International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 191-201
https://doi.org/10.70917/ijcisim-2026-5564
Article

Securing E-Prescribing Systems: Cybersecurity Risks And Solutions: Analyze The Cybersecurity Risks Associated With E-Prescribing Systems, Including Unauthorized Access, Data Breaches, And Prescription Fraud, And Explore Solutions To Address These Risks

Dr. Anjaiah Adepu[1], Dr. Dara Raj[2], Dr. Mohammed Yousuf Khan[3], Dr. N.Arjun[4], Dr. Aakunuri Manjula[5], Md Fasihuddin[6], Mujahid pasha Syed [7]

[1]Associate Professor, CSE, School of Engineering & Technology , Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: anjaniprasad.adepu@gmail.com
[2]Professor, Department of Computer Science and Engineering,Vignana Bharathi Institute of Technology, Aushapur,Ghatkesar, Hyderabad, Telangana, India.Email-id:rajurdara@gmail.com
[3]Associate Dean , School of Engineering & Technology & Principal ,Polytechnic ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: yusuf_lect@yahoo.com
[4]Associate Professor, Department of Computer Science and Engineering,Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad, Telangana, India.Email-id:arjun.nelikanti@vbithyd.ac.in.
5 Associate Professor, Department of Computer Science and Engineering,Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana, India.Email-id:manjula3030@gmail.com
[6]Assistant Professor, CSE School of Engineering & Technology ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: mdfasihuddin@manuu.edu.in
[7]Assistant Professor, CSE, School of Engineering & Technology ,Maulana Azad National Urdu University, Hyderabad, Telangana, India. Email-id: syedmuja@manuu.edu.in

Abstract: E-prescription systems are pivotal in modern healthcare, streamlining medication management and improving patient safety. However, their widespread use exposes them to cybersecurity risks like unauthorized access, data breaches, and prescription fraud. Breaches of sensitive health information and fraudulent prescriptions jeopardize both patient safety and public trust in healthcare systems. To mitigate these risks, it is crucial to implement a comprehensive cybersecurity strategy that incorporates strong authentication protocols, data encryption, regular system audits, and the integration of blockchain technology. These measures are essential to safeguard the integrity and security of e-prescription systems. This research examines the cybersecurity challenges and solutions in e-prescribing systems across eight representative countries: Canada, the USA, the UK, Australia, Spain, Japan, Sweden, and Denmark. It highlights the importance of these systems in enhancing pharmaceutical safety, protecting patient data, and mitigating health risks during global health crises.
Keywords: E-Prescription, Data breaches, Cyber Security, Digital Health, Blockchain technology, Digital Security.

1. INTRODUCTION

In recent years, the healthcare industry has undergone significant digital transformation, with electronic prescribing (e-prescribing) systems emerging as a critical innovation. These systems enable healthcare providers to

transmit prescriptions electronically to pharmacies, thereby reducing the risk of manual errors, enhancing medication accuracy, and improving patient safety[1]. E-prescribing systems offer several benefits, including faster prescription processing, better medication management, and improved access to patient medication histories[2]. As a result, they have become integral to modern healthcare delivery.

However, the digitization of prescription processes has also introduced significant cybersecurity vulnerabilities. E-prescribing systems store and transfer highly sensitive data, including personally identifiable information (PII) and protected health information (PHI), making them prime targets for cybercriminals[3]. The most pressing cybersecurity risks in e-prescribing systems include unauthorized access, data breaches, and prescription fraud[4]. Unauthorized access can lead to breaches of patient information, exposing individuals to identity theft and other forms of cyber exploitation[5]. Additionally, vulnerabilities within these systems may allow cybercriminals to forge or alter prescriptions to illegally acquire restricted medications, posing serious threats to public health and eroding trust in healthcare[6].

In the United States, several high-profile incidents illustrate the dangers of inadequate cybersecurity measures in healthcare systems, including e-prescribing. For instance, the 2015 attack on healthcare giant Anthem exposed the sensitive data of nearly 79 million patients and employees, highlighting the vulnerability of patient information across digital healthcare platforms[7]. Another notable incident occurred in 2019 when a ransomware attack on DCH Health System temporarily halted patient services, underscoring how system vulnerabilities can disrupt healthcare delivery[8]. Furthermore, recent studies have shown a rise in prescription fraud cases where cybercriminals exploited weak authentication systems in e-prescribing platforms to forge or alter prescriptions, leading to illicit drug acquisition and distribution[9].

