Journal of Information Systems Engineering and Management
2025, 10(19s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An Efficient AI and Blockchain Integrated Approach for Healthcare Management

Girish M. Ghormode[1], Soni A. Chaturvedi[2], A. A. Khurshid[3], Gajendra M. Asutkar[4]

[1] Research Scholar, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.
[2] Associate Professor, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, India.
[3]Professor, Department of Electronics Engineering, RamdeoBaba University, Nagpur, India.
[4] Professor, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, India.

ARTICLE INFO

Received: 25 Dec 2024

Revised: 28 Jan 2025

Accepted: 16 Feb 2025

ABSTRACT

Today, many remote patients are ensuring reliable treatments by using smart wearable devices on their bodies. Thus, the effectiveness of the healthcare industry has remarkably grown. However, it is affected by breaches in data security which had been a prime concern owing to the incredible rise in patient numbers. Intruders intercept the data over the channel, and system and tamper with the data which puts the privacy of the medical records at stake. The introduction of the 4.0 medical industry has enhanced the mode of diagnosis and treatment approaches. Medical practitioners or experts access digital information regarding the patient's condition to administer accurate and fast treatment. However, spoof attacks, manipulation, and hijacking are common vulnerable attacks seen on wearable gadgets. Tampered data passed to the concerned medical expert may put the patient's life at risk. Due to its transparency, security, and being an immutably decentralized network, blockchain is utilized to store information from patient's wearable devices. The authenticity of the information from wearable gadgets entering the blockchain can be effectively detected using Artificial Intelligence (AI) through machine machine-learned classifier. This paper introduces an AI and blockchain-based highly secured and trustworthy framework to eliminate malicious samples and allow authentic information to flow in the network which can be analyzed by the medical experts and followed by the patients. The dataset samples from the unbalanced WUSTL EHMS 2020 dataset considered for evaluation are efficiently processed by selecting significant features from 43 attributes. The dataset was augmented to balance, extending the lower class (attack) samples. The features were normalized, reduced in dimension and classified using the Support Vector Machine (SVM). Experimentation showed that the malicious samples were distinguished from the normal samples at an accuracy above 98% which is better than other recent competing researches.

Keywords: Smart wearable devices, healthcare industry, medical experts, vulnerable attacks, blockchain, Artificial Intelligence, and support vector machine.

INTRODUCTION

The Internet of Things (IoT) has transformed human-centric approaches to system-centric interactions. It has greatly revolutionized the healthcare domain by introducing promising advancements in the IoT. Today, medical services are intelligently provided by collecting information centrally, dispersed at low cost through customer-centric approaches that have all benefited using the IoT benefits. A sophisticated design with intelligent applications using IoT i.e. wearable devices are used in healthcare that are used to monitor, and measure several physical/clinical parameters from a remote patient. They also possess the capability to track various chronic diseases and receive medical reports from distant medical practitioners. AI has been a common tool used to analyze clinical parameters such as body temperature, heart rate, glucose level, blood pressure, blood oxygen level, etc., and also to predict immediate and future measures for patients [1-2]. The wearable devices are made reliable, efficient, and effective by the incorporation of data transmission technology. Despite this, these wearable devices are vulnerable to unseen attacks and threats where an intruder can misinterpret the patient's personal and medical information [3]. The patient's healthcare information is stored and processed centrally and analyzed for the patient's relief is also susceptible to various security harms that primarily include spoofs, hijacks, and manipulations [4-5]. Other factors that need attention include the protection of the central database system from vulnerabilities to safeguard patient's life at risk.

Researchers across the globe have suggested indispensable means to mitigate security attacks related to wearable devices. The work suggested in [6] introduced a cryptographic approach to safeguard the patient's data. The authors worked for data confidentiality, authenticity, integrity, and availability. The data was secured using ciphers. The authors in [7] limited the access to medical images using watermarking through symmetric key encryption. It was based on client authentication for the access of medical images. However, despite the two approaches that incorporated the cryptographic solutions and the encryption mechanism, the schemes showed minimum robustness against the attacker. Therefore, there needs to be some stringent mechanism that can prevent unauthorized access to healthcare data and subsequently distinguish between malicious and non-malicious intents.

The work introduced by authors in [8] used a lightweight naïve Bayes classifier that offered an efficient and privacy-preserving model. The objective of the work was to provide online primary diagnostic services to the end users without compromising data privacy. Their system ensures that the patient's query is forwarded straight to the server or service provider and the patients would only access the analysis report after decryption. Another approach presented in [9] used a watermarking strategy that included the key and image transform coefficients for securing healthcare records. The approach made data communication complex making it difficult to understand that ensured protection against attackers. Despite various advantages, AI-based healthcare systems are prone to copying once they are constructed. That implies that an intruder can perform adversarial attacks.

