A review of AI-Driven Anomaly Detection for Real-Time Monitoring of IoMT Networks

H.P. Theekshana Sahan Jayawardhana
Department of Computer System Engineering
Srilanka Institute of Information Technology
SLIIT Malabe Campus, New Kandy Rd,Malabe
theekshanasahan10@gmail.com

Abstract - Modern healthcare practice underwent transformation through the Internet of Medical Things (IoMT) which established real-time patient monitoring while permitting remote diagnosis and automated medical choices. However, the rapid expansion of IoMT Rapid expansion of IoMT networking systems has created new security vulnerabilities that expose patients to catastrophic threats such as cyber-attacks as well as unauthorized network intrusions and data breaches. The emerging nature of cyber-attacks against IoMT infrastructure exceeds the capabilities of traditional security approaches that use rule-based IDS and signature-based anomaly detection. Real-time security needs receive effective protection through AI-based anomaly detection that leverages ML and DL algorithms to study network traffic and find anomalous patterns while making threat predictions. The application of supervised and unsupervised and hybrid learning AI models enables IoMT security solutions to find both known and unknown attacks while building new attack pathway mappings in real time.

AI-driven anomaly detection for IoMT functions effectively yet faces significant challenges associated with data privacy and limited computing resources and AI model vulnerability to evasion attacks. When security systems utilize AI algorithms for IoMT devices which have limited computational power engineers must choose between powerful predictive capabilities or software scalability. Recent advances in AI-driven anomaly detection focus on utilizing three methods including federated learning and explainable AI in addition to feature selection techniques to improve IoMT security. Future research should work on enhancing real-time threat detection alongside false alarm reduction and automatic security solutions for the dynamic cybersecurity environment.

Index Terms— Internet of Medical Things (IoMT), AI, Anomaly Detection, IoMT Networks, Real-Time Monitoring, Healthcare IoT, Cybersecurity in IoMT

I. INTRODUCTION

Internet of Medical Things (IoMT) has revolutionized healthcare through its capability to monitor patients in real-time and make decisions based on evidence and conduct remote diagnostics. Wearable sensors together with intelligent medical devices and cloud healthcare platforms have enhanced both the patient care's delivery efficiency and its availability. The evolution of patient healthcare produces extraordinary cybersecurity and privacy complications when massive volumes of sensitive digital health information travel between connected medical devices. Modern cyber threats alongside data breaches ransomware denial-of-service (DoS) attacks and adversarial AI exploits now bypass traditional IDS intrusion detection systems and rule-based security systems due to their reduced efficiency in cybersecurity[1]. IoMT devices face two main difficulties: their limited processing resources create security risks which makes it impossible to apply advanced protection systems.

AI-driven anomaly detection models, fuelled by the advancements of machine learning (ML) and deep learning (DL), have emerged as remarkable solutions for pinpointing network irregularities and alleviating cyber threats in real time.These models harness the power of pattern recognition and adaptive learning, enabling them to identify security anomalies before they can escalate into full-scale attacks. This literature review examines state-of-the-art AI-driven anomaly detection techniques in IoMT security, contrasting supervised, unsupervised, and hybrid models for network traffic pattern recognition and response to cyber-attacks. It also addresses main challenges, such as data privacy, computational overhead, adversarial attacks, and high false positive rates, and outlines directions for future research towards enhancing IoMT security, regulatory compliance, and patient safety in an evolving healthcare landscape. [3]

II. RESEARCH OBJECTIVE

The research investigates how AI technologies detect anomalies in IoMT network systems. The utilization of advanced techniques in Internet of Medical Things networks enhances protection through better security performance. security, reliability, and threat management. It examines several AI techniques, including The detection methods include supervised together with unsupervised and hybrid AI models detecting anomalous network behavior and preventing cyber-attacks. It also discusses some of the significant challenges, such as serious data privacy concerns, computational resources, adversarial attacks, and high false positive rates, Several problems exist which reduce the operational success of current anomaly detection systems..By evaluating current methodologies, this research highlights significant The research investigates present gaps in knowledge through new hypotheses about innovative security models. [5] [6]

future advancements in AI-based security models. The development aims to create accurate and lean AI systems which maintain privacy specifications. The research focuses on developing privacy-protected AI models that will enhance security measures. Threat monitoring occurs in real-time under compliance standards with healthcare regulations, thereby improving IoMT security and patient safety.

