Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 19s (2025)
https://www.jneonatalsurg.com

Next-Generation Healthcare Management: AI and Blockchain Integration

Girish Ghormode*[1], Dr. Soni A. Chaturvedi[2], Dr. A. A. Khurshid[3], Dr. J.P. Rothe[4]

[*1]Research Scholar, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

[2]Associate Professor, Electronics and Communication Engineering Priyadarshini College of Engineering Nagpur, India

[3]Professor, Department of Electronics Engineering, RamdeoBaba University, Nagpur, India

[4]Professor, Electrical Engineering St. Vincent Pallotti College of Engineering and Technology, Nagpur, India

***Corresponding Author:**

Mr. Girish Ghormode

Email ID: Girish10693@gmail.com

.Cite this paper as: Girish Ghormode, Dr. Soni A. Chaturvedi, Dr. A. A. Khurshid, Dr. J.P. Rothe, (2025) Next-Generation Healthcare Management: AI and Blockchain Integration. *Journal of Neonatal Surgery*, 14 (19s), 760-768.

ABSTRACT

Many distant patients now use smart wearable devices on their bodies to ensure dependable therapy; as a result, the healthcare sector is now far more effective; however, it is impacted by data security breaches, which were a major worry because of the astounding increase in patient volume. The privacy of medical records is at risk when hackers intercept data over the channel, alter the data, and interfere with the system. Approaches to diagnosis and treatment have improved since the advent of the 40 medical industries to provide precise and prompt therapy. Medical professionals or specialists consult digital data on the patient's condition; however, frequent vulnerable assaults against wearable technology include spoofing, manipulation, and hijacking. Providing the concerned medical professional with tampered data could endanger the patient's life. Information from patient's wearable devices is stored on blockchain because of its immutable, decentralized network transparency and security. Artificial intelligence can be used to detect the legitimacy of wearable device data entering the blockchain by utilizing a machine-learned classifier. This study presents a highly secure and reliable framework based on air and blockchain technology to remove fraudulent samples and permit legitimate information to circulate throughout the network for patients to follow and medical professionals to evaluate. By picking important characteristics among 43 attributes, the dataset samples from the imbalanced west hems 2020 dataset that are being evaluated are processed effectively. The lower-class attack samples were expanded to balance the dataset; sums were utilized to normalize and decrease the dimension by SVM. And classification of the experiments revealed that the malicious samples could be differentiated from the normal samples with an accuracy of over 98%, outperforming other recent rival studies.

Keywords: *Smart wearable devices, healthcare industry, medical experts, vulnerable attacks, block chain, Artificial Intelligence,and support vector machine*

