Enhancing Healthcare Security with Blockchain and AI-Based Anomaly Detection

1st Rao Sharif Mansoob
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Punjab, Pakistan
raosharif.studies@gmail.com

2nd Muhammad Shoaib
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Punjab, Pakistan
Muhammadshoaib.studies@gmail.com

3rd Eman Fatima
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Punjab, Pakistan
emanfatima60860@gmail.com

4th Iftikhar Rasheed
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Punjab, Pakistan
iftikhar.rasheed@iub.edu.pk

5th Umar Fayyaz
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Punjab, Pakistan
umar.fayyaz@iub.edu.pk

***Abstract*—With the quick integration of digital solutions in healthcare systems, the importance of cybersecurity has become a significant concern. Safeguard sensitive patient data against cyber threats. This paper presents a novel approach to enhance the security of healthcare systems through the integration of blockchain technology and AI-based anomaly detection, thereby reducing the risk of brute force attacks. The system utilizes the Ethereum blockchain, offering a decentralized and tamper-proof nature that is used as an authentication mechanism for both the patient and the doctor. A secure and friendly web interface is developed for registration and login purposes, which allows users to log in where data integrity is preserved via blockchain smart contracts. Additionally, doctors can upload the medical data, like patient reports, to IPFS (via Pinata) ensuring decentralized and secure storage. To enhance security, we use supervised machine learning algorithms and apply random forest to detect brute force attacks on user accounts. Our AI model smartly separates the lawful user access and the unauthorized access by looking out for the login patterns and suspicious activity. The system is evaluated by using precision, recall, F1-score, and ROC-AUC metrics. The system's accuracy is so perfect that it accurately makes a difference between brute force attacks and legitimate logins in the system. Our proposed solution provides a user-friendly interface, enables stakeholders to interact efficiently with their data, and protects their accounts from unauthorized access.**

***Index Terms*—smart healthcare systems, cyber security, data privacy, blockchain, artificial intelligence, smart contracts, anomaly detection, supervised machine learning**

I. Introduction

The majority of businesses, institutions, and organizations employ third-party-managed centralized networks; transactions are sent in a centralized fashion, which leads to less effective data flow [1]. Blockchain technology has been implemented to safeguard resources, address central control challenges by overcoming bottleneck concerns, and optimize storage locations [2]. **Blockchain technology** has influenced numerous industries in recent years because to its distinctive and effective method of storing and sending data in a traceable and secure manner. The blockchain plays a crucial role in safeguarding user data and ensuring the anonymity of network participants. Moreover, blockchain technology has emerged as the optimal ledger for data transport and storage; it is a decentralized, tamper-proof ledger with guaranteed security [1], [3].

Effective access control models for healthcare systems must include security and privacy [4]. The adoption of key enabler technologies like blockchain, artificial intelligence (AI), the Internet of Things (IoT), and next-generation wireless networks (5G/6G) has significantly changed the healthcare industry. Individuals' quality of life and healthcare services have increased as a result of the healthcare industry's embrace of these technologies. [5], [6]. Clinical trials, patient medical records, and medical analytics are just a few examples of the vast amounts of data generated by the healthcare sector. It is not scalable or secure to store all of this data in one location. Blockchain is therefore the best choice to guarantee patient data integrity and confidentiality [7], [8]. Blockchain offers a decentralized framework for managing and storing data to prevent potential fraud or data loss [9]–[11].

Consequently, the researcher has embraced blockchain technology defined by decentralization, immutability, transparency, and security [12], [13], [14]. Pinto et al. in [15] examined the advantages of blockchain technology in the smart healthcare system, addressing the challenges of data integrity, transparency, and security. They presented a verifiable approach for electronic health records, enabling secure data flow between patients and users. A private blockchain was utilized through the implementation of HyperLedger Fabric, which maintains two distinct databases for data traceability [5].