III. REVIEW OF THE LITERATURE

A. The Evalution of IoMT Security

The development of medical technology alongside the increasing prevalence of cyberattacks caused Internet of Medical Things device security to transform over time. For medical devices in the past did not exist as part of networked systems since they operated independently and attacks were minimal.

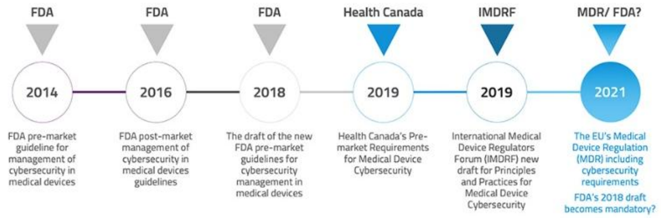
FDA
2014
FDA pre-market guideline for management of cybersecurity in medical devices
FDA
2016
FDA post-market management of cybersecurity in medical devices guidelines
FDA
2018
The draft of the new FDA pre-market guidelines for cybersecurity management in medical devices
Health Canada
2019
Health Canada's Pre-market Requirements for Medical Device Cybersecurity
IMDRF
2019
International Medical Device Regulators Forum (IMDRF) new draft for Principles and Practices for Medical Device Cybersecurity
MDR/ FDA?
2021
The EU's Medical Device Regulation (MDR) including cybersecurity requirements
FDA's 2018 draft becomes mandatory?

Figure 1: Evolution of Medical Device Security in IoMT Era

Security attacks began to happen when hospitals started using networked systems as well as internet-based medical devices. Strong defense systems became essential after this transition because cyberattacks threatened both patient wellness and medical information confidentiality. [7]

1.Early Security in Medical Technologies

Medical equipment worked independently during early times as hospital network connectivity was not needed for X-ray machines ECG monitors and infusion pumps. The medical equipment provided assistance to medical staff for diagnosing patients and delivering treatments without requiring systems-based interaction. [8], [9]The devices that functioned independently from hospital networks operated offline.

Medical professionals and hospitals of the 1990s to early 2000s failed to recognise that cybersecurity would become a significant challenge. Medical devices did not hold sufficient value to attract hackers, resulting in their omission of fundamental security measures like updated software and secure password protocols.Multiple medical devices included factory-set passwords which remained unalterable by users, thus making them vulnerable access points for cyber attackers. The practice of monitoring medical device access remained inadequate, which led to an increased potential for internal threats.

2.Advancement of Connected Healthcare Systems

During the mid-2000s the capabilities of Hospital IT networks increased thus enabling better medical device connectivity that improved efficiency and patient care delivery[11]. Medical institutions started implementing Electronic Health Records (EHRs) as they provided healthcare providers simple access to patient files Medical devices along with hospital networks developed new vulnerabilities to security threats immediately following their interconnection.

Cyber attackers use interconnection to breach patient-sensitive data because systems are linked together. Remote patient monitoring systems combined with wireless technology that connects medical devices to the internet made cyberattack risks surge enormously.

The interception of heart monitor along with insulin pump medical device information by attackers creates a threat to patient safety.

B. Models for Real-Time Anomaly Detection

The Internet of Medical Things (IoMT) utilizes real-time anomaly detection to identify security risks together with system failures alongside atypical medical data trends. Anomaly detection models make medical devices connected to networks secure while maintaining their reliability to protect against cyberattacks along with operational risk reduction. [13]

The core technologies supporting IoMT network security comprise two main components: rule-based systems with XAI (Explainable AI) as the second foundational model. Rule-based systems have simple anomaly detection processes and XAI creates trustworthy systems that analyze AI-based anomaly detection frameworks.

1) Rule-Based Systems

Cybersecurity implements rule-based systems as one of its initial and simplest anomaly detection methods. These systems function by applying pre-established rules and conditions which extract their threat information from known patterns of attacks. Any networking behavior that breaches a single condition within the predefined ruleset results in marking it as susceptible to anomalies. [14]

The main advantage of rule-based systems arrives from their clear operational features and minimal computational power needs which benefits resource-scarce IoMT devices.

