AN EFFICIENT MEDICAL RECORD SHARING TECHNIC USING BLOCKCHAIN WITH INSURANCE PROCESSING

Sri Dhanalakshmi A M[1], Ganesan T[2]

[1]*Student, Dept. of Computer Science Engineering, E.G.S Pillay Engineering College, Tamilnadu, India.*

[2]*Professor, Dept. of Computer Science Engineering, E.G.S Pillay Engineering College, Tamilnadu, India.*

ABSTRACT- Electronic health records possess the patient's medication details and their health history. The health information attract the attention of the attackers' as it possesses previous records. Loss of electronic health records leads to a wrong medication or surgery. Healthcare systems offer fewer security measures to secure the health information. In traditional electronic health records (EHRs), medical information is usually one at a time managed with the aid of specific hospitals and for that reason it results in the inconvenience of records sharing. Cloud-based EHRs sharing resolve the problem of facts sharing in the traditional EHRs. However, cloud-based EHRs suffer the centralized problem, i.e., cloud service center and key-generation center. Proposed work focus on creating a new EHRs paradigm which can help in dealing with the centralized problem of cloud-based EHRs. The solution is to make use of the emerging technology of blockchain to EHRs(denoted as blockchain-based EHRs for convenience). First, denfine the system model of blockchain-based EHRs in the setting of blockchain. In addition, the authentication trouble could be very important for EHRs. However, current authentication schemes for blockchain-based EHRs have their own susceptible factors. Here also propose an authentication scheme for blockchain-based EHRs. Our proposed scheme is provably secure in the random oracle model and has more efficient signing and verification algorithms than existing authentication schemes. This proposed work also concentrates on insurance claiming process for patients.

Index terms: EHRs Sharing, Blockchain, Implementation, Authentication Verification, Data Distribution, Insurance Claiming.

INTRODUCTION

Access control is a security technique that regulates who or what can view or use sources in computing surroundings. It is a basic concept in protection that minimizes risk to the enterprise or organization. Access control can be manipulated into two categories namely physical and logical. Physical access to manipulate limits access to campuses, buildings, rooms and physical IT property. Logical access control limits connections to computer networks, files and data. Access control structures perform identification authentication and authorization of customers and entities through evaluating required login credentials that may consist of passwords, personal identity numbers (PINs), biometric scans, protection tokens or different authentication elements. Multifactor authentication requires more authentication factors, is regularly a critical part of layered protection to defend access to manipulate systems.

The intention of access control is to reduce threat of unauthorized access to physical and logical structures. Access control is a fundamental thing of safety compliance programs that guarantees security technology and access control policy shield private records, consisting of client information. Recently many companies have infrastructure that limit access to networks, computer systems, packages, files and sensitive information, such as individually identifiable data and intellectual data access.

Access control structures are complicated and can be difficult to manipulate in dynamic IT environments that contain on-premises structures and cloud services. After some excessive-profile breaches, technology vendors have shifted faraway from single sign-on structures to unified access control, which offers access controls for on-premises and cloud environments

1.1 BENEFITS OF ACCESS CONTROL

Interest in cloud-based access to manipulate has surged in recent years, attracting businesses of various sizes and throughout industries. For everybody who has been seen the benefits of cloud-based systems, that's hardly a surprise.

From stream lined system management to pricing flexibility, cloud-primarily based access manipulates offers some very interesting characteristics while compared with conventional, on-premise structures. Some key examples are listed underneath.

1.1.1 Accessibility from anywhere with an Internet connection

While some conventional access control systems provide some remote connectivity, cloud systems are designed with mobile accessibility in thoughts. Authorized users can log into the relevant access to control app, web portal, or network to view or manage device interest. Aside from supplying convenience, this additionally enables customers to obtain alerts and take actions in the event of an incident or emergency.

1.1.2 Flexible cost management

Whereas conventional access control systems frequently include high upfront installation and equipment costs, cloud based services offer lots more flexibility in pricing. Instead of buying online equipment outright, users can prefer to lease equipment from an authorized reseller, avoiding high capital expenditure charges in prefer of modest ongoing operational expenses.

1.1.3 Reduced burden on user

Maintaining a business service takes time and effort, especially for undertaking-critical ones like access control. By turning over the hosting and renovation of on-web site PCs, servers, facts-redundancy infrastructure and associated processes to the integrator, customers can dramatically decrease the weight on their very own IT personnel. Depending on the software itself, a cloud based system can reduce burden of IT involvement by means of 97%. Should the consumer preference, management of the cloud services can be turned into partially or completely to the integrator as well.