These incidents emphasize the urgent need to address cybersecurity vulnerabilities in e-prescribing systems. With the rapid global adoption of these platforms, ensuring the confidentiality, integrity, and availability of prescription data has become a priority for healthcare providers and policymakers alike[10]. Implementing effective

cybersecurity measures is essential to protecting e-prescribing systems from unauthorized access, data breaches, and fraud, thereby safeguarding both patient safety and public trust in digital healthcare.

The study focuses at the cybersecurity issues connected with electronic prescription systems and offers solutions to such risks. Finding the best methods for system design, digital security, and authentication is the goal of this study, which compares and contrasts eight e-prescribing systems from the United States, Canada, the United Kingdom, Australia, Spain, Japan, Sweden, and Denmark.The study aims to develop a comprehensive strategy for enhancing the cybersecurity of e-prescribing systems worldwide, thereby protecting patient data and maintaining public trust in healthcare.

2. LITERATURE SURVEY

Safeguarding medical data (patient information) and effectively managing diverse supply chains, such as those for pharmaceuticals, organ donations, and medical equipment, are essential aspects of the healthcare sector in intelligent healthcare ecosystems.Blockchain technology is essential in addressing these challenges by offering enhanced security, privacy, reliability, and interoperability, which may significantly fortify the healthcare system [1]. By using an immutable and decentralized ledger, blockchain technology can securely store medical records, avoiding data breaches. Data is safeguarded and kept intact from manipulation by using cryptographic methods including digital signatures, asymmetric encryption, and hashing [2].

Furthermore, because to its decentralized architecture, every modification in a data transaction is instantly visible to all blockchain participants, hence enhancing the system's transparency. Given the potential risks in the healthcare sector, blockchain technology enables secure transfer of patient data, reduces disruptions, and ensures efficient management of medical resources. The authors established forward a smart healthcare system based on blockchain technology that prioritizes data privacy in [3]. In order to enhance decision-making in an open network, impose access limits, and validate data transfers, they developed a number of smart contracts.To augment user privacy,

differential privacy techniques were used. The study results demonstrate that the proposed system exceeds prior options in reliability, stability, and traceability [4].Several access control mechanisms for healthcare data have been proposed by various researchers. Li et al. introduced a Multi-Authority Attribute-Based Encryption (MAABE) system [5], where Attribute Authorities can operate independently, addressing the risk of collusion attacks. Their approach employs a special encryption scheme for obfuscation. Narayan et al. proposed a Privacy-Aware Access Control model using Public Searchable Encryption and Symmetric Key Encryption (SKE) [6]. While this model works effectively for electronic health record (EHR) searchability, it lacks flexibility and refined access control. Prince et al. introduced a Privacy Rating-based access control approach [7].

3. PROBLEM STATEMENT

Prior research on e-prescribing system security highlights several pressing cybersecurity issues that have serious implications for patient safety and the integrity of healthcare delivery. The transition from paper to digital prescriptions, while improving efficiency and reducing human error, has also introduced risks such as unauthorized access, data breaches, and prescription fraud. A major issue identified is the vulnerability of e-prescribing systems to hacking, often due to weak or inadequate authentication mechanisms. This flaw enables unauthorized individuals to gain access to sensitive patient information, threatening patient privacy and overall data integrity.

Data breaches are frequently observed risks that expose confidential patient information, including personal identification and medical histories, to cybercriminals. Such breaches can result in identity theft and financial exploitation, highlighting the urgent need for more robust security measures in data handling. Prescription fraud, facilitated by weak security protocols, is another critical issue. Malicious actors can manipulate or falsify digital prescriptions to illegally obtain medications, contributing to the misuse of controlled substances and jeopardizing public health. Moreover, research shows that inconsistent security standards across healthcare systems and countries lead to disparities in protection levels, leaving many e-prescribing systems vulnerable to cyberattacks. These challenges underscore the urgent need for robust, standardized security protocols that can mitigate persistent cybersecurity threats and protect the e-prescribing process globally.

4. PROPOSED MODEL

A blockchain-based model is proposed to address the cybersecurity challenges in e-prescribing systems. This model leverages blockchain's decentralized and immutable structure to enhance data security and integrity. Within this framework, blockchain operates as a distributed ledger where each prescription transaction is recorded as a unique block, cryptographically linked to prior blocks. This structure ensures that any attempt to alter a prescription will be immediately detected, as the altered block will no longer align with previous blocks. By decentralizing data storage across multiple nodes, the risk of unauthorized tampering is significantly reduced, fostering trust in the authenticity of prescriptions among doctors and users. Blockchain also facilitates data transparency and traceability, allowing authorized users to access prescription histories while safeguarding patient privacy through encryption. Access to sensitive data is restricted to verified entities, ensuring patient confidentiality throughout the entire process.

