Blockchain for Securing Health Records in Metaverse

Divya Jacob[1], Yan Bai[1(✉)], and Juan Li[2]

[1] School of Engineering and Technology, University of Washington Tacoma, Tacoma, WA, USA
{divjacob,yanb}@uw.edu
[2] Department of Computer Science, North Dakota State University, Fargo, ND, USA
j.li@ndsu.edu

Abstract Metaverse is an emerging technology which uses virtual reality, augmented reality, and other technologies to allow people to interact with each other as well as do business and engage in leisure activities. People can connect with one another and with digital content in real time in a world without physical borders. Before widespread adoption can occur, it is important to thoroughly assess the security and privacy threats connected to the underlying technology as well as the new digital environment. The security of healthcare records is a major concern in the metaverse. In order to ensure the safety of patient records, blockchain technology is being used to protect user data against malicious activities and other types of attacks. The objective is to strengthen security in the Metaverse and foster trust in the platforms and apps that make up this new digital environment.

Keywords: Metaverse · Security · Blockchain · Cloud computing

1 Introduction

The phrase "metaverse" refers to an emerging eld where avatars are employed for online social interaction, business transactions, and recreational pursuits. It is a world without borders where individuals can communicate in real time with each other and with digital content. With the advancement of virtual reality and augmented reality technologies, there has been a signi cant rise in interest in the concept of the metaverse in recent years. A variety of industries including healthcare are expected to bene t from this fast-developing technology. Metaverse can have a variety of applications in healthcare like telemedicine and telehealth where patients can have access to doctors and other healthcare services remotely, tness and mental wellness apps, medical education, and training for healthcare practitioners. In this project the plan is to focus on one aspect of the metaverse called digital twins. In the metaverse, a digital twin is a digital representation of a real-world object. In the context of healthcare, a digital twin will consist of data collected from various data sources like electronic health records from hospitals, biometrics data from sensors like heart rate and other symptoms collected from patients. By using digital twins' people can keep track and be aware of their health conditions which can help to nd potential issues on time and take the required measures.

K. Arai (Ed.): FICC 2024, LNNS 920, pp. 208–219, 2024.
https://doi.org/10.1007/978-3-031-53963-3_15

One of the signi cant challenges in widespread adoption of metaverse in healthcare is security and privacy concerns. Massive volumes of data, including biometrics data, about their employees, processes, and patients, must be gathered, stored, and used in order to integrate the metaverse with healthcare systems. There can be security issues like unauthorized access or tampering with data and there must be measures in order to protect the integrity of the stored data.

A viable strategy for improving security of healthcare records in the Metaverse is blockchain technology. Blockchain provides a tamper-proof and transparent mechanism for storing and exchanging data because of its decentralized and secure nature. There are two kinds of blockchain - public and private. Public blockchain are decentralized and open to everyone whereas private blockchain allow only authorized individuals control over the data. By its authentication, access control, and consensus methods, private blockchain technology secures data privacy in the metaverse by giving people ultimate control over their data. With private blockchain technology, patients also have more choice over who gets access to their health information, and healthcare practitioners can make sure that all applicable laws are followed. Blockchain technology is a powerful tool for ensuring the integrity of sensitive data since it can ensure the authenticity and immutability of health information. Data in the metaverse is securely protected using asymmetric-key encryption and hashing techniques used in the blockchain architecture [5]. A majority of nodes in the distributed ledger must accept any modi cations to the data, which makes data acquisition resistant to attacks. The distributed ledger in blockchain enables transaction record validation and data tracing in the metaverse. Every action on the blockchain is recorded as a transaction and saved in a block that includes a cryptographic hash of the preceding block, a date, and metadata to make the data unchangeable. Additionally, because each block is authorized and duplicates are nearly impossible to produce, blockchain technology ensures the dependability of data obtained through the metaverse's acquisition methods. Patients, healthcare professionals, and insurance companies may work together and share information more effectively using this secure and transparent system.