1.1.4 System reliability

Storing all records on web site can be quite risky task: Unless the person has robust safeguards in place, a energy surge or network failure can impact service operation or result in the destruction of that data. Cloud-based access control systems usually utilize centralized data centers that are formalized with efficient backup energy and storage systems to ensure the safety and integrity of the cloud service and information.

1.1.5 Round-the-clock updates and monitoring

Software updates and patches are critical for ensuring that the access control system is updated and that any vulnerability is addressed. However, these updates are only beneficial if they are implemented in a well-timed manner. With cloud based access to manage systems, updates may be pushed out quick and simultaneously throughout machine devices, rather than requiring employees to handle them. This helps growth device performance and security, at the same time as lowering the chance of human error. In addition, many cloud-primarily based systems offer 24/7 monitoring services, assisting enhance response time, provide peace of mind and free up stop person workforce to tackle more urgent enterprise challenges.

As with traditional access control system, cloud-based solutions vary from commercial enterprise to enterprise, as do the benefits that customers care maximum about. Perhaps the most exciting gain of all is that customers can locate new methods to not only strengthen facility security, but also optimize IT and other operations commercial enterprise-wide.

1.2 MEDICAL DATA SHARING IN CLOUD

Traditionally, medical data were recorded on paper, which were prone to get damaged and modified. Therefore, it was necessary to preserve the data electronically. However, the medical database could be tampered or deleted permanently. Then, there was also a concern on information blocking. Information blocking occurs when an entity, for example, a person may be with or without his intention to access the data which should not have been seen without the patient's or hospital's concern. Technology always plays a very significant role if it is about enhancing the quality or about resolving issues such as resource allocation along with information blocking, here in medical-care data sharing technology needed to be evolved with time. Generally, patients may have a lot of service providers in terms of medical healthcare that include general physicians or specialists or even therapists. Since a disease could be because of the previous disease, so they all need to share health record securely without any manipulation. Patient need not be always a professional or to have a good memory to remember all the data properly if all the data are stored and shared securely. Patients need to keep updating their own medical data history. Moreover, if the data that are transferred are in paper mode or even through email, there is time, speed, storage, and security issues. Storing data in a database has many limitations such as storage and prone to cyber-attacks. Attackers may intrude into the system and get some patient's sensitive data. One can also not rely upon a centralized database because practically different access controls for different users, searching procedure over an encrypted channel, large memory for medical data storage etc. Therefore, researches came up with a solution of blockchain technology in medical healthcare, which will not only protect data from being tampered but will also ensure

that the data leakage is stopped. This technology could preserve data and thus guarantee reliability. And if this technology is used along with cloud computing technology, problems related to storage can also be vanished, because cloud is trusted for storing and managing data. Also, the blockchain can address the security issues of the cloud. Indeed, medical data sharing and storing with Blockchain-based cloud can address a lot of issues of medical data.

LITERATURE SERVEY

[1] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems." IEEE Access 6 (2018): 11676-11686.

Present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of *N* from *N*-1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. Assuming that there is an EHRs system in a cloud storage platform, which consists of some departments, such as hospitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, an EHRs system with a blockchain structure is designed as shown in Fig. 3. Suppose that every patient owns one blockchain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. is encapsulated in one block. Patient treatments at different times will be generated in different blocks. Then, a series of blocks are generated according to the time sequence and a healthcare blockchain of this patient is constructed. Authorized entity might look over the health records of this patient by means of his blockchain, and has powerless to tamper the data in established block (such as drug allergy and dosage). When the patient goes to be treated in other clinical departments or hospitals next time, the new entity needs to identify this patient and authenticate his available blockchain, which could save the medical resources and avoid the repeated detection.

[2] Dagher, Gaby G., Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology." Sustainable Cities and Society 39 (2018): 283-297.

Propose a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. Our proposed framework, Ancile, uses six unique types of smart contracts for operation: Consensus, Classification, Service History, Ownership, Permissions, and Re-encryption. By using six separate contracts, we enable patients to benefit from increased utility while minimizing the need to interact with every contract. This improves the efficiency of the patient experience and reduces privacy threats. To create a high level of separation, we use the contracts to generate other contracts. In doing so, the patient can be the only node expressly given the location of their information. Using smart contracts, Ancile maintains cryptographic hashes of stored records and query links, confirming the integrity of EHR Databases. Patients can also view and control who has permissions for their private information by using a smart contract to manage access control. Moreover, patients may give transfer permissions to other nodes. This is possible through the use of identity-checking, to confirm who may access records, and proxy re-encryption, to avoid having to reencrypt the record for each transfer. Furthermore, by sending the query links for the records securely off of the blockchain, Ancile ensures that the three tools required to access an EHR, the encrypted record, the query link, and the symmetric key, are in different locations.