1. INTRODUCTION

Due of the thrilling fresh advances and innovations in the internet of things human-centric methods have been swapped out for system-centric interactions. This has completely changed by centrally collecting data and information from users; the healthcare industry and medical services are now intelligently provided and distributed at a low cost using customer-centric and various strategies that have all benefited from it. [2-3] Wearable medical technology, an intricate layout with clever applications that make use of the internet of things, is used to track various chronic illnesses. Measure and monitor a number of clinical and physical characteristics from a patient who is far away and get medical data from distant medical providers. AI is widely used to evaluate clinical parameters, including blood pressure, blood oxygen level, heart rate, glucose level, body temperature, and more, as well as to predict patients immediate and long-term treatment. Wearable medical technology uses [1-2] data transfer technologies to make them reliable, effective, and efficient. Nevertheless, these wearables are susceptible to invisible risks and assaults, which might lead to a hacker misinterpreting central processing, storing and analyzing patient health data, including personal and medical information, making them vulnerable to a number of security risks, chief among them being spoofs. Hijacks and manipulations [4-5] Protecting the central database system from vulnerabilities is another aspect that requires attention in order to preserve patients' lives. Researchers from all around the world have proposed essential ways to lessen wearable device security threats. A cryptographic technique was introduced in the work recommended in [6] to protect the patients' data in order to restrict access to medical photos. The authors used symmetric key encryption and watermarking, and client authentication was necessary in order to view medical images. They also worked to ensure data availability, integrity, and confidentiality by implementing ciphers and data availability. A stringent system that can prevent unauthorized access to medical records and later distinguish between malicious and benign intentions is necessary because the techniques showed the least amount of resilience against the attacker despite the fact that both strategies included encryption and cryptographic solutions. A lightweight naive Bayes classifier that provided an effective and privacy-preserving model was employed in the work presented by the authors in [8]. The work's goal was to offer end consumers online primary diagnostic services without jeopardizing data privacy. According to their method, the patient's inquiry is sent directly to the server or service provider, and they will only be able to view the analysis result once it has been decrypted in order to secure medical records. Another method described in [9] employed a watermarking technique that comprised the key and image transform coefficients. The method guaranteed protection against attackers by complicating data flow and making it hard to interpret. Despite their many benefits AI-based healthcare systems are easily imitated once they are put into place, which suggests the possibility of hostile attacks by an invader. Blockchain enhances the security of data collected from wearables. The technique improves privacy and builds confidence between many organizations involved in the healthcare system by storing data inflexibly. In [10-11], a system was established that included the attributes of health insurance portability and accountability. The data used by the writers came from central servers and wearable technology. Their lightweight approach made use of negotiated keys and a chaotic map design. Additionally, they focused on security, taking into account blockchain technology and guarding against data tampering. The goal of the work in 13 was to prevent intruders or attackers from manipulating doctor’s prescriptions. They created a blockchain-based, intelligent, transparent, and reliable pharmaceutical supply chain management system and made sure that patients received prescriptions that had not been tampered with to improve the security of the data on wearable devices. A blockchain-based highly trustworthy and safe system that integrates AI is desperately ended. This is due to the fact that wearable device security vulnerabilities cannot be addressed alone by utilizing the blockchain. The BAIST, a proposed blockchain-AI integrated safe and reliable framework, makes use of a machine learning model that was trained on a publicly accessible benchmark dataset that includes both normal and attack samples taken from wearable medical equipment. The goal is to use AI to classify the patient data and then restrict and allow it to enter the blockchain while the attacker samples are eliminated. The data from the confirmed patients is permitted to enter the system according to performance metrics. The suggested bait framework performed better than rival models in differentiating between secure and normal data.

2. MOTIVATION AND BACKGROUND

Millions of individuals worldwide suffer from a variety of illnesses and conditions that have a direct or indirect impact on the healthcare industry using a variety of methods medical care facilities gather patient personal and medical information which is then stored for study considering how private patient information is a lot of money is spent protecting it from unwanted access news broke that such data had been compromised by cyber-attacks and patient information was made public this was because the security only used one technology 1415 instead of a strong foundation. millions of people’s lives might be at danger if such private information is compromised in order to counter the growing number of cyber-attacks the research community that works to safeguard healthcare systems has combined AI with healthcare clinical information demographic information photographs videos claims and more are all included in patient records when it comes to analyzing such information AI excels at identifying patterns and insights that humans would not be able to discover on their own AI on its alone is insufficient to combat cyber attacks the location where data is stored should be protected to this purpose the blockchain can offer immutability and security it can lessen the blockchains internal intrusion. Proposed study uses artificial intelligence AI and healthcare integration to distinguish between normal and manipulated samples because an attacker needs access to more than 50 of the nodes that comprise theblockchain in order to alter data this strengthens data resilience and prevents the blockchain curtain from being lifted especially for the public blockchain.