Blockchain provides better security to data aggregated from wearable devices. The technology inflexibly stores data thus improving privacy and establishing trust between different entities connected in the healthcare system [10-11]. One such system that adopted the Health Insurance Portability and Accountability characteristics was introduced in [12]. The authors worked on data from the wearable devices and central servers. Their lightweight model used a chaotic map scheme using negotiated keys. They also concentrated on security considering the blockchain technology and prevented the system from data manipulation. Work in [13] focussed on securing doctors' prescriptions being manipulated by intruders or attackers. They developed a smart, transparent, and trustworthy supply chain management system for medicine with blockchain and ensured non-tampered prescriptions to the patients.

However, there is an intense need to develop a blockchain-based highly secured, and trusted mechanism that incorporates AI for enhanced security of the wearable device's information. This is because merely using the blockchain cannot confront the security breaches related to wearable devices. The proposed blockchain-AI integrated secure and trustworthy framework called the "BAIST" utilizes a Machine learning model trained on a publicly available benchmark dataset, which consists of normal and attack samples obtained from wearable healthcare devices. The objective is to restrict and permit the patient's data into the blockchain using AI after they are classified. The data from the verified patients is allowed to enter the system while the attacker samples are discarded. Performance parameters showed that the proposed BAIT framework outperformed other competing models in distinguishing the normal and the unsecured information.

MOTIVATION AND BACKGROUND

Millions of people across the world have different medical issues and ailments and connect to the healthcare sector directly or indirectly. Medical care centers collect patients' personal and medical information using various means and store them for analysis. A large amount is spent on securing the patient's data from unauthorized access since patient data is crucially sensitive. There were news regarding the breach of such data through cyber-attacks and information related to patients went online. This was because the security employed a single technology [14-15] rather it required a robust framework. The breach of such sensitive details can put the lives of millions of people at risk. Thus the research community working for the protection of the healthcare systems integrated AI with healthcare to combat the increasing cyber-attacks. Records collected from patients include clinical data, demographic data, images, videos, claims, etc. AI works perfectly on such records regarding evaluation, and uncovering insights and patterns that anybody would not be able to find on their own.

Lonely AI is not sufficient to handle cyber-attacks. Data should be guarded at the place of its storage. The blockchain can provide security and immutability at this end. It can mitigate the infiltration inside the blockchain. The decentralized nature of blockchain technology offers greater resistance to the data since an attacker needs to access more than 50% of the blockchain nodes to tamper with the information. This makes it impossible to tear the blockchain curtain, especially for the public blockchain. The proposed work uses healthcare integration with AI to identify the tampered and normal samples.

Millions of people across the world have different medical issues and ailments and connect to the healthcare sector directly or indirectly. Medical care centers collect patients' personal and medical information using various means and store them for analysis. A large amount is spent on securing the patient's data from unauthorized access since patient data is crucially sensitive. There were news regarding the breach of such data through cyber-attacks and information related to patients went online. This was because the security employed a single technology [14-15] rather it required a robust framework. The breach of such sensitive details can put the lives of millions of people at risk. Thus the research community working for the protection of the healthcare systems integrated AI with healthcare to combat the increasing cyber-attacks. Records collected from patients include clinical data, demographic data, images, videos, claims, etc. AI works perfectly on such records regarding evaluation, and uncovering insights and patterns that anybody would not be able to find on their own.

Lonely AI is not sufficient to handle cyber-attacks. Data should be guarded at the place of its storage. The blockchain can provide security and immutability at this end. It can mitigate the infiltration inside the blockchain. The decentralized nature of blockchain technology offers greater resistance to the data since an attacker needs to access more than 50% of the blockchain nodes to tamper with the information. This makes it impossible to tear the blockchain curtain, especially for the public blockchain. The proposed work uses healthcare integration with AI to identify the tampered and normal samples.

RESEARCH CONTRIBUTIONS

- We propose a blockchain-AI integrated secure and trustworthy framework called BAIST that efficiently detects attacker samples from healthcare samples acquired from wearable devices.

- The framework employs a feature selection mechanism that selects significant features from the available attributes of the WUSTL EHMS 2020 dataset.