Additionally, smart contracts are integrated into this blockchain-based model to automate and secure the prescription process. Smart contracts, which are self-executing programs that enforce predefined conditions, play a vital role in validating prescriptions and ensuring compliance. When a doctor issues a prescription, the smart contract verifies the prescriber’s credentials, checks the prescription for accuracy, and confirms compliance with relevant regulations before it reaches the user. This automation reduces the need for manual validation, thereby minimizing errors and opportunities for fraud. For prescriptions involving controlled substances, smart contracts can require authentication from the user, adding an additional layer of security. Each step in the process from prescription issuance to fulfillment is securely logged on the blockchain, providing full traceability and minimizing the risk of fraudulent activities. This blockchain-based approach not only strengthens security but also increases efficiency, reducing delays in the prescription process and ensuring reliable, secure e-prescribing systems.

DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized ledger system whereby each block encompasses a transaction record and a hash key linking it to the previous block, so creating a perpetually updated and replicated chain across all nodes in the network. This setup forms an interconnected series of blocks, referred to as a "blockchain" [3]. Any alteration of data inside a block leads to an immediate change in the hash key, enabling the detection of tampering. The first block in this series is designated as the Genesis Block. The "blockchain cloud" is seen as a more efficient substitute for traditional cloud computing infrastructure. Blockchain, first conceptualized in 2008, was primarily used as a payment mechanism for the Bitcoin cryptocurrency. It allows untrusted parties to collaboratively create a permanent, transparent, and immutable record of transactions without the need for a central authority.

Although hashing alone is not enough to fully prevent tampering (since recalculating hashes for multiple blocks can be done in just a few seconds), the integration of Proof of Work (PoW) significantly strengthens security. PoW is a mechanism that delays the creation of new blocks, making it much harder to modify them. Altering a block would require recomputing PoW for all subsequent blocks, which greatly increases the difficulty of tampering with the blockchain.

Blockchain security relies on the combined use of hashing, PoW, and its peer-to-peer (P2P) nature, which requires consensus from over 50% of peers to validate any changes. The continuous evolution of blockchain, including the development of smart contracts, represents one of the most recent advancements in this technology.

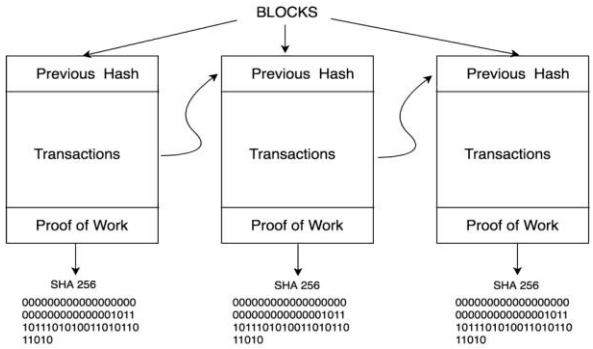


Figure.1 Block chain Model

This figure.1 illustrates the blockchain structure, where each block links to the previous one using a Previous Hash, creating a continuous chain. Each block contains Transactions that record data, and Proof of Work, a computational puzzle that miners solve to add the block securely. A unique SHA-256 Hash identifies each block, generated based on its contents. If any data in a block changes, its hash changes, breaking the chain's continuity. This linkage ensures data integrity across the blockchain, as altering one block affects all subsequent blocks. Together, these features make blockchain a secure, tamper-resistant system, ideal for maintaining an unchangeable record of transactions.

BLOCKCHAIN TYPES

Blockchain ledgers are broadly divided into two main categories: Public or Decentralized Ledgers and Private or Centralized Ledgers. Additionally, based on access permissions, blockchain systems can be classified into Permissioned and Permissionless types.

1. Public or Decentralized Blockchain

Public blockchains are open and decentralized, often using Proof of Work (PoW) consensus processes. They are permissionless, allowing anybody to observe, create, and send transactions. In these systems, the buyer creates a transaction or block, which is then verified and distributed by cryptographic hashing. Upon verification, the transaction is inscribed on the blockchain, and miners get remuneration for their efforts.. Trustless peer-to-peer interactions enable the seller to receive the transaction securely. Public blockchains commonly use consensus mechanisms like PoW and Proof of Stake (PoS) for security. Examples include Bitcoin, Ethereum, Monero, Dash, Litecoin, and Dogecoin.