The growing number of cyberattacks occurring in the healthcare ecosystem can be effectively addressed by implementing AI technology in smart healthcare systems [16]. In order to provide an autonomous security solution, the AI is crucial in analyzing the malicious actions of the attacker [5]. Despite the

© 2025 TechShield Publications
DOI: https://doi.org/10.67535/tsp.000001.003
Published under the ICACNC 2025 Proceedings

potential advantages of blockchain technology, it faces certain problems, and artificial intelligence is being utilized to address these issues [17]. Anomaly detection is essential in healthcare data because of the difficulties related to the integration of intelligent technology and healthcare. Anomalies in electronic health records may indicate an insider attempting to access and modify the data [18].

Given the fast increase in cyber attacks on healthcare systems, it is essential to implement measures that safeguard the privacy and security of patient data. Our proposed solution **Enhancing Healthcare Security with Blockchain and AI-Based Anomaly Detection**, not only secures patient data utilizing secure data storage, secure access control and secure data sharing but also identify and figure out unusual patterns and outliners in data in real time, preventing potential security threats and inefficiencies.

II. Proposed Methodology

Our proposed methodology is outlined in the block diagram given in Fig. 1, which represent the each step of Enhancing Healthcare Security with Blockchain and IPFS.

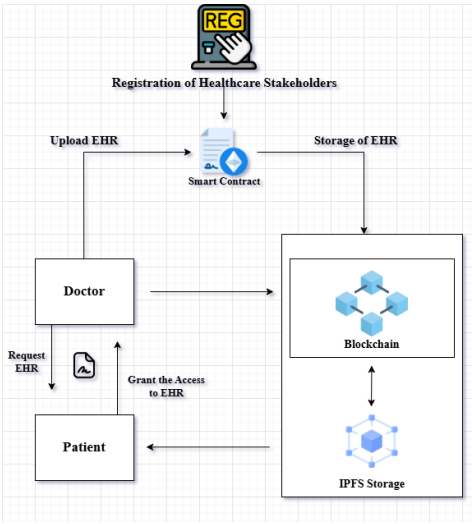

Fig. 1. Block Diagram for Proposed Model

A. Registration of Healthcare Stakeholders

Doctors, nurses, patients and laboratory staff will be considered as Stakeholders. Before interacting with the system, they have to register themselves using their meta-mask account addresses.

For sake of simplicity, we only mentioned doctor and patient in the block diagram of our system.

- **Doctor's Roles and Responsibility:** Doctors can only upload the electronic health records including medical reports etc of their corresponding patients into the system. Blockchain transactions require gas fees, making it difficult for the patients to directly upload their EHR into the system, that's why doctor is assigned to upload the EHR to make cost efficient system for the patients.
- **Patient Centric Data Sovereignty:** Patient retains the ownership of data.
  In proposed model, patient have to grant access to doctor so that, only authorized doctor can view or upload the corresponding patient's EHR to the system. This feature makes the patient supreme power in the system having complete control over the medical data.

B. Blockchain Used

The proposed system employs the **Ethereum Blockchain**. Ganache is a local platform for building blockchains that we used. A free and open-source Ethereum blockchain development platform, Ganache provides 100 ethers for ten account addresses. [19]. The Ethereum blockchain is presently one of the most well-known public blockchains [20]. The Ethereum blockchain utilizes Ether as a reward for the first node that successfully mines a block [21]. Once a block is confirmed and included into the chain, it cannot be removed [22]. The hash value of the desired block and all subsequent blocks must be recalculated when a block is modified or changed, making it extremely difficult for attackers to fabricate [23], [24]. Furthermore, attackers cannot alter a blockchain because it is kept across multiple nodes in a decentralized fashion [20], [25].

C. Smart Contract Design

The primary components of smart contracts include functions, events, state variables, and modifiers, all of which are articulated in the high-level programming language known as **Solidity**. The Remix and Kovan test networks have been utilized to deploy smart contracts on the testnet and to use testnet ethers for transaction fee payments. The production of a smart contract involves three stages: writing, compiling, and deploying, utilizing the Solidity programming language. Fig 2 illustrates the smart contract between doctor and patient. The bytecode is produced by the Solidity real-time compiler. The Ethereum Wallet has been employed for the deployment of smart contracts to the blockchain. [26].