- A Machine learning technique incorporating SVM detects malicious samples by properly selecting the relevant attributes from the dataset. The unbalanced dataset is suitably balanced using the min-max values of the existing low-count class samples.

- The BAIST framework is evaluated for classification accuracies that showed remarkable results than other state-of-the-art work.

The article is organized in the following manner: The immediate section, Section 2 covers the summary of related work from the literature. Section 3 describes the material used and the proposed BAIST methodology utilized for attack detection. Section 4 presents the experimental analysis and discussion using the proposed BAIST framework while the last section, section 5 concludes the article with future scope.

RELATED WORK

The authors in [16] carried out work limited to IoT testbed and suggested remedies to smart gadgets' security. They also simultaneously maintained information security. The proposed model was not tested on real-world data samples and thus the behavior of the model would be uncertain. The communication between sensors and medical practitioners was authenticated [17] using a lightweight model for wireless sensor networks concerned with medical applications [18]. An efficient framework to prevent intruders from accessing central systems and attacking devices from peeking was suggested in [19]. They used physically un-clonable attributes for their authentication technique for IoT in medical applications. However, their authentication scheme failed to resist advanced decryption tools that are capable of decrypting the encrypted keys.

A nonlinear SVM-based online cathartic pre-diagnosis system was introduced for data privacy by the authors in [20] that showed efficacy related to prediction. The authors obtained the highest classification accuracy of 90% using machine learning techniques to identify harmful tasks in smart healthcare systems [21]. They evaluated their model using four different machine-learning schemes. On the other hand, the authors in [21] worked to recognize dishonest medical equipment. They used the Bayesian inference by incorporating a trust-based mechanism for identifying dishonest devices connected to the healthcare system. The work showed no contribution towards data manipulation and integrity attacks.

A smart online health system was introduced in [23]. The system utilized blockchain to communicate medical data in an automated manner. For fast and secure patient information access [24], they proposed a tree-based data structure based on a modified Merkel scheme. A simulation-based healthcare system was evaluated in [25]. The author's strategy was based on rewards and Ethereum. Their model suggested a new scheme of essentially obtaining higher rewards for minimum spending. They showed that the bribed self-mining system in the blockchain can be affected by harmful attacks owing to higher prices and lower expenditure. The work neglected malicious attacks in the blockchain and rather considered the mining attacks. The solution to intrusion attacks was provided in [26] in an IoT-enabled healthcare system. The author used blockchain and deep learning techniques to detect the intrusion for secure information transmission. However, the author's neglected actual patient medical data, which if maliciously modified enters the blockchain and may threaten the life of the patient. Work in [27] suggested a comparable dataset for each patient in the blockchain-based healthcare environment. They suggested an advanced 5G model for the system but failed to handle real-time data. A complex model to detect anomalies in the patient's record was introduced in [28]. A secured healthcare network integrating patients, doctors, pathological laboratories, and administrators was developed in [29]. However, the system failed to operate successfully in a full-fledged manner.

The above review and its analysis showed that there is an intense need to amalgamate AI with blockchain since none of the work explored above has incorporated both technologies to alleviate the security issue relating to wearable devices. Also, secure healthcare schemes succeeded in detecting attacker samples at a maximum of 93% accuracy which eventually allowed malicious records to enter into the blockchain.

THE MATERIAL AND THE PROPOSED BAIST FRAMEWORK

The proposed BAIST framework is incorporated between the patient's wearable device and the blockchain to provide robust security by preventing malicious data from entering the blockchain. This will protect the precious life of the patients from unauthorized information that will threaten their life. The BAIST framework thus integrates the blockchain and the AI module and allows authentic information to flow in the network. An intruder can intercept data before entering the server through the gateways and can maliciously modify the contents acquired from the patient's wearable devices. The possible modifications or changes are concerned with the sensitive physical parameters and the patient's personal information that can affect proper diagnosis and treatment eventually putting the patient's life at risk. The BAIST thus combats the threats by identifying malicious samples and maintaining data integrity. The malicious samples detected by the BAIST framework are discarded and prevented from entering the blockchain shared by healthcare professionals, patients, pathologists, and system administrators. The proposed framework thus ensures accurate analysis by the pathologists, appropriate diagnosis and treatment by the medical practitioners, effective treatment for patients, efficient database management, development, monitoring, and implementation by administrators. The blockchain-AI integrated model is shown in Figure 1. The EHMS testbed is based on the data communicated through wearable devices. Though the database is constructed using the EHMS testbed, it consists of physical parameters acquired from the sensors present with the patient's internal or external body parts.