In order for a digital twin to be useful in healthcare, the data should be accurate and handle frequent data upload so as to ensure real time synchronization between the real entity and its digital twin [4]. For this reason, we need an enterprise-grade blockchain, transactions are executed more quickly and ef ciently, and the need for intermediaries is eliminated in many operations and data accuracy is maintained across all nodes. Hyperledger fabric, which is a private and permissioned network, is used to implement the blockchain which ensures that access to data is restricted to authorized members. Using this private blockchain on a cloud computing technology such as AWS will help to boost security. The following adversarial models have the potential to affect the security of medical records: Insider threats: Attacks carried out by those with permission to access health care records are referred to as insider threats. Employees of the healthcare provider who misuse their access rights to steal or misuse patient information may fall under this category. External attacks: These are carried out by individuals or groups who are not authorized to access the health care records. To access the records, these attackers could use social engineering methods like phishing, hacking, or other social engineering techniques. Ransomware attacks: Ransomware attacks involve encrypting the health care

records and demanding payment for the decryption key. Such attacks have the potential to disrupt patient treatment and jeopardize the con dentiality and availability of records. Denial of service attacks: These attacks involve flooding the servers of the healthcare provider with traf c to disrupt the availability of the health care records. In this paper, we design a system that is able to defend against all these four kinds of attacks.

The rest of the paper is organized as follows: Sect. 2 summarizes important related work. Sections 3, 4, and 5 present the implementation, detailed algorithms, and results, respectively. Finally, we point out directions for future work in Sect. 6 and conclude the paper in Sect. 7.

2 Related Work

The potential of metaverse technology to deliver a healthcare service experience that is interactive, immersive, and recreationally tailored to meet individual patients' needs is highlighted by a comprehensive review of the applications, challenges, and future directions of metaverse technology in healthcare [1, 7]. The authors look at the major enabling technologies for healthcare, such as sensors, big data, AI, wireless communication networks, IoT, edge computing, and immersive technology. They also investigate the enabling technologies of the Metaverse for healthcare. The paper also discusses the dif culties in implementing metaverse technology in healthcare, such as data privacy, security, and interoperability problems. The dif culties in safeguarding the metaverse are explored by Yuntao et al. [2] along with a number of security and privacy risks that may exist there. The authors speci cally look into seven major facets of the metaverse, including governance, network, economy, data management, privacy, and physical and social effects. In each of these areas, they highlight pressing issues and talk about potential remedies. The authors also review current security and privacy safeguards being used in academic and professional contexts and assess their usefulness in developing a secure and privacy-preserving metaverse paradigm. The paper also looks at the role blockchain technology plays in bridging the gap between the traditional economy and the metaverse economy. The use of blockchain technology to address concerns with security, privacy, con dentiality, and decentralization in electronic health data is explored in a paper by Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid [3]. The paper suggests a framework that makes use of blockchain technology for EHR and permits secure storage of digital records by using ne-grained access constraints for users. For the framework's implementation, Ethereum, a blockchain network, was employed. The authors also go into the consensus process that controls how each block is added to the chain. A scalable, safe, and comprehensive blockchain-based solution for EHR is made possible by the proposed framework's usage of off-chain record storage, which also tackles the scalability issue with blockchain technology. The security and privacy issues associated with the development of metaverse are discussed by Chen, Zefeng et al. [6]. The paper also contains the advantages and application scenario of metaverse. The authors also talk about the metaverse related technologies, and some security and privacy solutions derived from these technologies. The paper goes into great length on the various layers that make up the virtual world of the metaverse's security and privacy, as well as discuss the eight signi cant threats including identity theft, ethics, compliance, and so forth. They also

go through how blockchain, which is a decentralized ledger, uses point-to-point transmission, consensus mechanisms, and encryption algorithms to give users secure and dependable data transmission and storage. The paper also talks about the open problems and opportunities in the metaverse.

To the best of our knowledge, most current work addresses challenges in the eld of securing health records in Metaverse through a high-level theoretical analysis. Few research works have carried out experimental studies to demonstrate the effectiveness and practicality of proposed approaches. We developed a system to securely store healthcare records by making use of the hyperledger fabric blockchain in AWS, and showing its effectiveness in terms of security and network performance.

3 Implementation

Hyperledger fabric supports a permissioned model where the identities of all users participating in the network are veri ed. The orderer, peer, and MSP are the three main components of Hyperledger fabric.

