International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Study: Use of Machine Learning for Cyber Security

Nidhi Kataria Chawla[1], Monika Gaur[2]

[1]Assistant Professor, Computer Science & Engineering, B. S. Anangpuria Institute of Technology and Management, Faridabad

[2]Assistant Professor, Computer Science & Engineering, B. S. Anangpuria Institute of Technology and Management, Faridabad

Abstract: ***Machine learning is becoming prevalent in a variety of sectors, and machine learning algorithms are used in a variety of cyber security applications. Malware analysis, including zero - day malware detecting, risk evaluation, anomaly - based intrusion detection of common threats on critical systems, and other examples are just a few. Because signature - based methods are ineffective at detecting zero - day attacks or even slight modifications to existing attacks, researchers are employing machine learning (ML) - based identification in numerous security protocols. In this overview, we look at how machine learning is employed in several aspects of cyber - security. We also show how adversarial assaults on machine learning models can be used to change the data used to train and test models, rendering them useless.***

Keywords: Cyber security, machine learning, intrusion detection, malware detection

1. Introduction

A develop professionally networked society with extensive internet activity has evolved from the development of technology ranging from mobile phones to huge communication infrastructures. According to estimates, there are much more than 5 billion smart devices and 3 billion internet users on the planet today. Internet banking and purchasing, email, exchanging records or confidential material, video calls, and games, to name a few, all rely on this cyber connectivity. As a result, terabytes of data are created, processed, transferred, and saved every second by various appsin addition to the Internet of Things (IoT). In fact, 90 % of the data on the planet here come in the last two years alone, according to estimates [1]– [4]

Hackers and computer security professionals both use machine learning techniques in their attacks. On the cybercriminal side, ML approaches are being used by cyber attackers and criminals to uncover system flaws and to get through the security wall, you'll need to use advanced attack methods. On the security side, machine learning classifiers are helping to give more robust and intelligent strategies for improving work and early prediction of attacks, reducing the impact and the resulting damage [5]– [7]. To enhance the precision of accurate and early threat classification, machine learning techniques are coupled [8]– [10]. However, the majority of the research are conducted with an insufficient dataset. None of the studies looked into a full and integrated view of digital Smart phones and computer systems are vulnerable to risks and attacks.

We can list the following as key contributions of this survey article: Only three contributions will be merged and added.

- A description of the most common cyber security attacks and their countermeasures;
- A general summary of widely used ML and deep learning models;
- After a comprehensive classification using algorithms, extraction of features, and output map schemes, a survey of a wide variety of ML in cyber security is performed.;
- An overview of work on machine learning security (i. e., adversarial machine learning), covering the vulnerability of DL algorithms to malicious samples;

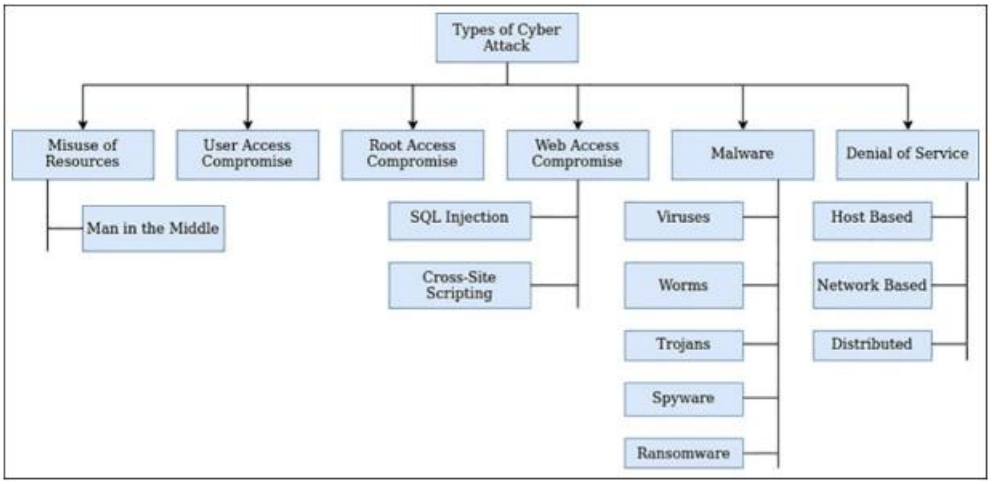

Figure 1: The taxonomy of cyber - attacks considered in this paper. [7]

The remaining sections of the paper are organized as follows. The second portion is a comprehensive evaluation of all key research on machine learning in cyber security from 2017 to 2021. A recommended methodology is presented in Section 3. The results and discussion are described in Section 4. Sections 5 and 6 discuss future research directions and conclusions, respectively.