[3] Mehmood, Abid, Iynkaran Natgunanathan, Yong Xiang, Howard Poston, and Yushu Zhang. "Anonymous authentication scheme for smart cloud based healthcare applications." IEEE access 6 (2018): 33552-33567.

Propose a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. The primary goal of this paper is to provide identity privacy for smart cloud based healthcare applications by providing anonymous authentication. The proposed scheme can be generalized and applied to other cloud based applications. In some scenarios, user can potentially be identified by the operations performed on a specific set of data over time. Therefore, the proposed scheme is most suitable for scenarios where the specific user cannot be identified by operations over the data. It is worth noting that other issues such as location privacy and query privacy in smart health application are equally important. The patients can book an appointment with a healthcare professional or call an ambulance in case of emergency using the smart phone without revealing their

identities. In remote health care monitoring, information of interest like blood pressure level or heart rate is gathered by the sensors attached to the body and transmitted by a controller (mobile devices or personal digital assistants) to a server where it is processed. Consider an example of a patient where an application raises an alarm automatically when the readings from the sensors go above the threshold. For example, relevant authorities (i.e., ambulance service) can be notified when patient's blood pressure goes above the threshold with the chronic heart disease or whenever a patient with dementia in assisted living facilities goes out of their defined boundaries on a given map.

[4] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42, no. 8 (2018): 152.

Propose a cloud-based EHR system uses attribute-based cryptosystem and blockchain technology. In this system, we use ABE and IBE to encrypt data, ensuring fine-grained access control for encrypted data, and use IBS to implement digital signatures. To achieve different functions of attribute-based encryption (ABE), identity-based encryption (IBE) and identity-based signature (IBS) in one cryptosystem, we introduce a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES). This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. In addition, we use blockchain technology to ensure that the medical data cannot be tampered with, and the data sources can be traced. Finally, we give a demonstrating application for medical insurance scene. In this system, patients authorize their data access policy (with their signature) to the hospital according to their actual need, and submit the signed authorization letters to the blockchain data pool to wait for the consensus nodes processing. The hospital will encrypt patients medical data under the specified access policy, and submit the encrypted data with hospitals signature to the data pool. The consensus nodes will keep monitoring the data pool, and capture the matched authorization letter (submitted by the patients) and encrypted data (submitted by the hospital). They will verify the corresponding signature to ensure that the data are complete and authorized by the patients. Then, the consensus nodes will perform a consensus protocol to select a bookkeeping node. The bookkeeping node will submit the encrypted data to the medical cloud and write the description of the data along with the address of the data in the cloud to the blockchain.

[5] Sun, You, Rui Zhang, Xin Wang, Kaiqiang Gao, and Ling Liu. "A decentralizing attribute-based signature for healthcare blockchain." In 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1-9. IEEE, 2018.

Propose a decentralized attribute-based signature scheme for healthcare blockchain, which provides efficient privacy-preserving verification of authenticity of EHR data and signer's identity. First, propose a decentralizing attribute-based signature (called DABS) scheme for providing privacy preserving verification service in a healthcare blockchain. The scheme has two salient features: (1) It can effectively verify the attributes of the signer without exposing the identity of the signer; (2) The decentralized attribute based signing property makes it suitable for the distributed blockchain system. In our DABS scheme, multiple attribute authorities may issue attribute certification and corresponding signature keys to users without relying on a central authority agency to supervise and manage them. Second, we propose a blockchain-based EHR data storage system for secure sharing EHR data among different CDOs though an effective on-chain and off-chain collaboration storage model. Our blockchain based storage system has a number of advantages: (1) Using blockchain to realize security sharing of EHR data across different CDOs such that the stored and shared EHR data are non tampered, unforgivable and verifiable. (2) Adopt the combination of on-chain and off-chain storage to realize the secure sharing of large-scale and distributed EHR data. The address of each EHR data record is stored in a transaction on the blockchain, and the EHR data is stored in each node off the blockchain. This makes it easier for users to locate each piece of EHR data while circumvents the storage limitation of the blocks. Finally, provide formal security analysis of the proposed DABS verification protocol with respect to unforgeability, security against collusion attacks, anonymity, and non-repudiation. Our experimental evaluation demonstrates that the proposed DABS scheme is effective and easily deployable.