2. Private or Centralized Blockchain

Private blockchains centralize writing rights within a single entity, while reading permissions can be either public or restricted. They leverage blockchain technology to minimize redundancy and lower transaction costs through internal transaction verification. Participants in private blockchains are preauthorized with verified identities. However, this type of blockchain has become less prevalent in recent times.

3. Permissioned Blockchain

Permissioned blockchains can be either public or private. For instance, Bitcoin operates as a public-permissioned blockchain, whereby any node inside the network participates in the consensus process. In a public-permissioned blockchain, those who meet certain criteria may download the protocol and verify transactions, often using Proof of Work (PoW).In contrast, private-permissioned blockchains restrict transaction validation to members of a specific consortium, using mechanisms such as Practical Byzantine Fault Tolerance (PBFT) or multi-signature protocols.

4. Permissionless Blockchain

Permissionless blockchains are publicly owned, accessible, and transparent in design. In systems using Proof of Work or related protocols, any person may download the protocol and verify transactions.

5. SYSTEM MODEL

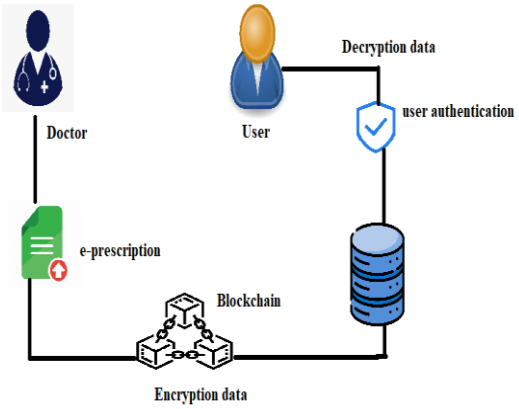


Figure.2 System Model

The figure.2 shows a secure, blockchain-based e-prescription system. A doctor writes an electronic prescription, which is then documented on the blockchain to ensure data integrity and authenticity. Information is safeguarded on the blockchain, protecting critical data. The patient is required to complete an authentication process to access the prescription information. Following authentication, the system decrypts the data, allowing the user secure access to their prescription.

6. IMPLEMENTATION FLOW FOR SECURE E-PRESCRIBING SYSTEM

1. **System Initialization and Key Management**

The first step in implementing the secure e-prescribing system is to initialize cryptographic keys and set up secure storage for them. AES-256 encryption is used to secure prescription and patient data, with a strong, unique key generated at the start. This key is stored securely in an encrypted vault, ensuring it remains accessible only to authorized entities. Additionally, a secure, unique timestamp is generated with each encryption session to enhance data security by adding randomness to each transaction.

2. **Doctor Module Security: Hashing and Data Encryption**

The doctor module's primary focus is on securing access to sensitive prescription data and ensuring that only authorized personnel can issue prescriptions. SHA-256 hashing with a unique salt is applied to passwords before they are stored in the database. This makes it extremely challenging for potential attackers to reverse-engineer or deduce the original password, as each hashed password is unique, even for identical entries. To further protect sensitive information, such as prescription details, AES-256 encryption is used before storage or transmission. AES encryption in Cipher Block Chaining (CBC) mode, combined with the timestamp, provides a high level of data security, as any intercepted data remains unreadable without the correct decryption key.

3. **User Module Security: Data Encryption and Session Management**

User registration and logging for all access events are implemented in this module. The user module handles patient data, which includes personally identifiable information. Before any sensitive data is saved to the database or transmitted, AES-256 encryption is applied. By keeping patient data encrypted throughout its lifecycle, unauthorized access is minimized. For secure session management, the system generates a session token using SHA-256 hashing. A unique, random session token is created each time a user logs in, ensuring secure and consistent session tracking. Since this hashed token is irreversible, it provides strong protection against session hijacking and impersonation, as only valid session tokens are accepted for authenticated activities. Regular monitoring of these logs helps identify and respond to potential threats in real time, adding a proactive layer of cybersecurity to the e-prescribing system. Users can also download e-prescribing documents as needed.