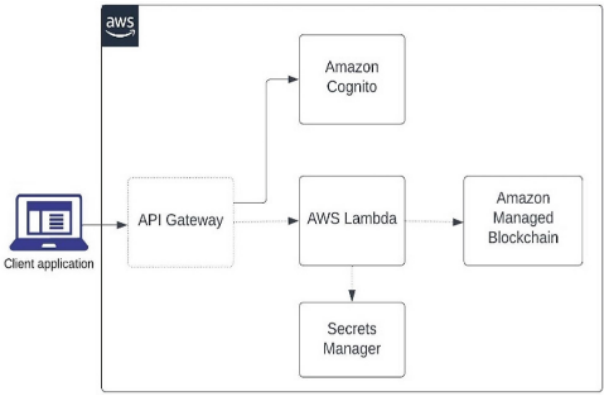

Fig 1 Hyperledger fabric framework in AWS

Orderer is a component that is responsible for making sure that transactions are sent to the relevant peer nodes for validation and endorsement.
Peer nodes are in charge of executing smart contracts, maintaining the ledger, and taking part in the consensus process.
Membership Service Provider (MSP) is a component that establishes the guidelines for identity management and authentication within a Hyperledger Fabric network. MSPs are used to con rm the legitimacy of network participants, including users, applications, and peer nodes.

We used Amazon Managed Blockchain service to create a private distributed ledger. Hyperledger Fabric is one of the blockchain frameworks that AMB supports. Digital certi cates are used by AMB to identify users and applications. AMB issues and manages

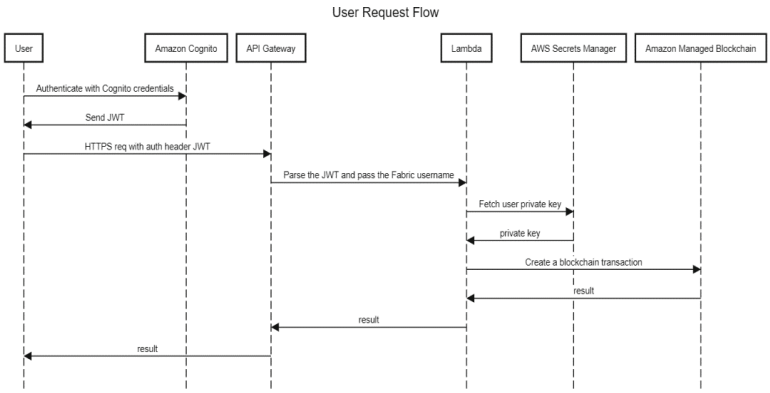

Fig 2 User request flow

these certi cates through the usage of Certi cate Authorities (CA). Built using Amazon QLDB technology, Managed Blockchain's ordering service offers an immutable change log that ensures that you durably save the data by maintaining the full history of every transaction in the blockchain network. AMB by default used the RAFT consensus algorithm which is simpler and consumes less resource than other algorithms. Figure 2 shows the user request flow.

Amazon Cognito is used for authentication. AWS Secrets Manager stores the enrollment credentials for the blockchain user who is registered (created) in the Certi cate Authority. Within the Cognito User Pool a corresponding user will be created with a custom attribute, fabricUsername, that helps to identify this user within the Certi cate Authority. The client application attempts to authenticate the user (via username and password) against a Cognito User Pool. Cognito returns a JSON Web Token (JWT) after successful authentication. This JWT is included by the client application in requests made to the API Gateway, which authorizes the user to invoke the API route. The fabricUsername custom attribute is retrieved by API Gateway from the JWT and sent to the Lambda function that will carry out the blockchain transaction. Lambda obtains the connection pro le which is required for connecting to the Amazon Managed Blockchain network from Amazon Systems Manager (Parameter Store) and the private key for the blockchain user from AWS Secrets Manager. In the Fabric chaincode, methods are added that use attribute-based access to restrict who can invoke the method.

4 Schema and Algorithm

The patient and doctor details are stored based on the following schema. Doctors who have granted access to the patients can be seen in the DoctorAcessList of the patient record. The electronic health record data is stored in the EHRList.