[6] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Enforcing role-based access control for secure data storage in the cloud." The Computer Journal 54, no. 10 (2011): 1675-1687.

An encryption scheme is proposed which incorporates the cryptographic approaches with RBAC and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. A real-time method is provided to maintain a secure communication in cloud computing which ensures security as well as trust-based access to cloud. The proposed model contains algorithms to explain data protection and user authentication problems.

A secure RBAC based cloud storage system is proposed in this paper. In our system, the Data Owner encrypts the data in such a way that only the Data Users with relevant access policies can decrypt and view the data. The cloud service provider (who stores the data) will not be able to see the content of the data without the specified access policy. To prevent the admission of malicious Data Owner to cloud, an Admission Policy is proposed. Based on this policy, only genuine Data Owners can get admission to cloud which is based on voting by existing Data Owners. The authentication mechanism plays a vital role in security enhancement. Authentication mechanism is like an entrance door and will allow only the trusted individuals to enter in the cloud premises. The mechanism should be robust enough to ensure availability by letting the right person in, any time and any place. Authentication mechanism can be combined with cryptographic techniques to ensure confidentiality of data.

[7] Gupta, Shubhi, Swati Vashisht, and Divya Singh. "Enhancing Big Data Security Using Elliptic Curve Cryptography." In 2019 International Conference on Automation, Technology Management (ICACTM), pp. 348-351. IEEE, 2019.

Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. In order to provide the safety and security assurance to the users data, we propose a Data security model that uses Elliptic curve cryptosystem for digital signature. Strength of the algorithm depends on the difficulty level of computing discrete logs in a large prime modulus. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient a reason to believe that the message was created by a known sender, and that it was not altered in transit. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington)as an alternative mechanism for implementing public-key cryptography. In this work both digital signature scheme and public key cryptography are integrated to enhance the security level of Cloud. The encryption of digital signature into cipher text is done.

[8] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. "Public integrity auditing for shared dynamic cloud data with group user revocation." IEEE Transactions on Computers 65, no. 8 (2015): 2363-2373.

Provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the scheme definition. Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users. The TPA could efficiently verify the integrity of the data stored in the cloud storage server, even the data is frequently updated by the group users. The data owner is different from the other group users, he/she could securely revoke a group user when a group user is found malicious or the contract of the user is expired. In this case, although the server proxy group user revocation way brings much communication and computation cost saving, it will make the scheme insecure against a malicious cloud storage server who can get the secret key of revoked users during the user revocation phase. Thus, a malicious cloud server will be able to make data m, last modified by a user that needed to be revoked, into a malicious data. In the user revocation process, the cloud could make the malicious data m′ become valid. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource ciphertext database to remote cloud and support secure group users revocation to shared dynamic data. We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. Also, the performance analysis shows that, compared with its relevant schemes, our scheme is also efficient in different phases.

[9] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8, no. 12 (2013): 1947-1960.

Propose a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. Our RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, we present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. In this paper, we present the design of a secure RBAC based cloud storage system where the access control policies are enforced by a new role-based encryption (RBE) that we proposed in the paper. This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation using an broadcast encryption1 mechanism. In our RBE scheme, the owner of the data encrypts the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The role grants permissions to users who qualify the role and can also revoke the permissions from existing users of the role. The cloud provider (who stores the data) will not be able to see the content of the data if the provider is not given the appropriate role. Our RBE scheme is able to deal with role hierarchies, whereby roles inherit permissions form other roles. A user is able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner dose not need to re-encrypt the data. A user can be revoked at any time in which case, the revoked user will not have access to any future encrypted data for this role. With our new RBE scheme, revocation of a user from a role does not affect other users and roles in the system. In addition, we outsource part of the decryption computation in the scheme to the cloud, in which only public parameters are involved. By using this approach, our RBE scheme achieves an efficient decryption on the client side.

[10] Fu, Anmin, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang. "NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users." IEEE Transactions on Big Data (2017).

Propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least t group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides nonframeability. Here establish a model for data (in a group) shared with multiple group managers, and propose a new privacy preservation public auditing scheme for multiple group managers in shared cloud storage. This proposed scheme can not only provide multi-levels privacy-preservation abilities (including identity privacy, traceability and non-frameability), but also can well support group user revocation. 2) We design a data structure based on a binary tree for clouds to record all the changes of data blocks. Group users can trace the data changes through the binary tree and recover the latest correct data block when the current data block is damaged. 3) We utilize an authorized authenticate process to verify TPA's challenge messages. Therefore, only the TPA who has been authorized by the group users can pass the authentication and then challenge the cloud, which protects clouds from malicious challenges.