4. **Data Access and Decryption Workflow**

When a user needs to access encrypted data, the system retrieves the relevant AES key and timestamp from secure storage. With this key and timestamp, the data is decrypted back into its original form, making it accessible to the authorized individual. This decryption only occurs at the moment of access, and sensitive data is kept encrypted at rest, ensuring its security during storage. By applying decryption on demand, the system minimizes the risk of unauthorized access, even if the database is breached, as any data accessed without the correct key will be unreadable.

5. **Routine Key Rotation and Security Updates**

To maintain long-term security, the system undergoes regular key rotation and software updates. Key rotation helps prevent security weaknesses from prolonged key usage, while updates ensure that all cryptographic algorithms and security protocols remain up to date with the latest standards. Additionally, all modules undergo regular security assessments and patches to keep the system resilient against evolving cybersecurity threats.

All these modules are integrated to secure the e-prescribing system, ensuring the confidentiality, integrity, and availability of sensitive healthcare data while meeting regulatory compliance.

This algorithm implements a blockchain-based e-prescribing system using SHA-256 for secure transaction records. It features a class structure to manage blocks, transactions, and the mining process, ensuring data integrity and confidentiality through encryption.

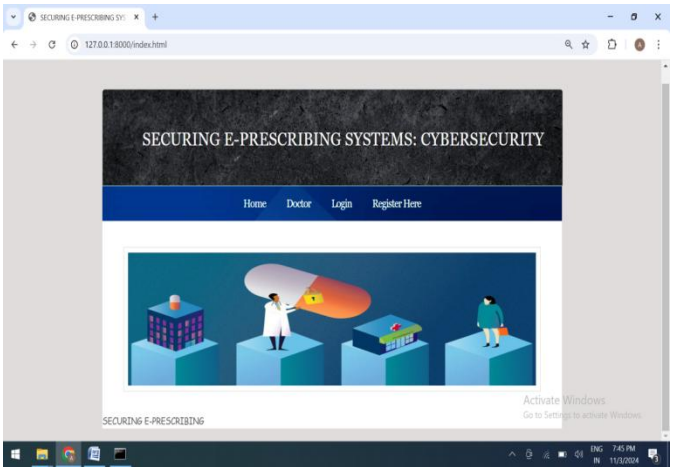
Algorithm: SHA-256 in E-PrescribingRecord

class Block:
  def __init__(self, idx, txs, timestamp, prev_hash):
self.index, self.transactions, self.timestamp, self.previous_hash, self.nonce = idx, txs, timestamp, prev_hash, 0
 	
  def calculate_hash(self):
  return sha256(json.dumps(self.__dict__, sort_keys=True).encode()).hexdigest()

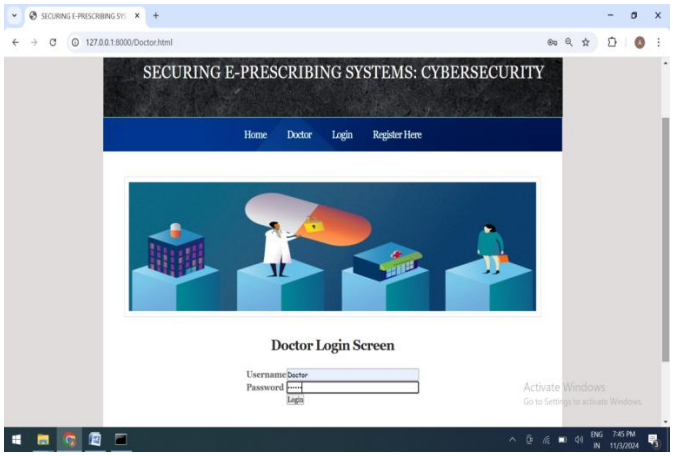
```
class Blockchain:
    def __init__(self):
self.chain, self.pending_transactions = [], []
self.initialize_genesis_block()

    def initialize_genesis_block(self):
genesis_block = Block(0, [], time.time(), "0")
self.chain.append(genesis_block)

    def add_transaction(self, transaction):
self.pending_transactions.append(transaction)

    def mine_block(self):
new_block = Block(len(self.chain), self.pending_transactions, time.time(), self.chain[-1].calculate_hash())
        while new_block.calculate_hash()[:2] != "00":
new_block.nonce += 1
self.chain.append(new_block)
self.pending_transactions = []

    def encrypt_transaction(self, transaction):
        return blockchain.encrypt(json.dumps(transaction).encode())

    def decrypt_transaction(self, encrypted):
        return blockchain.decrypt(encrypted)

#blockchain encrypted transaction
blockchain = Blockchain()
transaction = {"name": "dhinakaranrajendran", "receiver": "Patient", "record": "patientreport"}
encrypted_transaction = blockchain.encrypt_transaction(transaction)
blockchain.add_transaction(encrypted_transaction)
blockchain.mine_block()
```