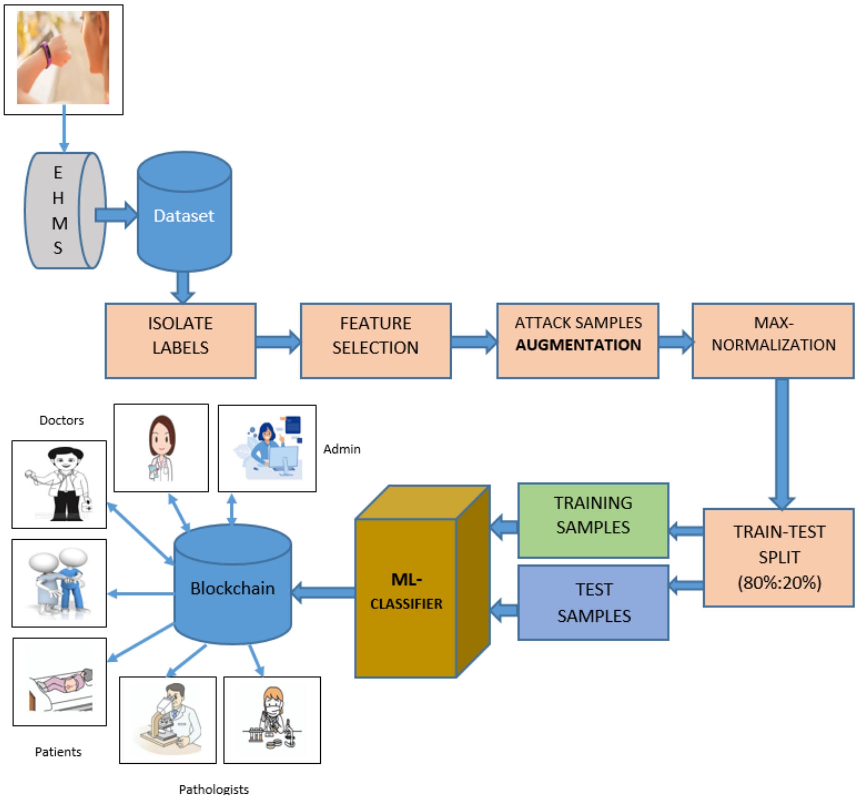


Figure 1 - The Proposed BAIST Framework

FEATURE SELECTION STRATEGY

Initially, the labels of the dataset samples are isolated from the last column (attribute – 44) of the dataset. Extensive experiments were carried out to obtain relevant features from the dataset for improving the detection/classification accuracy. The relevant or significant features were found by finding value changes in each of the feature columns. In the first case, value changes of more than one were found in each feature. We obtained 33 relevant out of 43 features. Features 1, 3, 4, 6, 11, 12, 16, 22, 24, and 34 were eliminated in the first round of the feature selection strategy since these features do not contribute to distinguishing the attack and normal samples. A maximum value change of 16315 was found for feature 5.

The experiment showed that using 33 features limited the classification accuracy between 90-92%. We performed classification eliminating more features from the available features. Analysis showed that feature value changes above 3 from the remaining features would increase the classification rate. Therefore, in the second stage, we eliminated features where the value changes are less than equal to 3. We found that 27 features were significant and showed improvement over the earlier classification accuracy of 92%. The significant feature headings found from the feature selection strategy are listed in Table 1. The complete feature description and type of features are explained in [30][31].

Table 1 – Significant features found using the feature selection strategy with value change greater than 3.

Sr. No.	Column	Parameter	Sr. No.	Column	Parameter
1	2	Flgs	15	27	Load
2	5	Sport	16	29	pLoss
3	7	SrcBytes	17	31	pDstLoss
4	8	DstBytes	18	32	Rate
5	9	SrcLoad	19	35	Packet_num
6	10	DstLoad	20	36	Temp

7	13	SIntPkt	21	37	SpO2
8	14	DIntPkt	22	38	Pulse_Rate
9	15	SIntPktAct	23	39	SYS
10	17	SrcJitter	24	40	DIA
11	18	DstJitter	25	41	Heart_Rate
12	23	dMinPktSz	26	42	Resp_Rate
13	25	TotPkts	27	43	ST
14	26	TotBytes			

Out of 27 significant features, features corresponding to column 2 consist of textual values (M, M*, Md, MR, e, es, and eR) while the rest of the feature values in the remaining columns are numeric. We found the unique text values in the 'Flg' column (Feature 2 in the original dataset) and substituted them with numeric values from 1 to 7. The textual values were represented as M-1, M*-2, Md-3, MR-4, e-5, es-6, and eR-7.