The PKG sets parameters for the entire system, distributes the group key pair {mpkl; mskl} and a shared public/private key pair {spk,ssk} used to authorize each GMl, and initializes the membership information Ω . Then, any GM generates a user signing key uski, a (public) user membership key upki, and a user revocation key rvki for Ui. GM also shares the authorization key pair {spk, ssk} with Ui in the Enroll procedure. Once a group user is revoked, GM invokes the Revoke algorithm to update Ω. The group user can compute the signatures of the shared data block from the issued keys in the Sign process. With the Authorize algorithm, the group authorizes TPA to generate authorized auditing challenges, and then the valid TPA can check the integrity of the shared data on behalf of the group user. Once the cloud receives a challenge from TPA, the cloud verifies whether the challenge has been authorized and decides whether to generate the audit proof via ProofGen. TPA checks the correctness of the proof via ProofVerify. Finally, in the Open process, at least t GMs work together to trace the real identity of the signer.

I. RELATED WORK

Guo, et.al,.[1] Present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of *N* from *N*-1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. Assuming that there is an EHRs system in a cloud storage platform, which consists of

some departments, such as hospitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse.

Dagher, et.al,.[2] Propose a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. Our proposed framework, Ancile, uses six unique types of smart contracts for operation: Consensus, Classification, Service History, Ownership, Permissions, and Re-encryption. By using six separate contracts, we enable patients to benefit from increased utility while minimizing the need to interact with every contract. This improves the efficiency of the patient experience and reduces privacy threats. To create a high level of separation, we use the contracts to generate other contracts. In doing so, the patient can be the only node expressly given the location of their information. Using smart contracts, Ancile maintains cryptographic hashes of stored records and query links, confirming the integrity of EHR Databases. Patients can also view and control who has permissions for their private information by using a smart contract to manage access control. Moreover, patients may give transfer permissions to other nodes. This is possible through the use of identity-checking, to confirm who may access records, and proxy re-encryption, to avoid having to reencrypt the record for each transfer.

Mehmood, et.al,.[3] Propose a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. The primary goal of this paper is to provide identity privacy for smart cloud based healthcare applications by providing anonymous authentication. The proposed scheme can be generalized and applied to other cloud based applications. In some scenarios, user can potentially be identified by the operations performed on a specific set of data over time. Therefore, the proposed scheme is most suitable for scenarios where the specific user cannot be identified by operations over the data. It is worth noting that other issues such as location privacy and query privacy in smart health application are equally important. The patients can book an appointment with a healthcare professional or call an ambulance in case of emergency using the smart phone without revealing their identities.

Wang, et.al,.[4] Propose a cloud-based EHR system uses attribute-based cryptosystem and blockchain technology. In this system, we use ABE and IBE to encrypt data, ensuring fine-grained access control for encrypted data, and use IBS to implement digital signatures. To achieve different functions of attribute-based encryption (ABE), identity-based encryption (IBE) and identity-based signature (IBS) in one cryptosystem, we introduce a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES). This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. In addition, we use blockchain technology to ensure that the medical data cannot be tampered with, and the data sources can be traced. Finally, we give a demonstrating application for medical insurance scene. In this system, patients authorize their data access policy (with their signature) to the hospital according to their actual need, and submit the signed authorization letters to the blockchain data pool to wait for the consensus nodes processing.

Sun, et.al,.[5] propose a blockchain-based EHR data storage system for secure sharing EHR data among different CDOs though an effective on-chain and off-chain collaboration storage model. Our blockchain based storage system has a number of advantages: (1) Using blockchain to realize security sharing of EHR data across different CDOs such that the stored and shared EHR data are non-tampered, enforceable and verifiable. (2) Adopt the combination of on-chain and off-chain storage to realize the secure sharing of large-scale and distributed EHR data. The address of each EHR data record is stored in a transaction on the blockchain, and the EHR data is stored in each node off the blockchain. This makes it easier for users to locate each piece of EHR data while circumvents the storage limitation of the blocks. Finally, provide formal security analysis of the proposed DABS verification protocol with respect to unforgeability, security against collusion attacks, anonymity, and non-repudiation. Our experimental evaluation demonstrates that the proposed DABS scheme is effective and easily deployable.