3. RESEARCH CONTRIBUTIONS

In order to effectively identify attacker samples from healthcare samples obtained from wearable devices we suggest a blockchain-AI integrated safe and reliable architecture dubbed BAIST the a machine learning approach that incorporates SVM identifies malicious samples by appropriately picking the relevant characteristics from the dataset the framework uses a method for choosing features that chooses important characters from the available attributes of the WUSTL EHMS 2020 dataset using the min-max values of the current low-count class samples the imbalanced dataset is appropriately balanced the when the BAIST frameworks classification accuracy was compared to comparable state-of-the-art studies the findings were impressive.

the article is structured as follows and an overview of relevant literature is provided in portion 2 the immediate portion in section 3 the materials and the suggested BAIST approach used for attack detection are described while section 5 wraps up the study with future scope section 4 gives the experimental analysis and discussion utilizing the suggested BAIST framework.

4. RELATED WORK

The authors in [16] conducted research that was restricted to IoT testbeds and proposed solutions for the security of smart devices at the same time they kept information secure the behaviour of the suggested model would be unpredictable because it was not tested on actual data samples a lightweight architecture for wireless sensor networks with medical applications was used to authenticate the communication between sensors and medical professionals [17-18] in [19] an effective architecture was proposed to stop hackers from gaining access to central systems and attacking devices from peeping their authentication method for IOT in medical applications made advantage of physically features their authentication method however was unable to withstand sophisticated decryption tools that may have decrypted the encrypted keys.

In [20] the authors presented a nonlinear SVM-based online cathartic pre-diagnosis system for data privacy that demonstrated prediction effectiveness using machine learning approaches the authors were able to identify dangerous tasks in smart healthcare systems with the greatest classification accuracy of 90% [21] they used four distinct machine-learning approaches to assess their model however the authors in [21] made an effort to identify fraudulent medical equipment they identified fraudulent devices linked to the healthcare system by combining a trust-based approach with bayesian inference the work demonstrated no involvement in integrity or data manipulation attacks.

In [23] a clever internet health system was unveiled the system used blockchain technology to automatically transmit medical data based on a modified merkel scheme they suggested a tree-based data structure for secure and rapid patient information access [24-25] a simulation-based healthcare system was assessed Ethereum and incentives were the cornerstones of the authors approach their model proposed a novel approach that effectively yielded greater results for the least amount of money spent they demonstrated how reduced spending and higher prices might lead to destructive attacks on the blockchains bribed self-mining system the approach focused on mining assaults instead than malicious attacks on the blockchain in [26] an Iot-enabled healthcare systems defense against intrusion assaults was shown.

To identify the intrusion and ensure safe information transmission the author employed deep learning and blockchain technology however the author failed to include the patients genuine medical information which may endanger the patient's life if it were maliciously altered and entered the blockchain a similar dataset for every patient in the blockchain-based healthcare setting was proposed by work in [27] although they proposed a sophisticated 5G architecture for the system they were unable to manage real-time data in [28] a sophisticated model for identifying irregularities in the patients file was presented in [29] a secure healthcare network was created that connected administrators physicians pathology labs and patients nevertheless the system was unable to function effectively in a comprehensive way.

Since none of the work examined above has combined both technologies to address the security issue pertaining to Wearable devices the research and analysis above demonstrated the urgent need to combine blockchain and additionally secure Artificial intelligence-powered healthcare systems were able to identify attacker samples with up to 93% accuracy which ultimately made it possible for malicious data to infiltrate the blockchain.

5. THE MATERIAL AND THE PROPOSED BAIST FRAMEWORK

By keeping hostile data off of the blockchain the suggested BAIST architecture is integrated between the patients wearable device and the blockchain to offer strong security by doing this the patients valuable lives will be shielded from potentially fatal knowledge thus the blockchain and ai module are integrated by the BAIST architecture which enables the network to transmit genuine information an intruder can intentionally alter the contents obtained from the patients wearable devices by intercepting data before it enters the server through the gateways sensitive physical characteristics and the patients personal information are the subject of potential alterations or changes that might compromise an accurate diagnosis and treatment ultimately endangering the patient's life. thus by detecting fraudulent samples and preserving data integrity the BAIST counters the threats the harmful samples identified by the BAIST architecture are eliminated and kept out of the blockchain that patients pathologists system administrators and healthcare professionals share as a result the suggested architecture guarantees that pathologists will conduct correct analyses that medical professionals will diagnose and treat patients appropriately that patients will receive effective therapy and that administrators will design monitor and execute databases efficiently figure1 depicts the blockchain-AI integrated model the data transmitted by wearable technology forms the foundation of the EHMS test bed physical parameters obtained from the sensors attached to the patients internal or exterior body parts make up the database even though it was built using the EHMS testbed.