EHR {
DoctorId string
Symptoms string
Diagnosis string
Treatment string }

PatientDetails {
PatientId string
FirstName string
LastName string
Email string
DoctorAccessList []string
PhoneNumber int64
EHRList []EHR }

DoctorDetails {
DoctorId string
FirstName string
LastName string
Email string
PhoneNumber int64
Department string
}

Algorithm

Smart Contract for Admin
Function Create Patient (*contains variables to add data*)
if (msg.sender.role == admin) **then**
#check if patient already exists
record = get patient record from blockchain(id)
if not record exists
create new patient record in blockchain
endif
else Abort session
endif
end Function

Function Create Doctor (*contains variables to add data*)
if (msg.sender.role == admin) **then**
#check if doctor already exists
record = get doctor record from blockchain(id)
if not record exists
create new doctor record in blockchain
endif
else Abort session

```
    endif
end Function

Smart Contract for Patients
Function Get Patient Record(patient id)
    if ( msg.sender.id == patient id) then
        record = get patient record from blockchain(id)
        return record
        else Abort session
    endif
end Function

Function Get All Doctors
    record = get all records from blockchain
    for record in records
        if record.id starts with 'DOC'
            add record to final records
    return final records
end Function

Function Grant Access(patient id, doctor id)
    if ( msg.sender.id == patient id) then
        retrieve patient record
        add doctor id to doctor access list of patient record
        save record to blockchain
    else Abort session
    endif
end Function

Function Revoke Access(patient id, doctor id)
    if ( msg.sender.id == patient id) then
        retrieve patient record
        remove doctor id from doctor access list of patient record
        save record to blockchain
    else Abort session
    endif
end Function

Function Update Patient Record():
    if ( msg.sender.id == patient id) then
        record = get patient record from blockchain(id)
        update fields in record
        save record to blockchain
    else Abort session
    endif
end Function
```

```
Smart Contract for Doctors
Function Get Patients (doctor id)
   record = get all records from blockchain
   for record in records
      if record.id starts with 'PAT' and record.doctorAccessList contains doctor id
            add record to final records
   return final records
end Function

Function Get Patient EHR (patient id)
   if ( msg.sender.role == doctor) then
      record = get patient record from blockchain(patient id)
      # check if doctor has access to patient record
      if record.doctor_access_list.contains(msg.sender.id)
         return record.ehrList
      else Abort session
      endif.
   else Abort session
   endif
end Function

function Add Patient EHR (patient id)
   if ( msg.sender.role == doctor) then
      record = get patient record from blockchain(patient id)
      # check if doctor has access to patient record
      if record.doctor_access_list.contains(msg.sender.id)
         add ehr record to patient's record.
      else Abort session
      endif
   else Abort session
   endif
end Function

Function Get Doctor Record(doctor id)
   if ( msg.sender.id == doctor) then
      record = get patient record from blockchain(id)
      return record
   else Abort session
   endif
end Function
```

5 Experiments and Results

A system shown in Fig. 1 was deployed in AWS and the admin, patient, and doctor chaincodes described in the algorithm section above were installed in the AMB peer nodes.

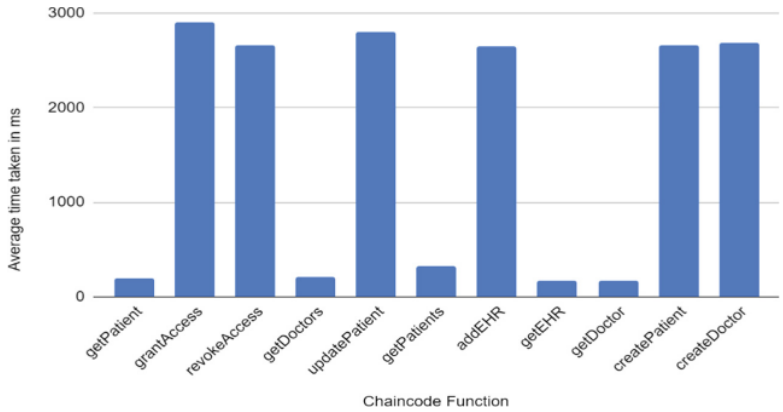

Fig 3 Latency for different functions

Figure 3 shows the average time taken for ten runs for each of the chaincode functions. As expected, the mutate functions take more time than the query functions. The query functions take less than 500 ms latency which shows that this system is a viable technology to deploy a large scale health application in the context of the metaverse. The mutate functions take a couple of seconds which can seem slow but since these functions won't be executed that frequently it will not affect the overall user experience.