7. RESULTS

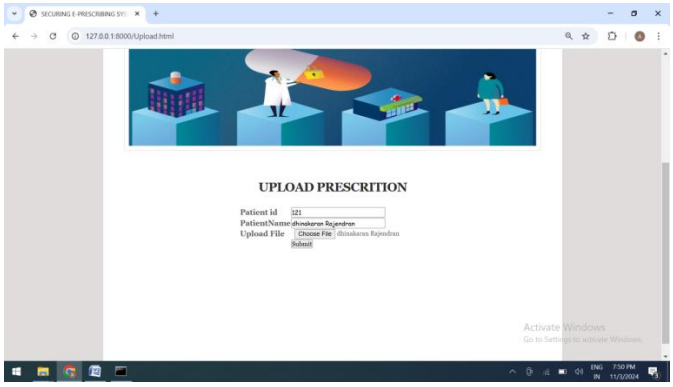
This project focuses on developing an application that facilitates e-prescribing using blockchain technology. By integrating secure and transparent transaction methods, it enhances the efficiency and reliability of the prescribing process. The following sections outline the application flow and all its functionalities.



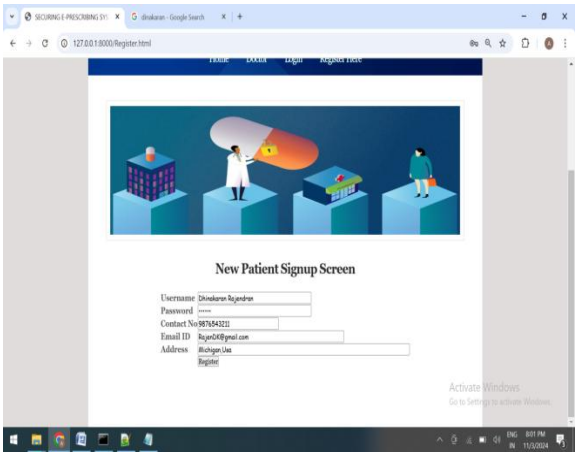
The home screen of the application includes two modules: Doctor and User.



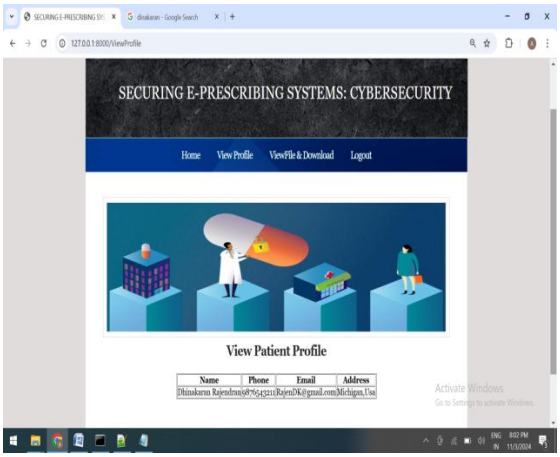
The doctor login page consists of fields for entering a username and password.



The doctor will upload the user's e-prescription along with details, which will be stored in the blockchain with encryption in the database.



The user signup page is where the user will register.



The user module includes options to view their profile and to view and download e-prescription files.

8. CONCLUSION

The integration of e-prescribing systems into modern healthcare has the potential to significantly improve patient safety, enhance medication management, and streamline prescription processes. However, as reliance on digital solutions grows, so do the associated cybersecurity risks. Unauthorized access, data breaches, and prescription fraud pose serious threats that can undermine patient trust and safety, underscoring the necessity of robust security measures.

The propose blockchain-based framework offers a thorough resolution to these issues by using the decentralized and irreversible properties of blockchain technology. This system ensures the integrity and authenticity of prescription data using a distributed ledger, while providing transparency and traceability for all transactions. The integration of smart contracts further automates prescription validation, reducing potential errors and minimizing opportunities for fraud. Moreover, implementing robust encryption techniques ensures that sensitive patient data remains confidential, even if intercepted. With authenticated users and strict validation protocols, this model addresses critical security vulnerabilities, safeguarding patient information and enhancing the reliability of e-prescribing systems.