2. Literature Review

An extensive overview of recent research on machine learning in cyber security is provided in this section. We additionally narrowed our search by taking into account algorithm details and efficiency, feature extractions and selection methods (if applicable), and the relevant dataset used to solve an issue. This document also includes a brief overview of all of the strategies.

Several publications have tackled this research area, with few describing the uses of introducing machine learning into domain of networking and others describing how specific machine learning models would be applied to a variety of networking challenges [11]. M. Wang tries to highlight the procedure, achievements, and potential for ML and Computer Networks in his paper [12]. He claims that using Machine Learning for Networking can aid in the resolution of old network questions/problems as well as the development of novel network applications. Because networks frequently encounter difficult challenges that necessitate quick solutions, ML would be a great contender for addressing this problem, as various powerful machine learning techniques can help. Machine Learning for Networks has a number of advantages, including improved decision - making, more general modeling, and approximated models of accuracy. M. Wang is able to provide a typical machine learning process for networks, which adequately and precisely specifies the phases involved. However, this method should be enhanced to account for a number of roadblocks to completely using machine learning in networking. Existing research in this area mainly focuses solely on lowering measurement costs, which is insufficient in the field of networking.

In his study [13], Bhutani says that by adding machine learning to networks, networks will be able to cope with the change and make judgments while still understanding about them. The authors explain that when it comes to wireless networks, They usually have to think about providing the best Quality of Experience (QoE) at the best cost while working with limited resources. They frequently have unreliable signal quality. ANNS, Naive Bayes (NB), and Logistic Regression (LR) [14] were highlighted in the study as common ML algorithms for wireless networks. While the majority of research has employed machine learning for solving various network difficulties, just a handful have taken into account how asset each of the machine learning algorithms is. Obtaining high quality of information for networking is also an issue, according to the study, because Techniques need an accurate model to prevent interruptions and resource waste.

M. Kulina et al. [15] analyzed the application of machine learning in networks by concentrating on the network layers protocol stack, whereas the other papers in this section discuss the uses of machine learning in networking. This post delves deeper into the technical aspects of applying machine learning to wireless technologies, which were not discussed in the previous sections. Signal - to - Noise ratio (SNR), latency, energy usage, and other performance measures are all used in wireless networks. Due to user needs and the variety of such wireless networks, modifying these parameters to obtain the appropriate performance is difficult. In such circumstances, machine learning can be utilized to predict trending patterns at various layers of a network. Similarly, our work aims to serve as a useful reference for newbies to the fields of AI and networking, as well as an empirical data - backed evaluation of various machine learning algorithms suitable for practitioners.

Elekar [16] advocated that different types of detecting attacks be accomplished utilizing various combinations of methods, such as J48 DT with such a combo of Random Forest, J48 with the Random Tree, and the Random Tree with Random Forest cooperation, to tackle the detecting rate problem. The combination of J48 and the Random Forest increased detection rates for DoS, U2R, and R2L attacks by 92.62 percent, with a low false positive rate for probing attacks.

Dash [17] presented a hybrid - based IDS where a neural network training was by using gravitational search (GS) and a combo of GS and particle swarm optimization (GSPSO), followed by the usage of the GS - ANN and GSPSO - ANN intrusion detection algorithms (). The authors compared their system to several optimization methods such as GA (genetic algorithm), PSO, and a GD - ANN (gradient descent - based ANN) to determine its effectiveness. This method, according to the author, is better for unbalanced datasets. The given technique obtained 94.90 percent and 98.13 percent accurate utilizing the GS and also GSPSO, respectively, on the NSLKDD dataset.

One of the most common reasons for IDS performance degradation is a "zero - day assault. " The zero - day assault has become a hot topic in cybersecurity since machine learning algorithms can't detect instances that aren't close to training data. To combat zero - day DDoS attacks, Saied et al. [18] offered the intriguing notions of "detection, defence, and cooperation mechanism. " The study was presented in two ways by the authors. To begin, they tested their strategy on old datasets that had not been updated with new attack types. A new dataset was used to test their strategy afterwards. The authors employed a JNNS (Java Neural Network Simulator) to process and preparation of dataset for training the classifier, which they created by performing many DDoS attacks. The authors compared their methods to Snort - AI and other relevant studies and discovered a 92 percent detecting accurately without addressing zero - day attack knowledge while employing up - to - date datasets, and a 98% detection accuracy. According to their findings, the more frequently detection of intrusion database is changed, the better the accuracy for unknown assaults.