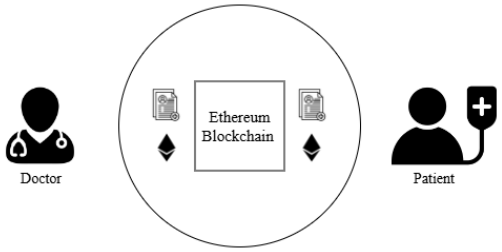

Fig. 2. Smart Contract Between Patient and Doctor

D. Storage Mechanism (Blockchain and IPFS)

We are using IPFS(InterPlanetary File System) to store patient's medical reports instead of storing them on the blockchain which would be expensive.

- **Blockchain Storage:** Blockchain (Ehtereum) is used to store;

- Smart Contracts
- Access Control Permissions (who can view or upload data)
- IPFS Hashes
- Anomaly Alerts

- **IPFS for Patient's Reports:** One such distributed file system is IPFS, which tries to connect all computers to one central server [27]. Therefore, IPFS aims to give computers a means of accessing and transferring data without the need for any central servers. Although universal adoption is the aim, not all client-server systems will necessarily be replaced. Nevertheless, IPFS offers a different framework in which information is not centralized and can circulate freely with virtually no chance of restriction [28]. The content of a file is hashed when it is uploaded to IPFS. The file can be retrieved using this hash, which gives the content a unique identity. The hash will be entirely different if we upload a different file, but we can always recalculate the hash locally to make sure it matches the original IPFS hash [29]. We are going to use **Pinata**; IPFS Pinning Service which enables users to easily upload and retrieve files from decentralized network.
- **Limitations of Blockchain and IPFS:** For sake of balanced and objective viewpoint, we are discussing the limitations of Blockchain and IPFS.
  The potential of blockchain technology to provide a variety of unique advantages in comparison to conventional centralized architectures is significant. Nevertheless, the technology demonstrates a number of constraints that must be taken into account when constructing a business case for its adoption [30], [31]. Following are the limitations of blockchain technology:
  - **High costs:** Replicating transaction history across all nodes in the blockchain is computationally expensive. This feature improves security but limits larger networks.
  - **Security model:** Blockchain transactions are authenticated and executed using public key encryption. This secure process requires public and private keys. The system has no added security if a party loses or accidentally publishes their private key.
  - **Flexibility limitations:** While blockchain's immutable append only nature ensures transaction integrity, it can hinder use cases that require transaction changes.
  - **Latency:** Every node in the blockchain stores the complete transaction history of every information block to ensure network security. Nevertheless, it currently takes a lot of time to add new blocks and transaction records [32]–[40].

  IPFS targets Web efficiency, decentralization, and resilience. Content-based addressing in IPFS addresses content rather than locations. Data is efficiently stored in IPFS due to its deduplication properties [41]. Following are the limitations of IPFS:
  - **Scalability Issues:** IPFS's low scalability may be due to each instance's limited bandwidth [42]. According to studies [43], [44], distributed file systems like IPFS are still developing. For instance, IPFS still has resolving and downloading bottlenecks and high I/O latency. IPFS must solve storage optimization, geo-distributed node deployment, file request performance, and other issues to support large-scale commercial applications.
  - **Privacy and Security Issues:** Although IPFS helps to share data, it now lets everyone in the network access kept files, which raises privacy issues. Extra security calls for additional protections including data hiding techniques and permission restrictions [45], [46].

E. AI-Based Anomaly Detection

Anomaly detection algorithms are models employed to identify harmful activities within healthcare systems. Anomaly detection algorithms can identify irregular network traffic or doubtful behavioral patterns inside the system, which can subsequently be utilized to initiate alarms or implement other precautionary measures [47].

We are employing two supervised machine learning algorithms: **Random Forest (RF)** and **Support Vector Machine (SVM)** for the identification of brute force attacks.

The proposed machine learning approach detects brute force attempts on our system is described in Fig 3.