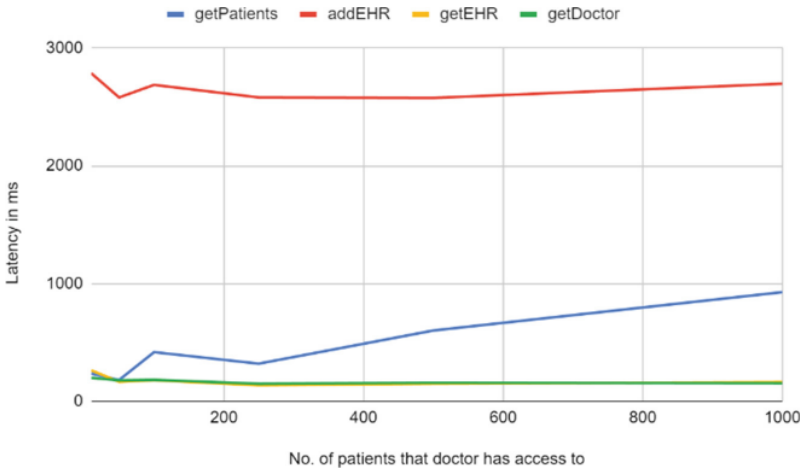

Fig 4 Latency incurred by the doctor functions vs. number of patients (1)

Figure 4 shows the latency incurred by the doctor functions as we increase the number of patients the doctor has access to. Only the latency of getPatients increases linearly as we increase the number of patients. This is expected as we need to iterate through all the patients in the function. The rest of the functions retrieve values based on the key

provided so they are not affected as the number of patients that the doctor has access to increases.

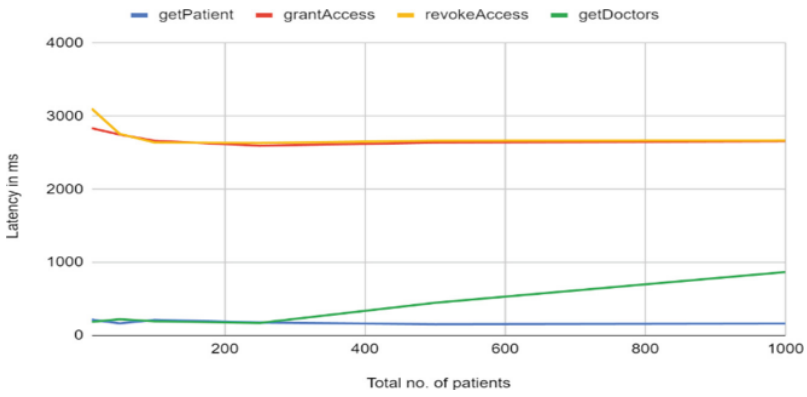

Fig 5 Latency for the patient functions vs. number of patients

Figure 5 depicts the latency incurred for patient functions as the total number of patients in the system increases. Here linearly as we increase the number of patients. Again, only the latency of getDoctors increases linearly as we increase the number of patients as we need to iterate through all the users in the blockchain to check if they are a doctor or not. The rest of the functions retrieve values based on the key provided so they are not affected as the number of patients stored in the blockchain increases.

Manual penetration testing was performed on this system. Insider attacks were easily prevented by role-based access control. If any user doesn't have the required role while executing a chaincode function, the blockchain will prevent them from executing it. For e.g. If an admin who has only access to create the initial patient or doctor record, tries to execute any of the patient or doctor functions like getting a patient EHR or granting access to an EHR record to a doctor, they will be prevented from doing so since their role doesn't match. The same restrictions apply to doctor and patient roles also. External attacks are prevented using a combination of the authentication provided by Amazon Cognito along with the role-based access control in the chaincode. If an attacker is able to get unauthorized access to a user's account, they will still only be able to execute functions that the compromised account has access to. In addition, if they can breach the system and get access to a peer node, the consensus mechanism ensures that the majority honest peer nodes will prevent any dubious transactions or malicious chaincode installation. Hyperledger fabric also makes use of secure cryptographic communication channels during communication between participants which helps prevent eavesdropping, tampering, and interception of data by external attackers.