We found that using the 27 significant columns, the classification accuracy deteriorated due to an imbalanced dataset. The attack samples were misclassified since the count of normal samples (14272) was significantly more than the attack samples (2046). That is, the classifier was biased towards the normal samples. On the other hand, reducing the features further degraded the classification accuracy below 92%. The same has been validated in the work carried out in [32]. The authors tested four machine learning techniques and an LSTM network by varying the number of features from 5 to 44. They obtained higher accuracy when the number of features was increased. The only remedy was to augment the low-count class samples to make the dataset balanced.

AUGMENTATION OF THE ATTACK SAMPLES

We employed a novel approach to augment the attack samples. Initially, we isolated the attack samples from the normal samples considering 27 significant columns obtained using the feature selection strategy. Then unique values for each feature in the attack samples were obtained. For generating 14272-2046 = 12226 attack samples, we used the unique values from each feature randomly and concatenated them to form a feature vector of 27 values. However, the count of unique values corresponding to the attack samples for features Flgs, SrcBytes, DstBytes, SIntPktAct, TotPkts, TotBytes, pLoss, pDstLoss, SpO2, and SYS was too minimum to compensate 12226 samples which would amount to redundant samples in the attack intra-class. Also, features SIntPktAct had no unique values other than 0, while pLoss and pDstLoss contained only two unique values including a 0 value.

Therefore, a separate code was used to find redundant samples from the generated samples, and the redundancy was eliminated and covered by generating a new set of samples. After manual inspection, it was found that the feature SIntPktAct imposes confusion regarding inter-class discrimination. The column contained 8 unique values including 0. However, all the finite unique values represented the normal class while the attack samples were represented by only 0 value. Therefore, the feature was eliminated to eliminate the confusion at the classifier. Figure 1 shows the marked feature (Highlighted using a Red color) that was eliminated. Finally, 26 features were used to train the classifier with the inclusion of the augmented samples.

NORMALIZATION AND SPLIT

The range of value each feature holds is different, therefore the feature values were normalized using a Max-normalization algorithm. The process involves finding the maximum value in each feature column and dividing each value by the maximum value to fit all values in the range [0 1]. The samples were segregated and labels were reconstructed due to the addition of augmented samples. The features are transformed to other coordinate axes using the Principal Component Analysis (PCA) which also serves to reduce the dimension of the features. For this work, we selected 20 PCA components. The samples were concatenated from both classes along with their respective labels to partition the samples in training and test sets using a ratio of 80%:20% respectively.

The Machine Learning–Based Classifier

We used SVM to classify the categories using SGDA optimizer with radial basis function kernel. The SVM performance regarding other optimizers was found to be nearer but inferior as compared to ISDA.

The Dataset

WUSTL EHMS 2020 dataset [33-34] was constructed using a real-time testbed (Enhanced Healthcare Monitoring System). To compensate for the scarcity of the dataset, the patient's biometrics were combined with network flow metrics. The testbed was partitioned into four sections: physical sensors, gateway, the network, and the control section used for visualization. The sensor acquires the physical parameter from the patient's body and carries it to the gateway. The data is visualized at the server which is routed via the switch and the router. An intrusion can occur before the information is arrived at the server. Therefore an Intrusion Detection System is required to capture the real-time data and detect the abnormalities in the data. The dataset is prone to man-in-the-middle attacks [35] comprising the spoof [36] and the injection attacks [37]. The former attack violates data confidentiality while the latter the data integrity. The following Table 2 gives the summarised description regarding the size and samples. The dataset is covered by 44 attributes or features and the samples are labeled by '0' and '1' for normal and attack categories respectively.

Table 2 – Description of the WUSTL EHMS 2020 dataset

Measurement	Size	Normal samples	Attack samples	Total samples
Value	4.4 MB	14272 (87.5%)	2046 (12.5%)	16138

The algorithm for the BAIST framework is listed below:

Algorithm 1 – The BAIST mechanism

```
Input - WUSTL EHMS 2020 dataset
Output – Legitimate Device samples

Load the Dataset
Isolate the Labels
Count the number of samples from each class
Apply feature selection strategy to eliminate un-relevant features
Augment the low-class samples using the unique values available with the features
Remove redundant samples
Eliminate confusing feature
Normalize the features using Max-Normalization Algorithm
Apply PCA and select components
Split the training and testing sets using ratio – 80%:20%
Train the ML-Classifier (SVM) with the training set
Test the classifier with the testing set
Evaluate the performance parameters
Discard the attack samples
Allow the normal samples to enter the Blockchain
```