II. EXISTING METHODOLOGIES

In EHRs, all medical-related data are digitized and stored in the server of hospital. Then, when a patient goes back to the hospital, he or the hospital can search previous information, including names of the patient and doctor, time, diagnosis, and so on. As an important application in the medical field, EHRs have attracted wide attention. Existing system works on creating a new EHRs paradigm which can help in dealing with the problems in cloud-based EHRs. The solution is to make use of the emerging technology of blockchain. Generally speaking, blockchain can be seem as a decentralized and distributed database. There is authority in traditional network architectures or application systems, such as KGC, cloud service provider, and so on. Authentication is very important for blockchain-based EHRs. It is different from the case of block chain which is

anonymous and thus there is no authentication mechanism for users, the data in blockchain-based EHRs must be authenticated, such as diagnosis from doctors. Therefore, design an efficient authentication scheme for blockchain-based EHRs. Existing proposal is an identity-based signature scheme with multiple authorities (MA-IBS) which has both efficient signing and verification algorithms and can resist collusion attack.

IDENTITY BASED ENCRYPTION

In existing work, implementing a revocable-storage identity-based encryption (RS-IBE), this provides the forward/backward security of cipher text by introducing additional functionalities of user revocation and cipher text update simultaneously.

IBE

Identity Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Identity-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted third party is denoted by Private Key Generator (PKG) that generates the corresponding private keys. The PKG first provides a master public key, and then provide the corresponding master private key. Given the master public key, any user can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To acquire a corresponding personal key, the user authorized to apply the identity ID contacts the PKG, which uses the master key to generate the personal key for Identity ID. Thus, users may additionally encrypt messages with out a earlier distribution of keys among individual contributors. This is useful in instances wherein pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized person must achieve the ideal personal key from the PKG.

RS-IBE

The non-revocable data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then reencrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the effect of secret key need to be restrained to best common decryption, and it is inadvisable to replace the cipher textual content periodically through the usage of secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

III. MEDICAL DATA SHARING USING BLOCKCHAIN WITH INSURANCE CLAIMING

In order to solve the problem of information sharing in the traditional EHRs, researchers introduced the notion of could based EHRs. The cloud-based EHRs can be seem as an application of the could computing technology in EHRs. In cloud-based EHRs systems, there still needs a cloud service provider who plays the role of authority. All medical-related data, from doc tor, pharmacy, diagnostic laboratory, insurance center, and so on, will be uploaded to the cloud server. Then, users can search and download useful information from the could server. If several organizations share a same cloud server, then they can share the data with a convenient way. Next, when patients transfer from a hospital to another one, the new hospital can obtain patients' medical-related data from the cloud and thus they have no need to, once again, get medical examinations. Therefore, cloud-based EHRs solve the problem of information sharing in the traditional EHRs. In addition, in cloud-based EHRs, all data are only maintained by the authority, i.e., cloud service provider, and thus the hospitals and other organizations could tamper the medical-related data only when they collude with the authority.

To enable data sharing in the Cloud, it is essential that only authorized users are able to get access to data stored in the Cloud. Proposed work divides the users of blockchain-based EHRs into two levels. The first level, denoted by Level 0, is the EHRs server. The second level, denoted by Level 1, contains medical insurance companies. In blockchain-based EHRs systems, all medical related data will be distributed stored by all Level 1 users who can reach a consensus, for the authenticity of the shared data, based on a specific mechanism. The responsibilities of Level 2 users are that generate medical-related information, such as medical records from doctors, insurance policies from insurance agent, and so on. The decentralized feature of blockchain gets rid of such dependence on authority. Therefore, many people considered the applications of blockchain in different types of real-world scenarios, including EHRs, we call it blockchain-based EHRs.

The authenticity of such information can be guaranteed by a proper authorization mechanism from Level 1 users to their patients. The proposed framework only allows verified users or stakeholders to access a system. The actions of the users can be monitored by the proposed blockchain-based framework. Sharing of patient's data is verified, by adopting the cryptographic techniques. The

system is a mediator between users and sensitive healthcare data. The system proposed by them used a lightweight blockchain that ensures fast transactions and proper efficiency. Therefore, cloud-based EHRs solve the problem of information sharing in the traditional EHRs. In addition, in cloud-based EHRs, all data are only maintained by the authority, i.e., cloud service provider, and thus the hospitals and other organizations could tamper the medical-related data only when they collude with the authority.