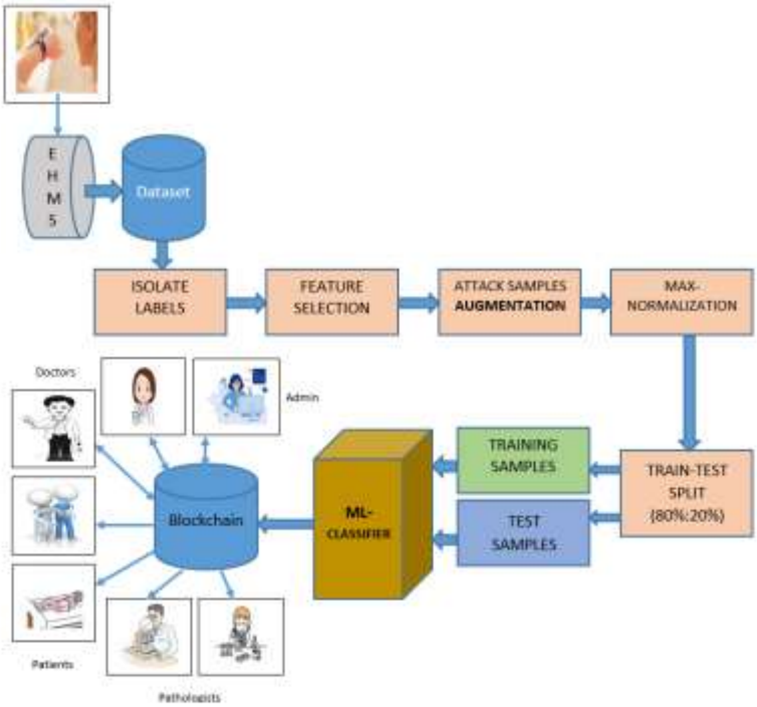


Figure 1: The Proposed BAIST Framework

Feature Selection Strategy

The labels of the dataset samples are first separated from the datasets last column attribute-44 numerous tests were conducted in order to extract pertinent characteristics from the dataset in order to increase the accuracy of detection and classification value changes in each characters column were used to determine the characteristics that were noteworthy or pertinent in the first instance each feature had several value adjustments out of 43 traits 33 were found to be meaningful in the first phase of the character selection technique 1, 3, 4, 6, 11, 12, 16, 22, 24 and 34 were removed since they don't help differentiate between attack and normal samples for feature 5 a maximum value change of 16315 was discovered. according to the experiment the classification accuracy was restricted to 9092 when 33 characteristics were used we classified the accessible characteristics by removing additional features according to the analysis the classification rate would rise if the feature values of the remaining characteristics changed by more than 3 consequently we removed features in the second stage when the value changes were smaller than three in comparison to the previous classification accuracy of 92 we discovered that 27 characteristics were important table 1 lists the noteworthy feature headings that were discovered during the feature selection process in 3031 the full feature description and feature type are described.

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**			

textual values (M, M*, Md, MR, e, es, and eR) corresponds to column 2 out of the 27 significant characteristics the other feature values in the other columns are numeric we identified the unique text values in the original datasets flg column feature 2 and replaced them with numbers ranging from 1 to 7 .The M-1, M*-2, Md-3, MR-4, e-5, es-6, and eR-7 stood for the textual values. we discovered that an unbalanced dataset caused the classification accuracy to decline while employing the 27 relevant columns because there were far more normal samples 14272 than assault samples 2046 the attack samples were incorrectly categorized in other words the classifier favoured the typical samples however the classification accuracy fell below 92 when the characteristics were further reduced the work done in [32] has confirmed the same thing the authors varied the number of features from 5 to 44 in order to evaluate an ISTM network and four machine learning algorithms as the number of characteristics rose they achieved greater accuracy to balance the dataset the low-count class samples have to be supplemented.