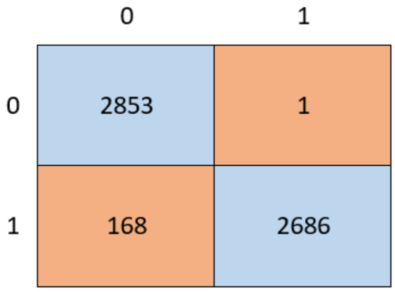
RESULTS AND DISCUSSION

The BAIST framework utilized for the intrusion detection system was evaluated by different performance parameters and executed on MATLAB 2019b environment. The framework was executed on the Windows 11 platform, with 16 GB RAM, 512 GB SSD, and a 2.84 GHz Intel i5 processor. Accuracy represents a better insight into a model's performance on a particular dataset. The machine learning model's performance for the IDS is presented in Table 3 concerning training and test accuracies, precision, recall, and F1-score. Table 4 shows the confusion matrix obtained using the BAIST framework. The IDS framework shows similar performance qualitatively and quantitatively with a value above 97%. The confusion matrix evaluated over the test samples shows that the normal samples were classified at a remarkable accuracy of 99.96% while encouraging results were shown for attack samples. The classification accuracy for the vulnerable samples was evaluated at 94.11%.

Table 3 – Performance of BAIST framework in Intrusion Detection.

Parameters	**Values**
Accuracy – Training	0.96453
Accuracy – Testing	0.97039
Precision	0.97039
Recall	0.97201
F1-score	0.9712

Table 4 – Confusion Matrix (Normal-0/Attack-1)



	0	1
0	2853	1
1	168	2686

The misclassified attack samples are due to restricted augmentation. Although the attack samples are augmented from the available attack samples using their range values, there exist very few unique values corresponding to some features (11 features). Generating 12226 samples increases the possibility of similar or nearer samples at least for the features with very few unique values. Thus due to greater imbalance, the normal network traffic class has a higher hand and so the attack samples are aligned in the normal class. However, the BAIST model is capable of discriminating the normal samples with higher accuracy.

Table 5 – Comparative analysis of BAIST framework for IDS with other competing models.

Parameters in %	**Reference**								
	[38]	[39]	[40]	[41]	[32]	[42]	[43]	[44]	Proposed BAIST
Accuracy	96.39	96.5	96.39	92.92	94.9	95.01	94	92.5	**97.04**
Precision	-	96	-	88	-	94.94	95	96.74	**97.04**
Recall	-	96	-	**1.00**	-	95.01	94	44.40	97.20
F1-score	86.12	95	-	93	-	-	94	60.87	**97.12**

Table 5 shows the comparative performance of the proposed BAIST framework for IDS with other recent competing models concerning the WUSTL EHMS 2020 dataset. Although the highlighted figures concerning the accuracy in the table show an improvement of just 0.65% over the work carried out in [38] and [40], it affects 186 samples in the dataset. The precision (not computed in [38] and [40]) is higher with the BAIST framework which proves that the proposed model is qualitatively better. However, the work proposed in [41] is quantitatively rich, but the harmonic average is poor. A significant part of the BAIST framework is the feature selection strategy which ensures better sample representation using the selected features.

CONCLUSION

The BAIST framework introduced in this work to detect vulnerable samples infected by spoof attacks, manipulations, and hijacking attacks performed better than other recent existing models. The model is simple and efficient and based primarily on a feature selection strategy. A better analysis is carried out on the available features to select significant features that would represent the network traffic samples. The advantage of the feature selection strategy is seen from the classification accuracy which is more than 97% for 20% of test data from both categories. The integrated AI-blockchain approach initially detects the vulnerable or harmful samples from the available WUSTL EHMS 2020 dataset samples that ensure the authenticity of the wearable device. Furthermore, the data of the legitimate wearable is allowed to enter the blockchain while discarding the dirty or illegitimate ones. Once the network accepts the pure or authentic samples, they are secured in the immutable ledger.

Although different researchers have put efforts into cleaning the data and recognizing the legitimate devices using different methodologies incorporating machine learning and deep learning techniques, low-count features (43), non-variability of the features (11 features), and imbalanced nature impose complexity. This article will assist interested researchers in developing a better IDS model by concentrating on 26 features that have been found crucial after our feature selection mechanism. Improving the performance will minimize the life risk of the connected patients, provide authentic biometric and flow metric data to pathologists, and eventually develop better trustworthy coordination between the doctors and patients.