2) Explainable Artificial Intelligence

Explainable AI (XAI) represents an effective solution which unites accuracy standards with human-understandable explanations of model operations. The purpose of XAI techniques is to generate simple explanations which humans can comprehend regarding AI model predictions. The detection of anomalies in real-time together with interpretation of reasons is achievable by doctors alongside IT professionals and decision-makers within the healthcare and cybersecurity fields. [15] ,[16]XAI facilitates improved trust and responsibility which allows stakeholders to make confident decisions making use of insights from AI systems with better understanding.

The integration of AI in anomaly detection is with high predictive power but also with a lack of transparency owing to its complexity. Explainable AI (XAI) remedies this by offering interpretability, where healthcare workers and cybersecurity specialists can

comprehend and have faith in AI-based anomaly detection systems.

C. IoMT Network Risks and Challenges

Internet of Medical Things (IoMT) network protection stands imperative for healthcare functionality because healthcare operations are directly affected by this network infrastructure as well as patient safety and secure medical data storage. IoMT networks face multiple security threats which create both device vulnerabilities for medical devices across networks and database exposure vulnerabilities. Multiple security

The complexity of security challenges rises because medical devices in IoMT work through extensive network connections. [11]. [13] This evaluation focuses on three main safety threats affecting IoMT networks which result from device vulnerabilities as well as network-layer attacks together with persistent data integrity vulnerabilities.

1) Security Flaws in IoMT Devices

Secure design principles are hindered at IoMT devices as they operate with limited processing ability and run unfinished software and have weak authentication systems in place. Cyber-attacks easily find their entry points due to these medical devices being easily vulnerable to online intrusions[15]

Limited Computational Power: The processing power of IoMT devices stays limited because manufacturers install low-power processors for both energy conservation and operational cost reduction. The economical manufacturing decision results in reduced functionality for complex security operations on these devices. Several IoMT devices lack sufficient computing capability to perform real-time encryption and secure data transfer along with intrusion detection operation needed to safeguard patient care information. These restrictions make these devices incapable of using modern security protocols and therefore they become susceptible to cyberattacks including advanced attacks which exploit these security weaknesses.

Outdated Software and Firmware: Security problems in IoMT devices stem mainly from keeping substandard software versions or allowing their firmware components to become outdated and inadequately supported. The failure to update devices makes their software both outdated and susceptible to attacks. The continuation of many IoMT devices operating from legacy systems on unmaintained outdated software platforms falls under the term sustaining engineering because manufacturers discontinue support after End of Life (EOL). These patient data breaches along with other cyber attacks are carried out by hackers who exploit vulnerable information.

Lax Authentication and Authorization: Most internet of medical things devices present problems due to their insufficient authentication protocols and access security measures. The security problem allows unapproved persons and attackers straightforward access to medical devices and their related networks which creates serious concerns. The authentication methods employed by IoMT devices frequently depend on basic default passwords together with naive authentication protocols. [19]Insufficient security measures in systems enable attackers to edit protected medical records as well as seize control of the device. Such minimal security measures put patients at risk while threatening the breakdown of device operation.

Data Transmission without Encryption: The unencrypted nature of data transmission stands out as the main safety concern for IoMT devices. The transfer of patient-related confidential data occurs through inadequate protection networks on many medical devices. The absence of secure data transmission makes these devices vulnerable to both MITM attacks and data interception faults. Unauthorized individuals who get access to these data can both modify it and steal or misuse it. Patient confidentiality violations through such acts lead to detrimental outcomes when identity criminals steal patient data and modify critical medical information.

Vulnerable Communication Protocols: Security features are missing from IoMT devices and systems which employ Wi-Fi and Bluetooth and ZigBee communication protocols. Such unsecured devices face vulnerabilities through different types of attacks including unauthorized intrusions and overhearing exposing privileged data. [20]

Security weaknesses in these systems allow both illegal control usurpation of devices and data monitoring during their information transfers. These systems face security threats due to malicious actions which include both personal data theft as well as modifications of normal device operations and data corruption and also enable remote device control resulting in privacy risks.

D. Anomaly Detection in IoMT

AI cybersecurity tools are currently integrated into IoMT systems across the connected healthcare domain. Security monitoring systems today utilize deep learning algorithms to detect anomalous activities continuously which activates security protocols in advance. These systems prioritize three essential elements which consist of data protection for patients and system reliability as well as accessibility and trustworthiness. [21]

1) Supervised Learning Methods

Supervised learning systems operate with tagged information where they initially identify normal along with abnormal patterns ahead of time.The methodology uses historical data to train itself in correct case classification.