Augmentation of the Attack Samples

We supplemented the attack samples using a new method using the feature selection technique we first separated the attack samples from the normal samples by taking into account 27 important columns each characteristic in the attack samples was then given a unique value we randomly selected the unique values from each feature and concatenated them to create a feature vector of 27 values in order to generate 14272-2046 = 12226 attack samples however for the characteristics Flgs, SrcBytes, DstBytes, SIntPktAct, TotPkts, TotBytes, pLoss, pDstLoss, SpO2, and SYS the number of unique values corresponding to the attack samples was too low to compensate 12226 samples which would have resulted in duplicate samples in the attack intra-class. additionally features pLoss and pDstLoss included just two unique values including a 0 value whereas features SIntPktAct had no unique values other than 0 as a result redundant samples were identified from the created samples using a different algorithm and the redundancy was removed and covered by creating a fresh set of samples upon manual examination it was discovered that the SIntPktAct feature creates misunderstandings about discrimination across classes there were eight distinct values in the column including 0 however only a value of 0 represented the attack samples but all of the finite unique values indicated the normal class in order to clear up any confusion at the classifier the feature was removed. The indicated feature that is indicated in red was removed is seen in figure 1 lastly using the supplemented data the classifier was trained using 26 characteristics.

Aug Normalization and Split

A max-normalization approach was used to normalize the feature values since each feature has a unique range of values each feature columns maximum value is determined and each value is then divided by the maximum value to accommodate all values in the range 0-1 because enhanced samples were added the samples were separated and the labels were recreated in addition to reducing the features dimension principal component analysis PCA is used to convert the features to other coordinate axes twenty PCA components were chosen for this project to divide the samples into training and test sets a ratio of 8020 was used the samples from both classes were concatenated together with their corresponding labels.

The Machine Learning–Based Classifier

To categorize the groups using SVM, we employed a radial basis function kernel and a SGDA optimizer in contrast to the performance of the SVM in relation to other optimizers was found to be closer but still subpar.

The Dataset

The Enhanced Healthcare Monitoring System, a real-time testbed, was used to build the WUSTL EHMS 2020 dataset [33–34]. Network traffic metrics were coupled with the patient's biometrics to make up for the dataset's lack of availability. The testbed was divided into four parts: the network, the gateway, the physical sensors, and the visualization control portion. The patient's body provides the sensor with the physical parameter, which it then transmits to the gateway. The server, which is connected to the switch and router, is where the data is displayed. Before the data reaches the server, an intrusion may take place.

To construct the WUSTL EHMS 2020 dataset in order to compensate for the datasets network traffic indicators were combined with the patients biometrics in a real-time testbed enhanced healthcare monitoring system absence of availability physical sensors the four components of the testbed were the network [33-34] the gateway and the visualization control area after the sensor collects the physical parameter from the patient’s body the switch and router send the information to the server for visualization there is a chance that an intrusion will occur before the data reaches the server.