For detecting unknown threats, Villaluna and Cruz [19] devised an cyber security system that performs marginally higher than Saied et al. [18]. The authors employed soft computing to identify zero - day attacks such that novel Assault characteristics are not misclassified, and they may be identified using some common characteristics. DoS, probing, U2R,

and R2L assaults can all be detected by their system. The authors compared the performance of fuzzy logic algorithm, ANN algorithm, and fuzzy based neural networks algorithm during network data analysis. According to their findings, the fuzzy based neural network algorithm takes less time to identify and performs better than the other two (96.19 percent accurately and 98.60 percent rate of detection) than the other two. The use of the ANN to detect threat in the cyber–physical world, environment has also been the subject of extensive research [4], [11]

For example, Kosek [20] suggested an anomaly detection technique for detecting fraudulent voltage control action in the low voltage grid. To identify the nature of control operations as well as any abnormalities in distributed energy resources (DERs), the technique used an artificial neural network (ANN). The proposed technique was tested in a co - simulated set - up testbed. In terms of anomaly control detection, the experimental outcome gave 56.00 % improved accuracy.

Teoh et al [21] released a work that employed Teoh et al's ANN for detection of malware, wherein the researchers used a semi - supervised learning methods to track malware. After extracting features from network data and assigning a weight to each feature, the authors analyzed the log history and developed a scaling technique. The FKM (fuzzy k - means) clustering approach is used to categorize the log history of network data into identified, unidentified, and attack classes. The authors examined their algorithmic performance using a private dataset and discovered that their solution had a lower false positive rate than traditional anomaly detection technologies. As Teoh et al [21] suggested, Saroare et al [22] offered a refined fuzzy based clustering technique that, if utilized, can increase the accuracy of identifying log history.

Table 1: Ansalysis and comparison of different studies with our paper
(legend: ● means covered; ≈ means partly covered; × meaning not covered).

S. No	Reference	Cyber Security							Machine Learning				
		Mobile Based			Computer Host / Network Based								
		Spam Detection	Malware Detection	IDS	Spam Detection	Malware Detection	IDS	Security Dataset	Technique	Matrix	Tool	Trustwor-thiness	Advance ML
1	[23]	×	×	×	×	×	×	×	≈	×	≈	×	×
2	[24]	×	●	×	×	●	×	×	●	×	●	×	×
3	[25]	×	×	●	×	×	×	×	●	×		×	×
4	[26]	×	×	×	×	●	×	≈	×	×	≈	●	×
5	[27]	×	≈	×	×	●	×	×	×	×	×	×	×
6	[28]	×	●	×	≈	≈	×	×	×	×	≈	×	×
7	[29]	×	●	×	≈	≈	≈	×	●	×	×	●	×
8	[30]	×	×	×	×	●	×	×	×	×	×		≈
9	[31]	×	×	●	×	●	×	≈	×	×	×	●	×
10	[32]	×	≈	×	×	×	×	×	×	×	×	×	×
11	[33]	×	×	×	×	×	×	×	●	×	×	×	≈
12	[34]	×	×	●	×	×	●	×	×	×	≈	●	×
13	[35]	×	×	×	×	●	×	×	≈	×			×

3. Proposed Framework

The suggested IoT–WBANs Cloud - based framework is presented in this section.

We suppose that the system has n. registered patients, P = {p1, p2,. . ., pn}. A unique identifier is assigned to each patient pi P. (pidi). We further suppose that every patient has access to a mobile phone with Global positioning system (GPS). As a result of their mobility, the location of the clients in Data storage on cloud computing is always changing.

Figure 2 shows the proposed structure for such a remotely patients' health condition surveillance system from a general view. The essential framework's recommended components are further as stated in the subsections that follow.

