer Science and Engineering in Sharda School of Computing Science and Engineering, Sharda University, Greater Noida, India. He can be contacted at email: shubham.kumar5@sharda.ac.in.



Dr. Yuvaraj Kunnathur Periyasamy    is working as an assistant professor in Department of Mechanical Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India. He can be contacted at email: cadyuva99@gmail.com.



Abhishek Raghuvanshi    is working as Professor in Department of Computer Science and Engineering in Mahakal Institute of Technology Management in Ujjain in India. He is having teaching experience of 21 years, research experience of 17 years and administrative experience of 12 years. His research areas include- machine learning, internet of things security, and health care analytics. He is having many publications in SCI and Scopus indexed journals. He has also worked on many governments of India funded research projects. He can be contacted at email: abhishek14482@gmail.com.