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

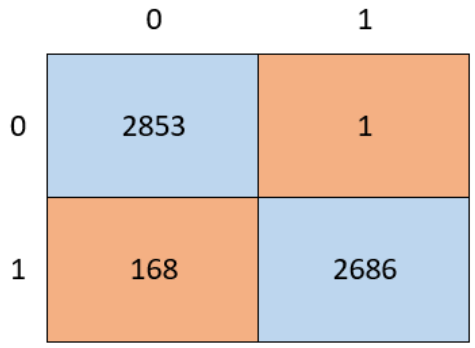
6. RESULTS AND DISCUSSION

The intrusion detection systems BAIST architecture was tested using MATLAB 2019b and assessed based on several performance metrics the framework ran on a 284 GHz Intel i5 processor running windows 11 with 16 GB of RAM and 512 GB of SSD an improved understanding of a models performance on a certain dataset is provided by accuracy table 3 displays the machine learning models performance for the IDS in terms of f1-score precision recall and training and test accuracies the confusion matrix derived from the BAIST framework is displayed in table 4. with a score exceeding 97% the IDS framework performs similarly both qualitatively and numerically according to the confusion matrix analyzed over the test samples, the assault samples demonstrated encouraging results while the normal samples were categorized with an impressive 99.96% accuracy 94.11% was the assessed classification accuracy for the susceptible samples.

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 erroneously categorized attack samples are the result of constrained augmentation, and there are very few unique values that correspond to some characteristics 11 features even though the attack samples are enhanced from the existing attack samples utilizing their range values at least for the characteristics with relatively few unique values the likelihood of comparable or nearby samples is increased by generating 12226 examples the attack samples are aligned in the normal class because of the increased imbalance which gives the normal network traffic class the upper hand nonetheless the BAIST model can more accurately distinguish between normal samples.

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**

Regarding the WUSTL EHMS 2020 dataset table 5 compares the performance of the suggested BAIST framework for IDS with that of other recent competing models 186 samples in the dataset are impacted even if the tables highlighted accuracy statistics only indicate a 0.65% improvement over the work done in [38] and [40] the suggested model is qualitatively superior as evidenced by the higher precision not calculated in[38] and [40] using the BAIST framework the work suggested in [41] however has a poor harmonic average despite being numerically rich the feature selection technique which guarantees improved sample representation using the chosen features is a crucial component of the BAIST system.

7. CONCLUSION

In comparison to other previous models the BAIST framework which was established in this work to detect vulnerable samples infected by spoof assaults manipulations and hijacking attempts performed better the model is based mostly on a feature selection method and is straightforward and effective to choose important features that will represent the network traffic samples a more thorough study of the available features is conducted for 20% of test data from both categories the classification accuracy is over 97% demonstrating the benefit of the feature selection approach to verify the wearable devices validity the combined ai-blockchain method first identifies the dangerous or susceptible samples from the WUSTL EHMS 2020 dataset. additionally the blockchain discards the soiled or fraudulent wearable data while allowing the data from the genuine wearable to enter the pure or authentic samples are stored in the immutable ledger after the network accepts them low-count features 43 non-variability of features 11 features and imbalanced nature impose complexity despite the efforts of various researchers to clean the data and identify the legitimate devices using various methodologies incorporating machine learning and deep learning techniques by focusing on 26 features that our feature selection algorithm has determined to be essential this paper will help interested researchers create a better IDS model. enhancing performance will reduce the connected patients chance of death give pathologists real biometric and flow metric data and ultimately lead to more reliable doctor-patient coordination future improvements to the BAIST model will focus on improving the augmentation approach correctly sequencing features prior to training and testing and creating and optimizing sequential custom networks.

REFERENCES

[1] Tanwar, S., Vora, J., Kaneriya, S., Tyagi, S., Kumar, N., Sharma, V., & You, I. (2020). Human arthritis analysis in fog computing environment using Bayesian network classifier and thread protocol. *IEEE Consumer Electronics Magazine, 9*, 88–94. https://doi.org/10.1109/CCEM.2020.9101655

[2] Patel, K., Mehta, D., Mistry, C., Gupta, R., Tanwar, S., Kumar, N., & Alazab, M. (2020). Facial sentiment analysis using AI techniques: State-of-the-art, taxonomies, and challenges. *IEEE Access, 8*, 90495–90519. https://doi.org/10.1109/ACCESS.2020.2994421

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

[4] Giliyar, A. (2022, December 22). *Evolution of health data storage for digital healthcare*. LinkedIn. https://www.linkedin.com/pulse/evolution-healthdata-storage-digital-healthcare-ambarish-giliyar/

[5] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. *IEEE Access, 8*, 168825–168853. https://doi.org/10.1109/ACCESS.2020.3026810

[6] Noura, M. (2019). *Efficient and secure cryptographic solutions for medical data* (Doctoral dissertation). Université Bourgogne, Dijon, France.