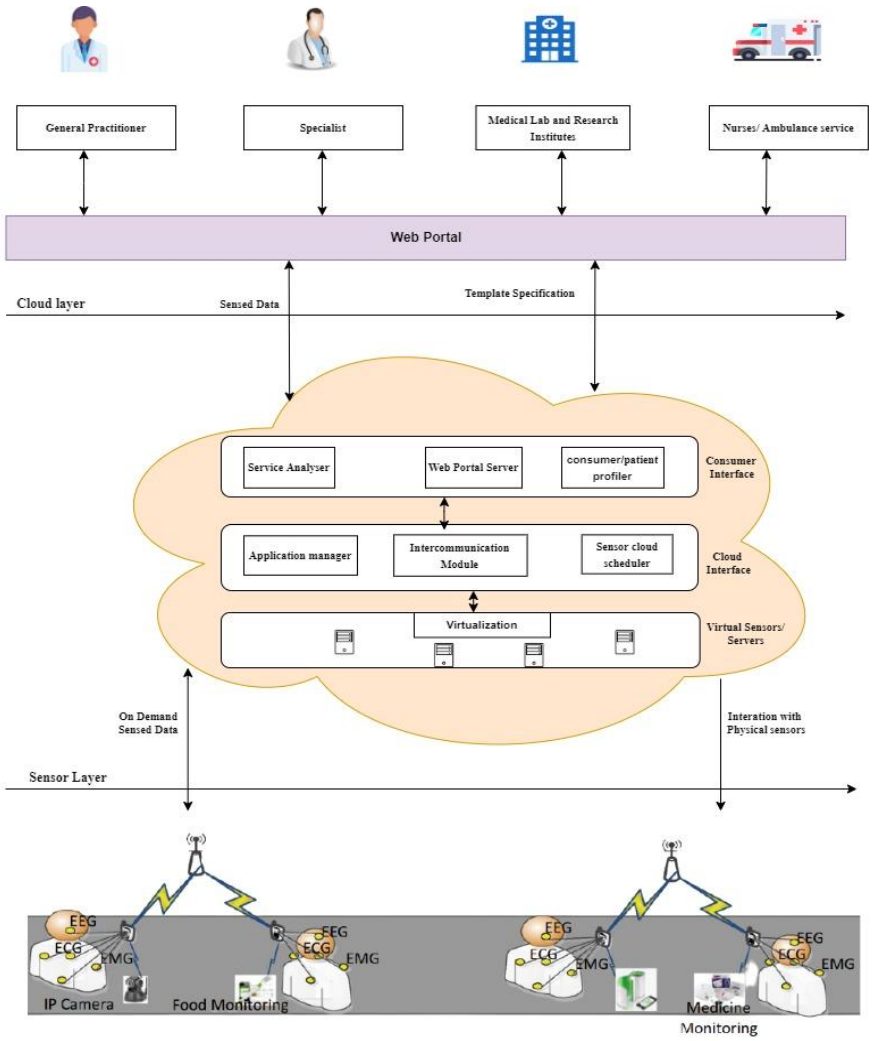

Figure 2: Framework for a cloud - based body area network

3.1 Platform layers

A user interface, a cloud interface, and a virtual sensor/server layer are all included. make up the proposed platform.

3.1.1 Layer of Consumer interface

Consumer and patient Profiler, Service Analyzer, and the Web server make up the consumer interface component. Consumers can log in and submit requests over the Web server. They can submit several applications for preset services by supplying information such as patient IDs and required data, as well as due timetables.

Service Analyser reads and examines the service needs of the consumers' application requested It is made up of a number of surveillance programs that are employed to gather and examine health data based on the existing condition of monitoring. The on - request monitoring procedure begins when Patients, doctors, and nurses, for example, are all authorized users of system, makes a request [36]. Finally, a process for periodic monitoring depending on a pattern with respect to periodic can be constructed.

3.1.2 Layer of Cloud

Application Manager, Intercommunication module, and an IoT– WBAN platform Scheduler make up the Cloud interface component. In short, the sensor - application Cloud's intercommunication module is at the heart of operational and judgement coordination between services [36]. Eventually, the IoT based WBAN platform Scheduler is in charge of prioritizing and scheduling the tasks to be completed. This layer's applications play a critical role in request scheduling. When an application submits a request, the apps also assign resources. It also maintains track of available resources so that they can be shared on the cloud through the Internet [10].

3.2 Layer of Sensor

The lowest layer of the healthcare monitoring system, there are two key procedures in this module. First method is concerned with data gathering section. During this section, Body sensor nodes are used to keep track of a patient's vital signs e. g blood pressure (bp), blood glucose, temperature, and so on. We suppose that enough sensor nodes are available, such as Electro - Cardio - Graphy (ECG), Electro - Myo - Graphy (EMG), motion sensor, temperature sensor, and so on. These devices of sensor can detect and process health information [37]. Other sensors obtain data besides vital signs, such as financial data, medication and food intake data, and IP cams for connecting with doctors.