The BAIST model will be improved in the future by concentrating on a better augmentation strategy, properly sequencing features before training and testing, and developing and fine-tuning sequential custom networks.

REFERENCES

[1] Tanwar, S.; Vora, J.; Kaneriya, S.; Tyagi, S.; Kumar, N.; Sharma, V.; You, I. Human Arthritis Analysis in Fog Computing Environment Using Bayesian Network Classifier and Thread Protocol. IEEE Consum. Electron. Mag. 2020, 9, 88–94.

[2] Patel, K.; Mehta, D.; Mistry, C.; Gupta, R.; Tanwar, S.; Kumar, N.; Alazab, M. Facial Sentiment Analysis Using AI Techniques: State-of-the-Art, Taxonomies, and Challenges. IEEE Access 2020, 8, 90495–90519.

[3] 8 Major Problems with the U.S. Healthcare System Today. Available online: https://www.medifind.com/news/post/problemsus-healthcare-system (accessed on 10 December 2022).

[4] Evolution of Health Data Storage for Digital Healthcare. Available online: https://www.linkedin.com/pulse/evolution-healthdata-storage-digital-healthcare-ambarish-giliyar/ (accessed on 22 December 2022).

[5] Anand, P.; Singh, Y.; Selwal, A.; Alazab, M.; Tanwar, S.; Kumar, N. IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. IEEE Access 2020, 8, 168825–168853.

[6] Noura, M. Efficient and Secure Cryptographic Solutions for Medical Data. Ph.D. Thesis, Université Bourgogne, Dijon, France, 2019.

[7] Kester, Q.A.; Nana, L.; Pascu, A.C.; Gire, S.; Eghan, J.M.; Quaynor, N.N. A Cryptographic Technique for Security of Medical Images in Health Information Systems. Procedia Comput. Sci. 2015, 58, 538–543.

[8] Liu, X.; Zhu, H.; Lu, R.; Li, H. Efficient Privacy-Preserving Online Medical Primary Diagnosis Scheme on Naïve Bayesian Classification. Peer-to-Peer Netw. Appl. 2018, 11, 334–347.

[9] Rai, A.; Singh, H. SVM-Based Robust Watermarking for Enhanced Medical Image Security. Multimed. Tools Appl. 2017, 76, 18605–18618.

[10] Gupta, R.; Shukla, A.; Tanwar, S. AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.

[11] Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of Blockchain for Mitigating the Distributed Denial of Service Attacks. Secur. Priv. 2020, 3, e96.

[12] Lee, T.F.; Chang, I.P.; Kung, T.S. Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations. Appl. Sci. 2021, 11, 10576.

[13] Zhu, P.; Hu, J.; Zhang, Y.; Li, X. A Blockchain-Based Solution for Medication Anti-Counterfeiting and Traceability. IEEE Access 2020, 8, 184256–184272.

[14] Tauqeer, H.; Iqbal, M.M.; Ali, A.; Zaman, S.; Chaudhry, M.U. Cyberattacks Detection in IoMT Using Machine Learning Techniques. J. Comput. Biomed. Inform. 2022, 4, 13–20.

[15] Lu, W. Detecting Malicious Attacks Using Principal Component Analysis in Medical Cyber-Physical Systems. In Artificial Intelligence for Cyber-Physical Systems Hardening; Springer: Berlin/Heidelberg, Germany, 2023; pp. 203–215.

[16] Yeh, K.H. A Secure IoT-Based Healthcare System With Body Sensor Networks. IEEE Access 2016, 4, 10288–10299.

[17] Wu, F.; Li, X.; Sangaiah, A.K.; Xu, L.; Kumari, S.; Wu, L.; Shen, J. A Lightweight and Robust Two-Factor Authentication Scheme for Personalized Healthcare Systems Using Wireless Medical Sensor Networks. Future Gener. Comput. Syst. 2018, 82, 727–737.

[18] Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Park, Y.; Tanwar, S. Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Networks. IEEE Access 2018, 6, 20673–20693.

[19] Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E.; Puthal, D. PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. IEEE Trans. Consum. Electron. 2019, 65, 388–397.

[20] Zhu, H.; Liu, X.; Lu, R.; Li, H. Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM. IEEE J. Biomed. Health Inform. 2017, 21, 838–850.

[21] Newaz, A.K.M.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems. arXiv 2019, arXiv:1909.10565.