[7] Kester, Q. A., Nana, L., Pascu, A. C., Gire, S., & Eghan, J. M. (2015). A cryptographic technique for security of medical images in health information systems. *Procedia Computer Science, 58*, 538–543. https://doi.org/10.1016/j.procs.2015.08.084

[8] Liu, X., Zhu, H., Lu, R., & Li, H. (2018). Efficient privacy-preserving online medical primary diagnosis scheme on naive Bayesian classification. *Peer-to-Peer Networking and Applications, 11*, 334–347. https://doi.org/10.1007/s12083-017-0591-9

[9] Rai, A., & Singh, H. (2017). SVM based robust watermarking for enhanced medical image security. *Multimedia Tools and Applications, 76*, 18605–18618. https://doi.org/10.1007/s11042-016-4136-9

[10] Gupta, R., Shukla, A., & Tanwar, S. (2020). AaYusH: A smart contract-based telesurgery system for healthcare 4.0. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1–6). Dublin, Ireland. https://doi.org/10.1109/ICCWorkshops49005.2020.9145274

[11] Singh, R., Tanwar, S., & Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. *Security and Privacy, 3*, e96. https://doi.org/10.1002/spy2.96

[12] Lee, T. F., Chang, I. P., & Kung, T. S. (2021). Blockchain-based healthcare information preservation using extended chaotic maps for HIPAA privacy/security regulations. *Applied Sciences, 11*, 10576. https://doi.org/10.3390/app111110576

[13] Zhu, P., Hu, J., Zhang, Y., & Li, X. (2020). A blockchain-based solution for medication anti-counterfeiting and traceability. *IEEE Access, 8*, 184256–184272. https://doi.org/10.1109/ACCESS.2020.3031423

[14] Tauqeer, H., Iqbal, M. M., Ali, A., Zaman, S., & Chaudhry, M. U. (2022). Cyberattacks detection in IoMT using machine learning techniques. *Journal of Computer and Biomedical Informatics, 4*, 13–20. https://doi.org/10.2139/ssrn.3901239

[15] Lu, W. (2023). Detecting malicious attacks using principal component analysis in medical cyber-physical systems. In *Artificial Intelligence for Cyber-Physical Systems Hardening* (pp. 203–215). Springer.

https://doi.org/10.1007/978-3-030-91607-6_12

[16] Yeh, K. H. (2016). A secure IoT-based healthcare system with body sensor networks. *IEEE Access*, *4*, 10288–10299. https://doi.org/10.1109/ACCESS.2016.2638038

[17] Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems*, *82*, 727–737. https://doi.org/10.1016/j.future.2017.10.003

[18] Banerjee, S., Odelu, V., Das, A. K., Chattopadhyay, S., Kumar, N., Park, Y., & Tanwar, S. (2018). Design of an anonymity-preserving group formation based authentication protocol in global mobility networks. *IEEE Access*, *6*, 20673–20693. https://doi.org/10.1109/ACCESS.2018.2816807

[19] Yanambaka, V. P., Mohanty, S. P., Kougianos, E., & Puthal, D. (2019). PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things. *IEEE Transactions on Consumer Electronics*, *65*, 388–397. https://doi.org/10.1109/TCE.2019.2907581

[20] Zhu, H., Liu, X., Lu, R., & Li, H. (2017). Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. *IEEE Journal of Biomedical and Health Informatics*, *21*, 838–850. https://doi.org/10.1109/JBHI.2016.2633960

[21] Newaz, A. K. M. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2019). HealthGuard: A machine learning-based security framework for smart healthcare systems. *arXiv*. https://arxiv.org/abs/1909.10565