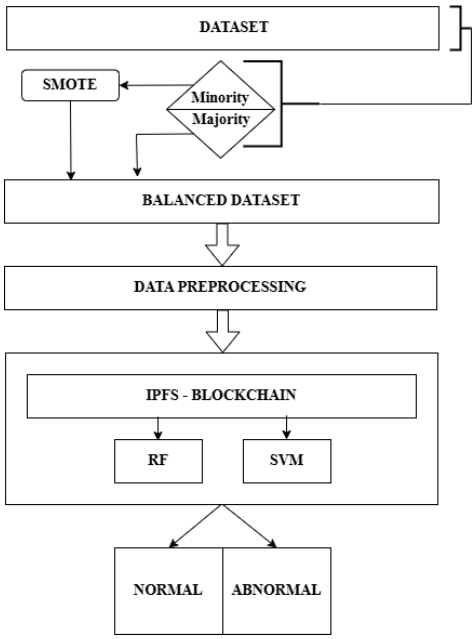

Fig. 3. Proposed Machine Learning Model

F. Environmental Setup Details

Our proposed solution implemented using python and its libraries including a) Pandas and Numpy for data acquisition

and preprocessing b) Scikit-Learn for implementing machine learning algorithms (e.g, RF and SVM).

G. Dataset Used

A well-structured and behaviorally rich dataset was used to train and evaluate the proposed anomaly detection framework. Among its many components are user identification (IP address, user ID), time information (timestamp), location information (user), device and browser information (user agent), and event information (login status, unsuccessful attempts, attack label).

Random Forest (RF) and Support Vector Machine (SVM) were employed to discern intricate and non-linear patterns in login data. These algorithms exhibit strong performance and precise classification for both balanced and imbalanced datasets. An alternative was to exclude K-Nearest Neighbors (KNN) and Naïve Bayes, which necessitate robust data distribution assumptions or extensive datasets. Empirical analysis demonstrated that RF and SVM exhibited greater reliability and precision compared to alternative brute-force attack detection models.

III. Implementation

A. Blockchain Development

As we described in methodology, we used solidity language for designing the smart contracts. We designed three smart contracts for admin, doctor and patient. For instance, admin smart contract is given below:

- **Algorithm: Smart contract for administrative information**
  Input: Hospital information including name, location, services offered, operating hours, profile name, and password.
  Output: HospitalRegistry Smart Contract Instance.
  1) Specify the Solidity version.
  2) Make the contract with the name **HospitalRegistry**.
  3) Define a struct **Hospital** that contains private members: name, location, services, workingHours etc.
  4) Create a mapping of address to Hospital to store hospital details and a list of registered hospitals.
  5) Define events for tracking hospital registration, updates, deletion, and admin authentication.
  6) Implement the **registerHospital** function:
     Ensure the hospital is not already registered.
     Store the hospital details and mark it as registered.
  7) Implement the **authenticateAdmin** function:
     Ensure the hospital is registered.
     Verify the profileName and password by hashing and comparing them.
     Return **true** if authentication is successful; otherwise, return **false**.
  8) Implement the **deleteHospital** function:
     Ensure the hospital is registered.
     Remove the hospital's record from the mapping.
     Remove the hospital's address from the hospitalAddresses array.
     Emit the **HospitalDeleted** event.
  9) Implement the **getAllHospitals** function:
     Retrieve all registered hospital details.
     Return the list of hospitals.

B. Interplanetary file storage

A decentralized cloud platform called Pinata has been utilized to store patient medical reports and images. Data is stored and retrieved from the cloud using the Pinata Python API. Every image submitted to the Pinata Cloud generates an IPFS hash that is saved in the blockchain [19].