While e-prescribing systems deliver significant benefits for doctors and patients, they also introduce cybersecurity challenges that must be addressed to maintain trust in digital health solutions. Unauthorized access, data breaches, and prescription fraud remain key risks that require a comprehensive cybersecurity approach. By implementing robust authentication methods, encryption and blockchain technology, Data provided by doctors can reinforce the security of e-prescribing systems and effectively protect sensitive patient information.

9. FUTURE ENHANCEMENTS

Future research could explore the integration of artificial intelligence (AI) in detecting and mitigating cybersecurity threats in real time. AI could analyze patterns of malicious activity and provide predictive insights to prevent breaches before they occur, enhancing proactive security. Additionally, the global standardization of e-prescribing security protocols could further strengthen the security of digital healthcare infrastructure, ensuring consistency across borders. Exploring biometric authentication and decentralized identity solutions may also enhance patient data privacy and add robust layers of security to e-prescribing systems. These advancements would provide a comprehensive approach to safeguarding digital healthcare and maintaining public trust.

REFERENCES

1. Gupta, R.; Reebadiya, D.; Tanwar, S.; Kumar, N.; Guizani, M. When Blockchain Meets Edge Intelligence: Trusted and Security Solutions for Consumers. IEEE Netw. 2021, 35.
2. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When Blockchain Meets Smart Grid: Secure Energy Trading in Demand Response Management. IEEE Netw. 2020, 34, 299–305.
3. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. IEEE J. Biomed. Health Inform. 2022, 26, 1917–1927.
4. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. A Taxonomy of Blockchain-enabled Softwarization for Secure UAV Network. Comput. Commun. 2020, 161, 304–323.
5. Li, J., Hu, S., Zhang, Y. et al. A decentralized multi-authority ciphertext-policy attribute-based encryption with mediated obfuscation. Soft Computing 24, 1869–1882 (2020). https://doi.org/10.1007/s00500-019- 04018-y
6. Narayan, S., Gagne´, M., Safavi-Naini, R.: Privacy preserving EHR system using attribute-based infrastructure. In: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop. ACM (2010)
7. Prince, P.B., Lovesum, S.P.J. Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System. SN COMPUT. SCI. 1, 239 (2020). https://doi.org/10.1007/s42979- 020-00246-4
8. X. Liu, X. Yang, Y. Luo, L. Wang, and Q. Zhang, "Anonymous Electronic Health Record Sharing Scheme Based on Decentralized Hierarchical Attribute-Based Encryption in Cloud Environment," IEEE Access, vol. 8, pp. 200180-200193, 2020.
9. Prince, P.B., Lovesum, S.P.J. "Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System." SN COMPUT. SCI., 1, 239 (2020).
10. Li, J., Hu, S., Zhang, Y. et al. "A decentralized multi-authority ciphertext-policy attribute-based encryption with mediated obfuscation." Soft Computing, 24, 1869–1882 (2020).
11. Ullah I, Amin N, Almogren A, Khan MA, Uddin MI, Hua Q. "A lightweight and secured certificate-based proxy signcryption (CB-PS) scheme for e-prescription systems." IEEE Access., 2020; 8: 199197-212.
12. S. Kanaga, Suba Raja, A. Sathya, and L. Priya, "A HYBRID DATA ACCESS CONTROL USING AES AND RSA FOR ENSURING PRIVACY IN ELECTRONIC HEALTHCARE RECORDS," 2nd International Conference on Power Energy Control and Transmission Systems, 2020.
13. I. Ullah, N. U. Amin, M. Zareei, A. Zeb, H. Khattak, A. Khan, and S. Goudarzi, "A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications," Symmetry, vol. 11, no. 11, p. 1386, Nov. 2019.
14. M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," J. Inf. Secur. Appl., vol. 45, pp. 156–175, Apr. 2019.
15. Wassim Alexan, Ahmed Hamza, and Hana Medhat, "An AES Double-Layer Based Message Security Scheme," 2019 International Conference on Innovative Trends in Computer Engineering (ITCE'2019), pp. 2-4, February 2019.
16. L. Li, S. Zhou, K.-K.-R. Choo, X. Li, and D. He, "An efficient and provably-secure certificateless proxy-signcryption scheme for electronic prescription system," Secur. Commun. Netw., vol. 2018, pp. 1–11, Aug. 2018.
17. D. S. Gupta and G. P. Biswas, "Design of lattice-based ElGamal encryption and signature schemes using SIS problem," Transactions on Emerging Telecommunications Technologies, vol. 29, no. 6, pp. e3255, 2018.
18. Khushbu Jakhotia, Rohini Bhosale, and Chelpa Lingam, "Novel Architecture for Enabling Proof of Retrievability using AES Algorithm," IEEE International Conference on Computing Methodologies and Communication (ICCMC), 2017.
19. K.M Akhil, M Praveen Kumar, and B.R Pushpa, "Enhanced Cloud Data Security Using AES Algorithm," International Conference on Intelligent Computing and Control (I2C2), 2017.
20. Taufik Hidayat, Franky D Sianturi Tigor, and Rahutomo Mahardiko, "Forecast Analysis of Research Chance on AES Algorithm to Encrypt during Data Transmission on Cloud Computing," IEEE Transactions on Cloud Computing, May 2015.
21. Arshdeep, B., Madisetti, V.K. "A cloud-based approach for interoperable electronic health records (EHRs)." IEEE J. Biomed. Health Inform., 17(5), 894–906, 2013.
22. Hossein Rahmani,ElankovanSundararajan,Zulkarnain Md. Ali,Abdullah Mohd Zin,"Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud," The 4th International Conference on Electrical Engineering and Informatics (ICEEI), 2013.