[22] Meng, W.; Choo, K.K.R.; Furnell, S.; Vasilakos, A.V.; Probst, C.W. Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. IEEE Trans. Netw. Serv. Manag. 2018, 15, 761–773.

[23] Chelladurai, U.; Pandian, S. A Novel Blockchain-Based Electronic Health Record Automation System for Healthcare. J. Ambient. Intell. Humaniz. Comput. 2022, 13, 693–703.

[24] Mistry, C.; Thakker, U.; Gupta, R.; Obaidat, M.S.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. MedBlock: An AI-Enabled and Blockchain-Driven Medical Healthcare System for COVID-19. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. Thakker, U.; Mistry, C.; Tanwar, S.; Kumar, N.; Obaidat, M.S. AI-Enabled and Blockchain-Driven Digital Twin for Network Management of 6G-Enabled Internet of Medical Things. IEEE Internet Things J. 2021, 8, 2343–2351.

[25] Manogaran, G.; Lopez, D. A Survey of Big Data Architectures and Machine Learning Algorithms in Healthcare. J. King Saud Univ. Comput. Inf. Sci. 2019, 31, 415–425.

[26] Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.

[27] Kuo, T.-T.; Kim, H.E.; Ohno-Machado, L. Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220.

[28] Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In Advances in Computers; Raj, P., Deka, G.C., Eds.; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.

[29] Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A. Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-Like Epidemics: A Survey. IEEE Access 2021, 9, 95730–95753.

[30] Tian, F. An Agri-Food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. In Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.

[31] Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of Things Security: A Top-Down Survey. Comput. Netw. 2018, 141, 199–221.

[32] Esposito, C.; Ficco, M.; Palmieri, F.; Castiglione, A. Blockchain-Based Authentication and Authorization for Smart City Applications. Comput. Netw. 2018, 159, 192–203.

[33] Seebregts, C.J.; Dane, P.Y.; Parsons, A.N.; Fogwill, T. Digital Health Systems: Perspectives from the Global South. Annu. Rev. Public Health 2021, 42, 395–410.

[34] Jindal, A.; Jindal, R.; Jindal, N.; Dua, A.; Kumar, N. Blockchain-Based Cybersecurity for AI-Driven Systems: State of the Art, Challenges, and Future Research Directions. IEEE Internet Things J. 2022, 9, 14712–14738.

[35] Cha, S.C.; Yeh, K.H.; Luo, M.Y. Blockchain-Based Privacy-Preserving Authentication for Smart Healthcare Systems. Future Gener. Comput. Syst. 2020, 107, 146–160.

[36] Boireau, M.; Oliveira, J.L. Interoperability and Security in Digital Health: Challenges and Perspectives. Health Inform. J. 2020, 26, 1022–1032.

[37] Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain Technology: A Survey on Applications and Security Privacy Challenges. Internet Things 2019, 8, 100107.

[38] Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in Smart Hospitals. IEEE Trans. Ind. Inform. 2018, 14, 1656–1665.

[39] Rani, S.; Suthar, P.; Tanwar, S.; Kumar, N.; Obaidat, M.S. AI-Enabled and Blockchain-Driven Personalized Healthcare System. In Proceedings of the 2021 International Conference on Machine Learning and Cybernetics (ICMLC), Adelaide, SA, Australia, 3–6 July 2021; pp. 1–6.

[40] Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. HealthChain: A Novel Framework on Blockchain for Privacy-Preserving Smart Healthcare Systems. IEEE Access 2019, 7, 102985–102999.

[41] Mamoshina, P.; Ojomoko, L.; Yanovich, Y.; Ostrovski, A.; Botezatu, A.; Prikhodko, P.; Izumchenko, E.; Aliper, A.; Zhavoronkov, A. Converging Blockchain and Next-Generation Artificial Intelligence Technologies to Decentralize and Accelerate Biomedical Research and Healthcare. Oncotarget 2018, 9, 5665–5690.

[42] Min, J.; Kim, H. Blockchain-Based Secure EHR System Using Homomorphic Encryption. Comput. Stand. Interfaces 2020, 69, 103408.

[43] Park, Y.R.; Lee, E.; Na, W.; Park, S.; Lee, Y.; Lee, J.H. Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed-Methods Study to Test Feasibility. J. Med. Internet Res. 2019, 21, e12533.

[44] Shukla, S.; Sohi, B.S.; Kumar, N.; Tanwar, S.; Obaidat, M.S. A Blockchain-Based Framework for Security and Privacy in Smart Healthcare Systems. In Proceedings of the 2021 International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.