The transmission phase is the subject of the second process. During this section, the monitored data that is monitored, is

transferred to the Cloud storage with a smart phone. Bluetooth based IEEE 802.15.1, ZigBee based IEEE 802.15.4, UWB based IEEE 802.15.6, and identification of radio frequency are all examples of IEEE 802.15.1 - based technologies are some of the sensor transportation protocols available (RFID). According to a study published in [14], [38], [39], communication methods like Bluetooth and Wi - Fi are insufficiently energy - efficient for usage in a wireless body area network. IEEE 802.15.4 is a grade, on the other hand, was created expressly for WBAN to facilitate less power and energy utilization.

3.3 Description of the framework used

This part show how suggested framework can be used in real - world applications. The major goal is to demonstrate the use of the framework's main components in situations when patients must be observed remotely. Despite the reality that cloud based On IoT framework can be used in in a range of medical situations, like identifying muscle anomalies in monitoring scheme, monitoring patients with Myopathy or Neuropathy disorders have focus in this study.

EMG, which stands for Electromyography, is a frequent test for diagnosing muscular neuropathy and myopathy [40]. Wireless EMG physical sensors are most likely to be linked with bodies of the patients. We have undergone with the assumption that smart phones that patients have, support IEEE 802.15.4 communication standard. Patients' personal record must be saved in the system. Their medical histories are included in their profile details, which are saved in an IoT - cloud database. The information about the patient is indexed using the patient's identifying number (ID).

The workflow for patient monitoring utilizing the proposed IoT - cloud platform is shown in Figure 3. Monitoring process of authorized users can be initiated in cloud by sending the requests i. e. application. The necessary data for various health applications is present on the Cloud already [10]. Following that, requested applications, each one of them, is reviewed and scheduled to guarantee that the module of virtualization in question is not overburdened by other submitted applications. The layer of virtualization provides an allocation between the virtual sensors (virtual) and actual nodes of detector once requests have been prioritizing and scheduled to be completed. The allocation procedure is based on the location of the patients. After the configuration is finished, the sensors begin collecting data to communicate to mobile telephone.

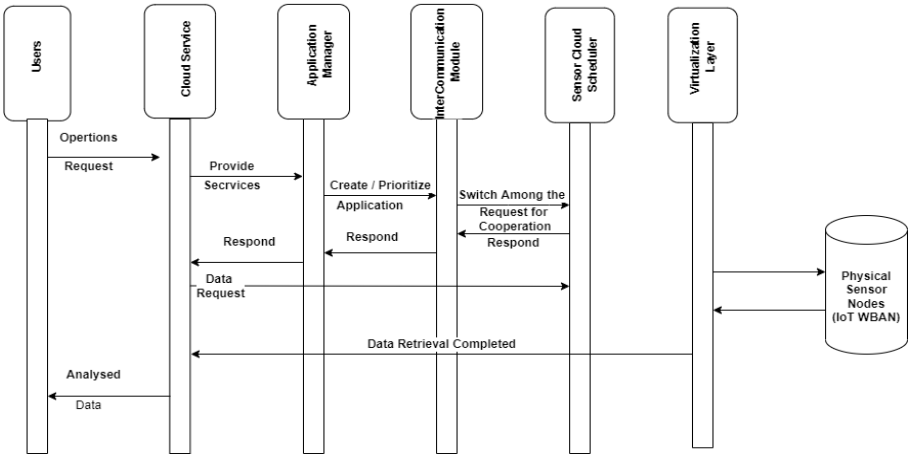

Figure 3: Workflow for remote based patient health condition monitoring via IoT cloud

The data will be sent from the phone to cloud based IoT, where the Cloud service module will process it. The sensor devices will be de - allocated after that, also made available for future applications. According to the suggested framework, the suggested WBAN in IoT based platform includes a cloud service component handles the majority of the computational calculations and decision - making. EMG signals, for example, are very tiny and require amplifiers so that it can be evaluated and displayed on a screen. High and low frequency disturbances, as well as any other elements that may have an impact on the data's conclusion, are likewise removed by the Cloud service.

Following that, the data would be analyzed on the Cloud service using a variety of approaches. For example, based on the difference between the measured value and a preset upper and lower limits value of the healthcare indicator, the system would automatically assess the sufferers' health state. If there is a significant difference between the patients' previous and already defined data, the condition can be categorized as critical. Because of system already connects emergency departments and ambulances, they may enrol for the resources they require right away.