C. AI-Based Anomaly Detection

- **Description of Steps Involved in AI-based Anomaly Detection**
  After reviewing the current work in machine learning, we come to point that, resampling techniques and feature selection enhances the performance of ML models.
  - **Synthetic Minority Oversampling Technique (SMOTE):** We used the SMOTE approach to obtain balanced datasets, as shown in figure 3. The premise behind this approach is to oversample the minority class by creating artificial instances from its constituents while maintaining the majority number. In addition to being exact replicas of minority cases, the new samples are produced by combining features from the minority instances and their nearest neighbors in the feature space. [48], [49].
  - **Data Preprocessing:** In order to deal with the examples of raw data sets, some analysis and display of the included values are necessary. Duplicating some rows can lead to overfitting issues. Spaces, nulls, and other sorts of data are examples of filthy values found in some columns. The chosen dataset should be preprocessed to remove any flaws that could interfere with the postprocessing procedure in order to address the aforementioned issues [49]. We employed z-score normalization, one hot encoding, and data cleaning as part of the preprocessing step.
  - **Feature Selection:** By choosing the most associated features, this phase lowers the computational cost of the high-dimensional feature space and helps create effective machine learning models [49]. We used **Variance Thresholding** to remove the features that have low variance with the attack. We selected those features which most influences the accuracy of model.

D. Performance Metrics

We evaluated the performance of our model as follow: Evaluation metrics are essential for assessing the performance of machine learning models. The following standard metrics were used to evaluate the effectiveness of our anomaly detection system:

Accuracy measures the proportion of correctly predicted instances among the total number of cases:

$$\text{Accuracy} = \frac{\text{True Positives} + \text{True Negatives}}{\text{Total Number of Instances}} \tag{1}$$

Precision indicates the proportion of correctly predicted positive observations to the total predicted positives:

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \tag{2}$$

Recall, also known as sensitivity, measures the proportion of actual positives correctly identified:

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \tag{3}$$

F1 Score is the harmonic mean of Precision and Recall, providing a balance between the two:

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

TABLE I
PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS

Model	Performance Metrics			
	Accuracy	*Precision*	*Recall*	*F1 Score*
RF	0.97	1.00	0.94	0.97
SVM	0.96	1.00	0.92	0.96

Table I illustrates that the Random Forest (RF) model beats the Support Vector Machine (SVM) regarding recall and F1-score, establishing it as the optimal selection for our classification task.

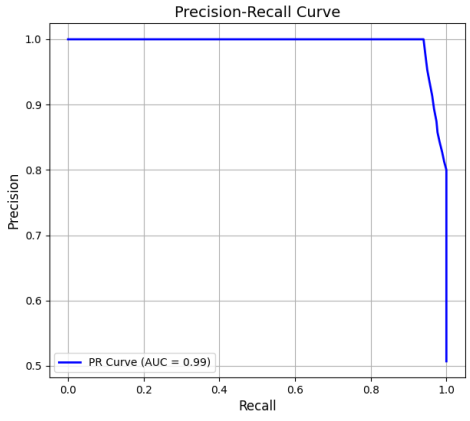

Fig. 4. Precision Metrics

The Precision-Recall Curve, shown in Fig. 4, shows outstanding effectiveness in identifying abnormalities with very few false positives.

ROC-AUC (Receiver Operating Characteristic - Area Under Curve) is a performance measurement for classification problems at various threshold settings. One key component of ROC is the False Positive Rate (FPR), defined as:

$$\text{FPR} = \frac{\text{False Positives}}{\text{False Positives} + \text{True Negatives}} \tag{5}$$

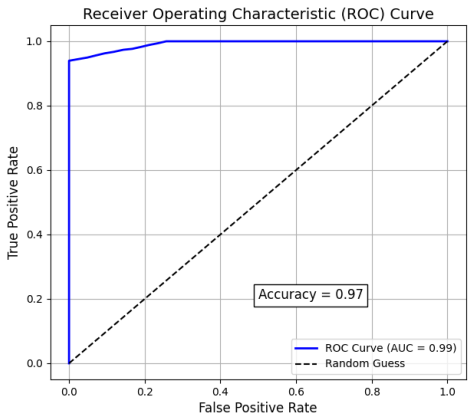

Fig. 5. ROU-AUC Curve

The True Positive Rate (Recall) is plotted against the False Positive Rate to create the ROC Curve, which illustrates the model's performance in Figure 5. A better model is indicated by a higher curve. The model appears to be very successful in differentiating between normal and abnormal activity, as indicated by its AUC of 0.99.