23. A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," Annual Cryptology Conference, 2011, pp. 578-595.
24. Lapane KL, Waring ME, Dubé C, Schneider KL. "E-prescribing and patient safety: Results from a mixed-method study." Am J Pharm Benefits., 2011; 3(2): e24-34. PMID: 24179595.
25. Narayan, S., Gagne, M., Safavi-Naini, R. "Privacy preserving EHR system using attribute-based infrastructure." In: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, 2010.
26. B. Smith, A. Austin, M. Brown, J. King, J. Lankford, A. Meneely, et al., "Challenges for Protecting the Privacy of Health Information: Required Certification Can Leave Common Vulnerabilities Undetected", Proceedings of the second annual workshop on Security and privacy in medical and home-care systems, pp. 1-12, October 08, 2010.
27. H.-Y. Lin, T.-S. Wu, S.-K. Huang, and Y.-S. Yeh, "Efficient proxy signcryption scheme with provable CCA and CMA security," Comput. Math. Appl., vol. 60, no. 7, pp. 1850–1858, Oct. 2010, DOI: 10.1016/j.camwa.2010.07.015.
28. H. Elkamchouchi, M. Nasr, and R. Ismail, "A new efficient strong proxy signcryption scheme based on a combination of hard problems," in Proc. IEEE Int. Conf. Syst., Man Cybern., Oct. 2009, pp. 5123–5127, DOI: 10.1109/icsmc.2009.5346018.
29. Peleg, M., et al. "Situation-based access control: privacy management via modelling of patient data access scenarios." J. Biomed. Inform., 41(6), 1028–1040, 2008.
30. H. Elkamshouchy, A. K. AbouAlsoud, and M. Madkour, "New proxy signcryption scheme with DSA verifier," in Proc. 23rd Nat. Radio Sci. Conf. (NRSC), 2006, pp. 1–8, DOI: 10.1109/nrsc.2006.386345.
31. Yang Y, Han X, Bao F, Deng RH. "A smart-card-enabled privacy-preserving e-prescription system." IEEE Trans Inf Technol Biomed., 2004; 8(1): 47-58. DOI: 10.1109/titb.2004.824731.
32. Z. Zhang, Q. Dong, and M. Cai, "A new publicly verifiable proxy signcryption scheme," in Progress on Cryptography, 2004, pp. 53–57, DOI: 10.1007/1-4020-7987-7_7.
33. Bourka A, Kaliontzoglou A, Polemi D, Georgoulas A, Sklavos P. "Enriching healthcare applications with cryptographic mechanisms and XML-based security services." Technol Health Care., 2003; 11(1): 61-76. PMID: 12590159.
34. Blobel B, Bleumer G, Muller A, Flikkenschild E, Ottes F. "Current security issues faced by health care establishments." In: The ISHTAR Consortium (ed). Studies in Health Technology and Informatics., Vol 66. IOS Press, 2001.
35. C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," in Proc. 22nd Australas. Comput. Sci. Conf., 1999, pp. 420–431.
36. Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," in Proc. Annu. Int. Cryptol. Conf., Springer, 1997, pp. 165–179.