IoT based WBAN platform's storage of data keeps track of the users' ids and health records data. Depending on the customer's service priority and/or the accessibility of doctors, the doctor may view the users' info as reqiured [41]. Simultaneously, automated notifications based on this data can be sent to his/her relatives via various telecommunication means. Using Cloud connectivity, medical staff's smart devices are able to show enhanced video streaming of mobile from remote based cameras.

3.4 Evaluation of Performance

The performance analysis strategy is examined and compared in this section with a conventional WBAN. Measuring performance in terms of energy consumption and the sensor nodes'

maximum probable life period. The suggested health monitoring system's deployment, maintenance, and rental expenses are also examined.

We assumed that the node's The128 bytes packet length and the transmission rate is 1Mbps. The speed provided by the 3G network to the WBAN is expected to just be 15 Mbps, according to [42]. Patients can either stay put or move around at random. The values were first assumed, and then updated using the trial - and - error process in order to achieve a clear and consistent result for each scenario.

We employed energy usage, monitoring network lifetime, and cost efficiency for performance measures to research and analyse the performance of the proposed framework properly, as they were used in [43] to evaluate QoS.

3.4.1 Energy consumption

The effectiveness with which monitoring systems consume energy is a critical component that can improve service quality. The following Equation. is used to compute a sensor network node energy usage (E).

$$E = Etr + Er + Es + EProc \quad (1)$$

In this model, the energy measures usage for WBAN and suggested IoT based WBAN platform are assumed to be the equal. When comparison with WBANs, an IoT - based WBAN platform reduces energy usage. This is due to a variety of factors. Intranet work communication in a WBAN begins with recurrent multi - hop communication, followed by packet transfer to a data centre.

Energy costs associated with transmission in an IoT–WBAN system, on the other hand, are mostly linked to reaching via multi - hop transmission to the cloud service. Because communication between sensor nodes is extremely infrequent, a significant quantity of power is saved. Furthermore, unlikely WBAN, even if a sensor network node is application compliant, it does not necessarily assist a user or organization. A collection of applied sensor nodes, on the other hand, can be employed for many applications under the suggested framework.

3.4.2 Lifetime of Sensor Node

In this approach, the lifetime of WBAN is specified by the period of time a sensor network node must perform until its remaining energy meets a predetermined energy value. The following equation [43] is used to compute the lifespan rate of a sensor network node:

$$Lt = t - (Er\ s - Eth) \times \tau \quad (2)$$
$$Ein$$

Where Er s is the sensor node's residual energy, Ein is the node's beginning energy, t is the sensor node's expected time to execute, and τ is the average time required for a node's functioning The sensor network node lifespan is calculated as the number of detecting operations it performs. It begins when it is deployed and continues until its leftover energy falls below the lowest attainable value.

When comparing the IoT devices' energy usage rates in WBAN and the suggested framework has a lower reduction in lifetime rate than WBAN. This is because packets are sent to data centres after multihop interactions. Energy usage in the suggested approach is primarily attributable to data transmission to the Cloud via multihop communication.

4. Conclusion

Machine learning and cyber security have gotten a lot of attention from academics and industry, resulting in a lot of publications, especially in the previous decade. By offering a complete examination of the crossings between the two disciplines, In this research, we were able to fill the gap between machine learning approaches and risks to computer technology and mobile connectivity. We provide an IoT - based system for analyzing patient health status inside this study, which connects WBAN to cloud services via smartphones. The suggested framework is location agnostic and enhances collaboration between various requested apps. It can also run multiple apps at the same time while collaborating on resources. Evaluation process revealed that the recommended design outperformed the regular WBAN by a significant margin. The suggested framework did not take security and privacy concerns into account. In the future, we want to resolve these concerns.

References

[1] S. Sarwar, S. Tahir, M. Humayun, M. F. Almufareh, N. Z. Jhanjhi, and B. Hamid, “Recommendation of Smart Devices Using Collaborative Filter Approach, ” in *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 2022, pp.1–4. doi: 10.1109/MACS56771.2022.10022407.

[2] M. F. Almufareh, S. Kausar, M. Humayun, and S. Tehsin, “A Conceptual Model for Inclusive Technology: Advancing Disability Inclusion through Artificial Intelligence, ” *J. Disabil. Res.*, vol.3, no.1, p.20230060, 2024.

[3] M. A. Al - Garadi, A. Mohamed, A. K. Al - Ali, X. Du, I. Ali, and M. Guizani, “A survey of machine and deep learning methods for internet of things (IoT) security, ” *IEEE Commun. Surv. \& Tutorials*, vol.22, no.3, pp.1646–1685, 2020.