IV. CONCLUSION

In this paper, we proposed a smart and safe healthcare system utilizing blockchain technology with AI-driven anomaly detection. We guarantee data integrity and decentralization by using the Ethereum Blockchain for authentication, while IPFS (via Pinata) offers a safe and decentralized medical record storage option. By successfully detecting brute force login attempts, our Random Forest-based anomaly detection approach improves system security. When evaluating performance, criteria like precision, recall, F1-score, and ROC-AUC show that brute force login threats can be detected with high accuracy. The technology provides a user-friendly interface for smooth interaction in addition to reinforcing cybersecurity in the healthcare industry. Future research might concentrate on adding more blockchain security features and enhancing threat detection skills.

ACKNOWLEDGMENT

REFERENCES

[1] O. Fadi, Z. Karim, E. G. Abdellatif, and B. Mohammed, "A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments," *IEEE Access*, vol. 10, pp. 93 168–93 186, 2022.

[2] F. M. Benčić and I. P. Žarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in *2018 IEEE 38th international conference on distributed computing systems (ICDCS)*. IEEE, 2018, pp. 1569–1570.

[3] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, "Blockchain-powered parallel healthcare systems based on the acp approach," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 942–950, 2018.

[4] A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud, J. Ali, and M. Baz, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, p. 2034, 2021.

[5] A. Alabdulatif, I. Khalil, and M. Saidur Rahman, "Security of blockchain and ai-empowered smart healthcare: application-based analysis," *Applied Sciences*, vol. 12, no. 21, p. 11039, 2022.

[6] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, and E. Harjula, "Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications," *Sensors*, vol. 21, no. 7, p. 2502, 2021.

[7] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for iot applications: taxonomy, platforms, recent advances, challenges and future research directions," *Electronics*, vol. 11, no. 4, p. 630, 2022.

[8] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACm Computing surveys (CsUr)*, vol. 53, no. 2, pp. 1–27, 2020.

[9] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of network and computer applications*, vol. 135, pp. 62–75, 2019.

[10] Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 40, 2022.

[11] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-based uav path planning for healthcare 4.0: Current challenges and the way ahead," *IEEE Network*, vol. 35, no. 1, pp. 20–29, 2021.

[12] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned uav communication using 6g networks: Open issues, use cases, and future directions," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5416–5441, 2020.

[13] R. Gupta, A. Shukla, and S. Tanwar, "Aayush: A smart contract-based telesurgery system for healthcare 4.0," in *2020 IEEE international conference on communications workshops (ICC Workshops)*. IEEE, 2020, pp. 1–6.

[14] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a blockchain-based platform for healthcare information exchange," in *2018 ieee international conference on smart computing (smartcomp)*. IEEE, 2018, pp. 49–56.

[15] R. P. Pinto, B. M. Silva, and P. R. Inacio, "A system for the promotion of traceability and ownership of health data using blockchain," *IEEE Access*, vol. 10, pp. 92 760–92 773, 2022.

[16] K. Patel, D. Mehta, C. Mistry, R. Gupta, S. Tanwar, N. Kumar, and M. Alazab, "Facial sentiment analysis using ai techniques: state-of-the-art, taxonomies, and challenges," *IEEE access*, vol. 8, pp. 90 495–90 519, 2020.

[17] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE communications surveys & tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[18] M. Tabassum, S. Mahmood, A. Bukhari, B. Alshemaimri, A. Daud, and F. Khalique, "Anomaly-based threat detection in smart health using machine learning," *BMC Medical Informatics and Decision Making*, vol. 24, no. 1, p. 347, 2024.

[19] B. Gayathri D and D. Sangeetha, "Enhancing security in digitized healthcare system using blockchain technology," *Technology and Health Care*, vol. 32, no. 6, pp. 5105–5127, 2024.

[20] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 international conference on electrical and computing technologies and applications (ICECTA)*. IEEE, 2017, pp. 1–4.

[21] O. Ely, "What is the ether?" *Popular Astronomy, vol. 18, pp. 525-532*, vol. 18, pp. 525–532, 1910.