SVM: The Support Vector Machines (SVM) method operates best when processing high-dimensional medical databases through hyperplane discrimination of normal versus abnormal patterns. The model targets binary classification duties proficiently and therefore works for detecting cybersecurity risks in IoMT systems.

RF: Random Forest (RF) builds its framework from multiple decision trees which collectively predict for better accuracy during classification. RF demonstrates strong resistance against overfitting so healthcare providers often use it to track medical patient data and detect outliers in biomedical sensors.

DT: Decision trees utilize hierarchical models through data partitions which depend on significant feature values to assist anomaly classification. [10]Decision trees enable clear decision-making and perform effectively at identifying untypical patterns in the network traffic of IoMT devices. [19]

2) Unsupervised Learning Methods

The machine learning process using unsupervised learning techniques enables algorithms to learn by analyzing data which has no corresponding outputs.

The model training in unsupervised learning operates on unlabeled data whereas supervised learning uses labeled input-output pairs for its training process. The model needs freedom to discover valuable data patterns and cluster relationships without human intervention. Such methods demonstrate great value when we have no clear expectations about hidden patterns in the data which makes unsupervised learning an ideal tool for exploratory analysis. [15], [16]

K-Means Clustering: Using K-Means Clustering similar data points will group according to feature similarities and separate outliers by placing them as distant points. The technique serves the healthcare sector by identifying both discriminatory sensor outputs and exceptional patient bodily patterns.

Principal Component Analysis: PCA successfully reduces data dimensions through maintaining important data variance until it reaches large-scale IoMT databases to identify anomalies. PCA identifies untypical patterns that may appear in ECG traces and MRI scans alongside imaging diagnosis methods.

Autoencoders: The results of learned neural network structures used to encode standard data allow the classification of deviations as probable anomalies. Autoencoders find high utilization in identifying cybersecurity attacks and machine faults and patient abnormal states that exist within IoMT networks.

3)Deep Learning Approaches

Deep learning analyzes complicated dataset patterns by using neural networks structured in stacked multiple layers known as deep neural networks. The organization of learning models utilizing human-like network arrangements allows them to process larger data sets.

All hardware data passes successively through Feedforward Neural Network (FNN) network layers until achieving basic prediction outcomes. The distinctive structure of CNNs allows them to recognize complex patterns at every image level starting from edges up to object identification which makes CNNs suitable for

visual applications. RNN databases use their looping structure to store memory which allows them to handle time-based patterns together with sequence-based data analysis.

As an enhanced RNN version LSTM addresses dependency retention problems to work effectively in speech recognition and language translation tasks. GANs function by operating as data generating systems through two neural networks known as generator and discriminator to establish an adversarial battle that results in authentic new information creation.

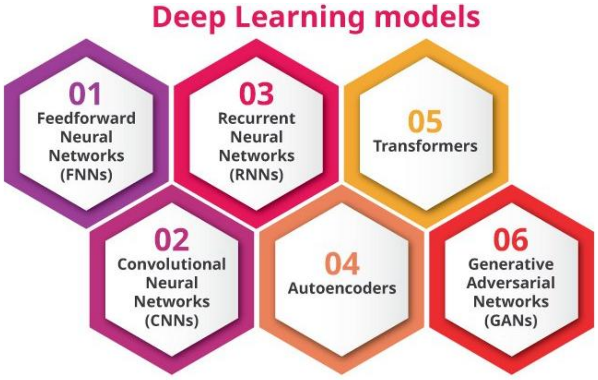
Deep Learning models
01
Feedforward Neural Networks (FNNs)
03
Recurrent Neural Networks (RNNs)
05
Transformers
02
Convolutional Neural Networks (CNNs)
04
Autoencoders
06
Generative Adversarial Networks (GANs)

Figure 2 : Deep Learning Models

Convolutional Neural Networks: The Convolutional Neural Networks (CNNs) excel at processing spatial data since they work efficiently with medical imaging and bio signals. The system learns hierarchical features through which it identifies irregularities in X-rays as well as MRI and CT scan images while enhancing diagnostic outcomes.

Recurrent Neural Networks: Repeat networks offer optimal capabilities for processing spatial medical data including imaging scans and body signal devices. The detection of anomalies in X-rays and MRI scans and CT scans becomes more accurate with the hierarchical features learned by these networks.