Blockchain technology functions are reliable for use in a hashing crypto method, which helps create an adequate and strong hashing code and convert it from a bit of fixed size data to strings of character. Each transaction proposed in a blockchain are hashed together before shoving in a block, and the hash pointers connect each block to the next block for holding of previous hash data as it is undisputable. Therefore, any changes in the blockchain transaction of hashing function will result in different hash string of character and affect all the involved blocks.

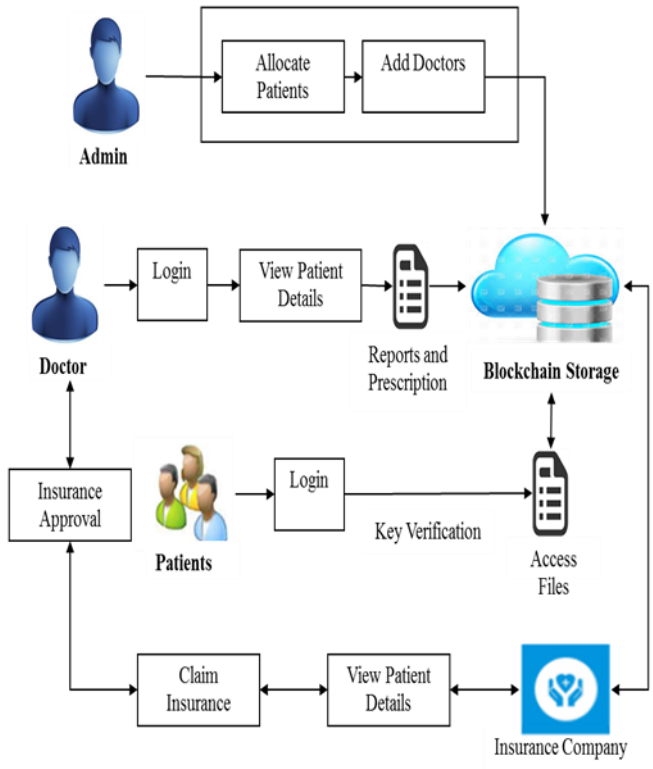

Fig 4.1: Architecture for Proposed Work

METHODOLOGY

Blockchain Technology

A blockchain is a digital concept to store **data**. These blocks are chained together, and this makes their data immutable. When a block of data is chained to the other blocks, its data can never be changed again. It will be publicly available to anyone who wants to see it ever again, in exactly the way it was once added to the blockchain.

The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA2, and SHA-256) encryption because of their unique quality of hash function that creates unique outputs when given different inputs. The hash function here is a unique key created to identify a transaction that at the same time identifies an individual in the petroleum supply chain.

Block and Hash Generation

1. Each data generates a hash.
2.A Block containg information about current transactions.
3. A hash is a string of numbers and letters.
4.Transactions are entered in the order in which they occurred.
5.The hash depends not only on the transaction but the previous transaction's hash.
6. Even a small change in a transaction creates a completely new hash.
7. The nodes check to make sure a transaction has not been changed by inspecting the hash.
8. If a transaction is approved by a majority of the nodes then it is written into a block.
9. Each block refers to the previous block and together make the Blockchain.
10.A Blockchain is effective as it is spread over many computers, each of which has a copy of the Blockchain.

AES Encryption

The AES cipher is also known as the block cipher. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes from a look-up table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size. For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption.

Algorithm Procedure

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages.

This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key
The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns
Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

V EXPERIMENTAL RESULTS

Experimental result shows the overall performance of the proposed system. Here access control based medical data sharing and insurance claiming process are implemented using ASP.NET as front end and SQL as back end software. This will helps to improve file security.

BLOCK CHAIN STORAGE

This explains about secure health record storage using blockchain system. This framework consists of doctor login, user login, new user registration, insurance company login and new insurance company registration process.

ADMIN CREDENTIALS

Admin is an authority to access application and maintain the details of proposed application. Admin should have the process of login, view user details, new user registration process, and new doctor registration process and allocate the patients for specified doctors based on their problems.

DATA UPLOAD

Doctor is a cloud client who registers with the CSP (Cloud Service Provider) by admin. Doctor outsources data to cloud in encrypted form. Doctors are anonymously get authenticated to cloud while getting duly authenticated. Doctors can view the allocated patient details and upload medical records of the patients to the block based cloud storage. It is the duty of the doctor to prevent the admission of malicious Patient's to cloud. The encrypted medical record is uploaded to the cloud by the doctor. SHA 256 used for hash key generation in cloud storage. Each data has unique hash code and depends on the preceding data block. This framework has following process like doctor login, view patient request, provide confirmation for patient request then upload reports for patient. The uploaded data are stored based on the blockchain technology. Data are sealed with the help of sealing using hash code generation.