[22] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied innovation*, vol. 2, no. 6-10, p. 71, 2016.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Satoshi Nakamoto*, 2008.

[24] R. Bhuvana, L. Madhushree, and P. Aithal, "Blockchain as a disruptive technology in healthcare and financial services-a review based analysis on current implementations," *International Journal of Applied Engineering and Management Letters (IJAEML)*, vol. 4, no. 1, pp. 142–155, 2020.

[25] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain application in healthcare systems: a review," *Systems*, vol. 11, no. 1, p. 38, 2023.

[26] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, p. 94, 2020.

[27] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[28] D. Ward, "An analysis of the interplanetary file system and its future."

[29] N. Sangeeta and S. Y. Nam, "Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks with keyword search capability," *Electronics*, vol. 12, no. 7, p. 1545, 2023.

[30] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain–the gateway to trust-free cryptographic transactions," in *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016*. Springer Publishing Company, 2016, pp. 1–14.

[31] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services," *Journal of management information systems*, vol. 35, no. 1, pp. 220–265, 2018.

[32] Axios, "Corporate america's blockchain and bitcoin fever is over," 2018.

[33] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.

[34] J. G. Coyne and P. L. McMickle, "Can blockchains serve an accounting purpose?" *Journal of emerging technologies in accounting*, vol. 14, no. 2, pp. 101–111, 2017.

[35] D. Drescher, *Blockchain basics*. Ascent Audio, 2020.

[36] M. Bennett, "Predictions 2018: The blockchain revolution will have to wait a little longer," *Forrester, Nov*, vol. 9, 2017.

[37] Y. Shifferaw and S. Lemma, "Limitations of proof of stake algorithm in blockchain: A review," *Zede Journal*, vol. 39, no. 1, pp. 81–95, 2021.

[38] N. O. Nawari and S. Ravindran, "Blockchain and the built environment: Potentials and limitations," *Journal of Building Engineering*, vol. 25, p. 100832, 2019.

[39] D. Mahmudnia, M. Arashpour, and R. Yang, "Blockchain in construction management: Applications, advantages and limitations," *Automation in construction*, vol. 140, p. 104379, 2022.

[40] N. E. Villanueva, "Blockchain technology application: Challenges, limitations and issues," *Journal of Computational Innovations and Engineering Applications*, vol. 5, no. 2, 2021.

[41] E. Daniel and F. Tschorsch, "Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 31–52, 2022.

[42] O. Wennergren, M. Vidhall, and J. Sörensen, "Transparency analysis of distributed file systems: With a focus on interplanetary file system," 2018.

[43] J. Shen, Y. Li, Y. Zhou, and X. Wang, "Understanding i/o performance of ipfs storage: a client's perspective," in *Proceedings of the international symposium on quality of service*, 2019, pp. 1–10.

[44] R. Norvill, B. B. F. Pontiveros, R. State, and A. Cullen, "Ipfs for reduction of chain size in ethereum," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1121–1128.

[45] H. Huang, S. Zhou, J. Lin, K. Zhang, and S. Guo, "Bridge the trustworthiness gap amongst multiple domains: a practical blockchain-based approach," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[46] J. S. Plank, "A tutorial on reed–solomon coding for fault-tolerance in raid-like systems," *Software: Practice and Experience*, vol. 27, no. 9, pp. 995–1012, 1997.

[47] R. Karim, M. A. I. Rizvi, and M. S. Arefin, "A survey on anomaly detection strategies," in *Second International Conference on Image Processing and Capsule Networks: ICIPCN 2021 2*. Springer, 2022, pp. 289–297.

[48] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "Smote: synthetic minority over-sampling technique," *Journal of artificial intelligence research*, vol. 16, pp. 321–357, 2002.

[49] S. Moualla, K. Khorzom, and A. Jafar, "Improving the performance of machine learning-based network intrusion detection systems on the unsw-nb15 dataset," *Computational Intelligence and Neuroscience*, vol. 2021, no. 1, p. 5557577, 2021.