Long Short-Term Memory Networks (LSTMs): Medical data with long-term dependency learning is possible through the complex recurrent neural network design known as Long Short-Term Memory Networks (LSTMs).

IV. FUTURE RESEARCH

New solutions are needed to secure dependable anomaly detection since the number of advanced IoMT devices continues to grow. Through studies of specific relevant fields researchers should create superior security models through artificial intelligence. Further research needs to establish artificial intelligence models that work effectively with minimum size constraints.

AI standard models cannot meet real-time processing demands on most IoMT devices because they operate under memory storage power restrictions coupled with limited computational resources. The development of efficient resource-saving machine learning and deep learning algorithms needs additional research to achieve peak accuracy results. Researchers need to conduct tests which combine model pruning techniques with quantization algorithms and knowledge distillation methods to optimize efficiency in anomaly detection systems that preserve performance levels. [18]

Another potentially useful direction is federated learning, which has the promise of getting around data privacy concerns in IoMT networks. Typical AI approaches need to centralize data for training the model, which creates additional security and privacy concerns. Federated learning allows AI models to be trained locally on IoMT devices without sending potentially sensitive medical information to distant servers. Future research needs to look at how federated learning may be implemented with IoMT networks with model accuracy, security, and adaptability for different healthcare settings in mind.

Advanced threat intelligence is another area that should be explored in the future. AI-based threat intelligence has the potential to predict, detect, and eliminate cyber threats in advance, before they impact IoMT systems. Future research needs to focus on developing AI models that can learn threat patterns in real-time, predict incident modes of cyberattacks, and increase incident responses. Automated threat detection systems, in combination with artificial-intelligence risk-assessment systems, could provide a good way to improve IoMT networks' resilience to emerging security threats. [20]

Ultimately, quantum AI could transform anomaly detection in IoMT networks. Quantum computing assures increased processing power that can improve AI performance as the improved processing capacity of AI models in computing will improve efficiency and faster real-time anomaly detection. Future studies will have to explore how quantum machine learning algorithms can be used in cybersecurity for IoMT with the aim of improving security algorithms, encryption algorithms and predictive analytics for threat detection. In conclusion, future studies of AI-based anomaly detection in IoMT networks will have to focus on efficiency, privacy, threat intelligence, and raw computation technology; once these issues have been resolved, researchers can build better performing, more secure, and highly scalable AI models to protect IoMT systems in real-world healthcare environments.

V. CONCLUSION

The use of AI-based anomaly detection for real-time IoMT network security monitoring represents a potential solution to the increased security challenges in healthcare. This review recognizes the promise of AI technologies and its ability to improve anomaly detection in IoMT devices. Specifically, these capabilities are threat detection, detecting abnormal patterns, and predicting cyberattacks. Some of the key areas that offer future research scope are: the development of light-weight AI models, the use of privacy based federated learning, and the integration of next generation threat intelligence frameworks. Quantum AI also has promising applications to improve anomaly detection for IoMT networks.

Future research must also include the elements of computational efficiency, privacy and developing cyber threats. Enhancements in AI capabilities and their incorporation into IoMT networks, will all contribute to an increase in healthcare systems resilience against cyberattacks, protect patient data, and facilitate seamless healthcare services. Therefore, Future research must entail the aspects to enhance model performance, preserve privacy, and dynamic provision of the healthcare environment to maintain security and patient safety.

ACKNOWLEDGEMENTS

The author would like to extend a sincere thank you to Mr. Kanishka Yapa for his help and support during the whole process of preparing this work. The author also expresses appreciation to the esteemed faculty and supervisors from SLIIT University for their guidance and encouragement, which has greatly benefitted the author's academic advancement and the development of his research. The author has greatly appreciated their comments and expertise, which have truly enhanced his learning and experience in the field.

REFERENCES

1) Lin, Y., & Huang, T. (2020). A Rule-Based Framework for Secure Medical IoT Systems. IEEE Access, 8, 181726–181738.

2) Adadi, A., & Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, 52138–52160.

3) Abdel-Basset, M., Manogaran, G., Mohamed, M., & Rushdy, E. (2021). Deep learning techniques for cybersecurity in IoT and IoMT: A survey. Journal of Information Security and Applications, 55, 103093.