[4] S. Naaz, “Detection of phishing in internet of things using machine learning approach, ” *Int. J. Digit. Crime Forensics*, vol.13, no.2, pp.1–15, 2021.

[5] T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security, ” *IEEE Trans. Neural Networks Learn. Syst.*, 2021.

[6] K. Geis, “Machine learning: Cybersecurity that can meet the demands of today as well as the demands of tomorrow, ” Utica College, 2019.

[7] N. Khan, B. Hamid, M. Humayun, N. Z. Jhanjhi, and S. Tahir, “Information Retrieval from Healthcare Information System, ” in *Computational Intelligence in Healthcare Informatics*, Springer, 2024, pp.107–125.

[8] N. Tariq, A. Alsirhani, M. Humayun, F. Alserhani, and M. Shaheen, “A fog - edge - enabled intrusion detection system for smart grids, ” *J. Cloud Comput.*, vol.13, no.1, pp.1–34, 2024.

[9] M. Thangavel, A. S. TGR, P. Priyadharshini, and T.

Saranya, "Review on machine and deep learning applications for cyber security, " in *Research Anthology on Machine Learning Techniques, Methods, and Applications*, IGI Global, 2022, pp.1143–1164.

[10] M. Humayun, A. Alsirhani, F. Alserhani, M. Shaheen, and G. Alwakid, "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency, " *J. Cloud Comput.*, vol.13, no.1, pp.1–21, 2024.

[11] A. Upadhyay, S. Naaz, V. Thakur, and I. R. Ansari, "Machine Learning Approach to the Internet of Things Threat Detection, " in *International Conference on Data Science and Network Engineering*, 2023, pp.407–418.

[12] G. Bhutani, "Application of machine - learning based prediction techniques in wireless networks, " *Int'l J. Commun. Netw. Syst. Sci.*, vol.2014, 2014.

[13] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, "Machine learning for networking: Workflow, advances and opportunities, " *Ieee Netw.*, vol.32, no.2, pp.92–99, 2017.

[14] M. Shaheen, S. M. Awan, N. Hussain, and Z. A. Gondal, "Sentiment analysis on mobile phone reviews using supervised learning techniques, " *Int. J. Mod. Educ. Comput. Sci.*, vol.11, no.7, p.32, 2019.

[15] M. Kulin, T. Kazaz, E. De Poorter, and I. Moerman, "A survey on machine learning - based performance improvement of wireless networks: PHY, MAC and network layer, " *Electronics*, vol.10, no.3, p.318, 2021.

[16] K. S. Elekar, "Combination of data mining techniques for intrusion detection system, " in *2015 International Conference on Computer, Communication and Control (IC4)*, 2015, pp.1–5.

[17] T. Dash, "A study on intrusion detection using neural networks trained with evolutionary algorithms, " *Soft Comput.*, vol.21, no.10, pp.2687–2700, 2017.

[18] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks, " *Neurocomputing*, vol.172, pp.385–393, 2016.

[19] J. A. Villaluna and F. R. G. Cruz, "Information security technology for computer networks through classification of cyber - attacks using soft computing algorithms, " in *2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*, 2017, pp.1–6.

[20] A. M. Kosek, "Contextual anomaly detection for cyber - physical security in smart grids based on an artificial neural network model, " in *2016 Joint Workshop on Cyber - Physical Security and Resilience in Smart Grids (CPSR - SG)*, 2016, pp.1–6.

[21] T. T. Teoh, Y. Zhang, Y. Y. Nguwi, Y. Elovici, and W. L. Ng, "Analyst intuition inspired high velocity big data analysis using PCA ranked fuzzy k - means clustering with multi - layer perceptron (MLP) to obviate cyber security risk, " in *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC - FSKD)*, 2017, pp.1790–1793.

[22] M. K. Saroare, M. S. Sefat, S. Sen, and M. Shahjahan, "A modified penalty function in fuzzy clustering algorithm, " in *2017 Intelligent Systems Conference (IntelliSys)*, 2017, pp.446–451.

[23] R. G. Mohammed, S. Tarek, E. Khaled, and M. Ausif, "Data Mining Based Network Intrusion Detection System: A Survey, " *Coll. Comput. Sci. Inf. Technol. Sudan Univ. Sci. Technol. Int. J. Eng. Adv. Technol.*, 2010.