Ransomware attacks are prevented as the blockchain is distributed which means it stores multiple copies of the blockchain across the peer nodes this ensures that even if an attacker encrypts the data in one of the peer nodes, the data in the other peer nodes will still be accessible.

DDoS attacks are prevented with a combination of native AWS security measures and the distributed nature of the blockchain. AWS Shield is a managed DDoS protection service that is enabled for all AWS customers. Since our system uses AWS, we get this feature for free making our system resilient to DDoS attacks. Due to the distributed nature of blockchain, we can provision peer nodes in multiple AWS availability zones allowing us to failover peer nodes in case of a DDoS attack.

6 Future Work

Future work in this area can include ways to make the system even more resilient to attacks. The following vulnerabilities are identi ed and mitigation steps for each of them are outlined below:

1) Social engineering attacks - An attacker especially in the metaverse can impersonate a doctor and lure an unsuspecting patient to grant access to their EHR.
   These kinds of attacks are hard to prevent but precautions can be taken to minimize risks including storing the hospital that the doctor is af liated to in the blockchain along with the doctor's public key. Any time a patient grants access to their EHR to a doctor, they can check if the hospital af liation or public key matches that of the doctor that they intend to give access to.
2) Compromised patient authentication - Systems like AWS Cognito that rely on username/password for authentication can inadvertently be compromised by an attacker using a keylogger, social engineering or even password guessing. Adding two factor authentication using either digital tokens or physical tokens like YubiKey can help mitigate these attacks. In addition, a noti cation service can be deployed that sends a noti cation to a user if someone tries to access their EHR.
3) AWS Administrator credentials compromised – This can lead to an attacker being able to install malicious chaincode or even get the private key of patients from AWS secrets manager allowing them unchecked access to patients EHR records. These attacks can be prevented by following the principle of least privilege ensuring that no humans are granted the admin role or only certain individuals whose function requires such access are able to do so.
4) DDoS attacks - In addition to AWS Shield, Hyperledger Fabric can be integrated with external security measures, such as rewalls, intrusion detection systems (IDS), and rate-limiting mechanisms, to help mitigate DDoS attacks.
5) Developer Errors - Automated code vulnerability scanning tools can be con gured to detect security vulnerabilities in the code before allowing chaincodes to be redeployed.

7 Conclusion

This paper describes a system for securely storing healthcare records by making use of hyperledger fabric blockchain in AWS. Experiments were conducted to test the latency of different functionalities which proves that the system is suitable for storing healthcare records in the context of metaverse. The use of blockchain technology will also guarantee the con dentiality and protection of sensitive data, rendering it impervious

to unauthorized changes or hacking attempts. The different types of attacks that could occur and ways in which the system can prevent them are also explained in the paper. Additional ways to make the system more secure are discussed which could be taken up as future work.

Acknowledgment This work was in part supported by the National Science Foundation (NSF) (award numbers 1722913 and 1921576).

References

1. Rajeswari, C., et al.: Metaverse for healthcare: a survey on potential applications challenges and future directions. IEEE Access **11**, 12765–12795 (2023)
2. Wang, Y., et al.: A survey on metaverse: Fundamentals, security, and privacy. IEEE Commun. Surv. Tutor. (2022)
3. Shahnaz, A., Usman, Q., Khalid, A.: Using blockchain for electronic health records. IEEE Access **7**, 147782–147795 (2019)
4. Song, Y.-T., Qin, J.: Metaverse and personal healthcare. Procedia Comput. Sci. **210**, 189–197 (2022)
5. AWS Samples. Non-Pro t Blockchain. GitHub Repository. https://github.com/aws-samples/non-pro t-blockchain
6. Gadekallu, T.R., et al.: Blockchain for the metaverse: a review, arXiv preprint arXiv:2203.09738 (2022)
7. Chen, Z., Wu, J., Gan, W., Qi, Z.: Metaverse security and privacy: an overview. arXiv preprint arXiv:2211.14948 (2022)