4) Alshehri, M. D., Alghamdi, A. S., Alzahrani, B. A., & Muhammad, G. (2022). An AI-Based Anomaly Detection Framework for Enhancing IoMT Security. IEEE Access, 10, 14712–14722.

5) Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115.

6) Bisio et al., "AI-Enabled Internet of Medical Things: Architectural Framework and Case Studies," IEEE Internet of Things Magazine, vol. 8, no. 2, pp. 121–128, Mar. 2025,

7) L.Christodoulou, A. Chari, and M. Georgiades, "AIenhanced Healthcare IoT System: Advanced ML Detection and Classification Algorithms for Real-Time Cardiovascular Monitoring," pp. 440–449, Apr. 2024,

8) Sondes Ksibi, Faouzi Jaidi, and Adel Bouhoula, "IoMT Security Model based on Machine Learning and Risk Assessment Techniques," Jun. 2023,

9) Arun V, P. Shenbagavalli, Sridhar T, Manivannan B, M. T. R, and K Anitha, "Machine Learning Algorithms for the Detection of Threats in IoT Healthcare," Dec.

10) Mirza Akhi Khatun, Sanober Farheen Memon, C. Eising, and Lubna Luxmi Dhirani, “Machine Learning for HealthcareIoT Security: A Review and Risk Mitigation,” IEEE Access, vol. 11, pp. 145869–145896, Jan. 2023

11) Mohammadi, H. Ghahramani, S. A. Asghari, and M. Aminian, “Securing Healthcare with Deep Learning: A CNNBased Model for Medical IoT Threat Detection,” pp. 168–173, Oct. 2024,

12) S. D. Kafait, A. Tanseer, I. Tanseer, Z. Hassan, and F. Tanseer, “Securing the Pulse of Healthcare: A Survey of IoMT Security Challenges and AI-Powered Defenses,” 2024 International Conference on IT and Industrial Technologies (ICIT), pp. 1–6, Dec. 2024,

13) K. Ramesh, N. C. Miller, A. Faridi, F. Aloul, I. Zualkernan, and A. R. Sajun, “Efficient Machine Learning Frameworks for Strengthening Cybersecurity in Internet of Medical Things (IoMT) Ecosystems,” 2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), pp. 92–98, Nov.2024,

14) S. Pillai, S. S. Poddar, Y. Nagendar, Piyush Kumar Pareek, and P. Zanke, “Automated Cybersecurity Attack Detection Using Prairie Dog Optimization and Multilayer Perceptron in Healthcare System,” pp. 1–6, Apr. 2024,

15) J. A. P, A. Shankar, A. N. JR, P. Gaur, and S. S. Kumar, “Smart Non-Invasive Real-Time Health Monitoring using Machine Learning and IoT,” Dec. 2023,

16) Pragya Bajpayi, S. Sharma, and M. S. Gaur, “AI Driven IoT Healthcare Devices Security Vulnerability Management,” Mar.2024,

17) Rasheed, J. (2021). AI-Driven IoMT: Smart Healthcare for Real-Time Monitoring. Sensors, 1-17.

18) Reis Burak ARSLAN, C. a. (2022). A Wearable System Implementation of Internet of Medical Things, 1-4.

19) Sarma, R. (2021). Deep Learning for Anomaly Detection in Healthcare IoT. IEEE Access, 104485–104504.

20) Shitharth, S., & Durbha, S. (2021). An Efficient Lightweight Anomaly Detection Technique for IoMT Devices. Journal of Medical Systems, 1-12.

21) Conor Bronsdon, “F1 Score: Balancing Precision and Recall in AI Evaluation - Galileo AI,” Galileo AI, 2025.

22) S. Pogrebivsky, “Precision, Recall and F1 Explained (In Plain English),” DataGroomr.com, May 21, 2021.

AUTHOR PROFILE

H.P.Theekshana Sahan is a Cybersecurity undergraduate third-year student at Sri Lanka Institute of Information Technology (SLIIIT). In one of the academic modules called "Applied Information Assurance (AIA)", their academic focus includes anomaly detection, IoMT network security, and advanced threat intelligence. They aim to gain a wealth of knowledge for the development of intelligent and adaptive security frameworks for real-time threat detection in IoMT environments.

AIA_Resources Folder Link:

AIA Assignment