[24] D. P. Vinchurkar and A. Reshamwala, "A review of intrusion detection system using neural network and machine learning, " *J. Eng. Sci. Innov. Technol*, vol.1, pp.54–63, 2012.

[25] M. Z. Mas' ud, S. Sahib, M. F. Abdollah, S. R. Selamat, and R. Yusof, "Analysis of features selection and machine learning classifier in android malware detection, " in *2014 International Conference on Information Science \& Applications (ICISA)*, 2014, pp.1–5.

[26] E. Gandotra, D. Bansal, and S. Sofat, "Malware analysis and classification: A survey, " *J. Inf. Secur.*, vol.2014, 2014.

[27] R. H. Jhaveri, A. Revathi, K. Ramana, R. Raut, and R. K. Dhanaraj, "A review on machine learning strategies for real - world engineering applications, " *Mob. Inf. Syst.*, vol.2022, 2022.

[28] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection, " *IEEE Commun. Surv. \& tutorials*, vol.18, no.2, pp.1153–1176, 2015.

[29] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods, " *IEEE Access*, vol.7, pp.51691–51713, 2019.

[30] R. Das and T. H. Morris, "Machine learning and cyber security, " in *2017 international conference on computer, electrical \& communication engineering (ICCECE)*, 2017, pp.1–7.

[31] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey, " *arXiv Prepr. arXiv1701.02145*, 2017.

[32] Y. Wei, J. Jang - Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE - MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification, " *IEEE Access*, vol.9, pp.146810–146821, 2021, doi: 10.1109/ACCESS.2021.3123791.

[33] M. Abdullahi *et al.*, "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review, " *Electronics*, vol.11, no.2, p.198, 2022.

[34] R. Baldoni, E. Coppa, D. C. D'Elia, and C. Demetrescu, "Assisting malware analysis with symbolic execution: A case study, " in *Cyber Security Cryptography and Machine Learning: First International Conference, CSCML 2017, Beer - Sheva, Israel, June 29 - 30, 2017, Proceedings 1*, 2017, pp.171–188.

[35] B. Molina - Coronado, U. Mori, A. Mendiburu, and J. Miguel - Alonso, "Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process, " *IEEE Trans. Netw. Serv. Manag.*, vol.17, no.4, pp.2451–2479, 2020.

[36] S. Adhikari *et al.*, "A Novel Machine Learning - Based Hand Gesture Recognition Using HCI on IoT Assisted Cloud Platform., " *Comput. Syst. Sci. \& Eng.*, vol.46, no.2, 2023.

[37] M. Yuriyama and T. Kushida, "Sensor - cloud infrastructure - physical sensor management with virtualized

sensors on cloud computing, ” in *2010 13th international conference on network - based information systems*, 2010, pp.1–8.

[38] M. Quwaider and Y. Jararweh, “Cloudlet - based efficient data collection in wireless body area networks, ” *Simul. Model. Pract. Theory*, vol.50, pp.57–71, 2015.

[39] N. U. Sama, N. Z. Jhanjhi, M. Humayun, and A. U. Rahman, “Digital twin evolution, application areas and enabling technology, ” in *AIP Conference Proceedings*, 2024.

[40] Y. Zhang and H. Xiao, “Bluetooth - based sensor networks for remotely monitoring the physiological signals of a patient, ” *IEEE Trans. Inf. Technol. Biomed.*, vol.13, no.6, pp.1040–1048, 2009.

[41] A. Zaheer, S. Tahir, M. F. Almufareh, and B. Hamid, “A Hybrid Model for Botnet Detection using Machine Learning, ” in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 2023, pp.1–8.

[42] S. Berrahal, N. Boudriga, and A. Bagula, “Cooperative sensor - clouds for public safety services in infrastructure - less areas, ” in *2016 22nd Asia - Pacific Conference on Communications (APCC)*, 2016, pp.222–229.

[43] A. Beloglazov, J. Abawajy, and R. Buyya, “Energy - aware resource allocation heuristics for efficient management of data centers for cloud computing, ” *Futur. Gener. Comput. Syst.*, vol.28, no.5, pp.755–768, 2012.

[44] Adhikari, S., Gangopadhayay, T. K., Pal, S., Akila, D., Humayun, M., Alfayad, M., & Jhanjhi, N. Z. (2023). A Novel Machine Learning - Based Hand Gesture Recognition Using HCI on IoT Assisted Cloud Platform. *Computer Systems Science & Engineering*, *46* (2).