DATA ENCRYPTION

Uploaded medical data could be encrypted with the help of AES (Advanced Encryption Standard) algorithm. Encryption helps to increase the confidentiality of the shared information. The algorithms procedure of AES could convert the data into unpredictable form. Authorized users can only decrypt and access encrypted information from cloud with data owner's permission. Otherwise no one can access original information from cloud.

AES Encryption

The AES cipher is also known as the block cipher. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes from a look-up table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size. For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption.

Algorithm Procedure

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key
The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns
Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

This explains about data encryption process. Here AES algorithm was implemented to convert the uploaded data into encrypted form. Authorized users can only access data with the help of secret key and decryption approach. Otherwise no one can access data without secret key.

INSURANCE CLAIM

Insurance claiming is the process of claim the insurance to patients for those who are present in need. Company should register and authenticated for accessing medical data sharing application. Then they can view patient details and send request for insurance claiming. Company should register and create login id. Then add policy information in database. After that companies can view user information and provide insurance request to the doctor. After getting approval from doctor, company can claim insurance for the specified patient.

VI CONCLUSION

Blockchain technology maximizes security and accessibility. The technology can be used in many different areas of the healthcare system, such as for storing and sharing medical records and insurance information in healthcare venues and remote monitoring systems, and for clinical trials. This research work provides efficient access control policy based on users role also implement secure encryption using AES encryption algorithm. The cloud storage requires secure access control to preserve privacy of data. This proposed blockchain based storage model which allows a healthcare organization to store data securely in a public cloud. The proposed model also performs the insurance claiming operations efficiently.

REFERENCES

[1] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, ``Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,'' Sustain. Cities Soc., vol. 39, pp. 283297, May 2018.
[2] W. J. Gordon and C. Catalini, ``Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,'' compute. Structural Biotechnol. J., vol. 16, pp. 224230, 2018.
[3] R. Guo, H. Shi, Q. Zhao, and D. Zheng, ``Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,'' IEEE Access, vol. 6, pp. 1167611686, 2018.
[4] H. Li, Y. Dai, and X. Lin, ``Efficient e-health data release with consistency guarantee under differential privacy,'' in Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom), 2016, pp. 602608
[5] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, ``Anonymous authentication scheme for smart cloud based healthcare applications,'' IEEE Access, vol. 6, pp. 33552_33567, 2018.
[6] U. Premarathne et al., ``Hybrid cryptographic access control for cloud-based EHR systems,'' IEEE Cloud Comput., vol. 3, no. 4, pp. 58_64, Aug. 2016.
[7] H. Wang and Y. Song, ``Secure cloud-based EHR system using attribute-based cryptosystem and blockchain,'' J. Med. Syst., vol. 42, no. 8, p. 152, 2018
[8] W. Xu, L.Wu, andY.Yan, ``Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption,'' J. Comput. Res. Develop., vol. 55, no. 10, pp. 2233_2243, 2018.
[9] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenboloom, ``FHIRChain: Applying blockchain to securely and scalable share clinical data,'' Computed. Structural Biotechnology. J., vol. 16, pp. 267_278, 2018.
[10] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, ``Privacy-preserving attribute-based access control model for XML-based electronic health record system,'' IEEE Access, vol. 6, pp. 9114_9128, 2018.
[11] KohilaKanagalakshmi T; Ms. Lavita; Shweta Biradar. "A Conceptual Study of Blockchain to Financial Sector". International Research Journal on Advanced Science Hub, 2, 8, 2020, 112-117. doi: 10.47392/irjash.2020.103
[12] Neetha S.S; Michel Rwibasira; Suchithra R. "A Survey Paper on Cloud Security Based on Distributed Ledgers of Blockchain". *International Research Journal on Advanced Science Hub*, 3, 3, 2021, 38-42.
[13] Sona Solanki; Asha D Solanki. "Review of Deployment of Machine Learning in Blockchain Methodology". *International Research Journal on Advanced Science Hub*, 2, 9, 2020, 14-20. doi: 10.47392/irjash.2020.141
[14] KohilaKanagalakshmi T; Ms. Lavita; Shweta Biradar. "A Conceptual Study of Blockchain to Financial Sector". *International Research Journal on Advanced Science Hub*, 2, 8, 2020, 112-117. doi: 10.47392/irjash.2020.103