ADVANCE ENCRYPTION STANDARD BASED ACCESS CONTROL WITH BLOCK CHAIN SECURITY IN PERSONAL HEALTH RECORDS

Shobana T.S[1], Rohan H S[2] Aditya Lall[3], Gagan Kashyap M[4]
[1]Assistant Professor Dept. of Information Science B.M.S. College of Engineering (affiliated to VTU) Bengaluru, India.
[1]shobanats.ise@bmsce.ac.in
[2,3,4]UG Scholar, Dept. of Information Science B.M.S. College of Engineering (affiliated to VTU) Bengaluru, India
[2]rohan.is17@bmsce.ac.in, [3]1bm16is097@bmsce.ac.in, [4]1bm16is033@bmsce.ac.in

Abstract— Personal health records (PHR) Associate in Nursing growing health statistics alternate model, that allows PHR owners to expeditiously proportion their private health information amongst a range of customers in addition to interest specialists nonetheless as own circle of relatives and buddies to verify PHR proprietors control in their outsourced PHR information, characteristic primarily based totally by and large encoding (ABE) mechanisms are notion of. A patient-centric, characteristic primarily based totally more often than not PHR sharing topic which would possibly deliver flexible get entry to for every professional customers like medical doctors nonetheless as non-public customers like own circle of relatives and friends. each PHR document is encrypted Associate in Nursing preserve on in a totally interest cloud on the facet of an characteristic primarily based totally more often than not get entry to coverage that controls the get entry to the encrypted resource.

Keywords— Personal Health Record (PHR),Block chain Technology, Advanced Encryption Standard, Cipher key Generation, Security and Privacy.

INTRODUCTION

In current year, Personal Health Record (PHR) has evolved due to the fact the growing fashion in the care generation and via way of means of that the sufferers location unit expeditiously capable of produce, control and percentage their non-public health info. Cloud garage allows the PHRs to be outsourced to cloud infrastructures in preference to storing them regionally. This technique probably finally ends up in better handiness of fitness information likewise as relieving the sufferers from the weight of keeping them. It is extraordinarily important to own the high- quality grained get entry to control over the data with the semi-relied on server. But at some point of this the PHR system, the safety, privacy and health information confidentiality location unit developing demanding situations to the customers as soon as the PHR keep within the third party storage area unit like cloud services.

The PHR information should be secured from the outside attackers and conjointly it should be guard from the internal attackers such from the cloud server company itself. Block chain has drawn interest because the next-era monetary era because of its safety that fits the information era. In particular, it gives safety via the authentication of peers that percentage digital cash, encryption, and the generation of hash value

According to the worldwide economic industry, the marketplace for security-primarily based totally block chain era is predicted to develop to approximately USD 20 billion by 2020. In addition, block chain may be implemented past the Internet of Things, (IoT) environment; its applications are anticipated to expand. Cloud computing has been dramatically followed in all IT environments for its performance and availability. In this paper, we talk the idea of block chain technology and its warm studies trends. In addition, we are able to examine a way to adapt block chain security to cloud computing and its steady answers in detail.

Storage has many benefits, along with always-online, pay-as-you-go, and cheap. During those years, greater information are outsourced to public cloud for chronic garage, such as private and commercial enterprise documents. It brings a protection difficulty to information proprietors the general public cloud isn't trusted, and the outsourced information must now no longer be leaked to the cloud company without the permission from information proprietors.

Many garage structures use server-ruled get right of entry to control, like password-primarily based totally and certificate-primarily based totally authentication. They overly consider the cloud issuer to defend their touchy records. The cloud vendors and their personnel can study any report no matter records owners' get admission to policy. Besides, the cloud issuer can exaggerate the useful resource intake of the record garage and price the payers greater without imparting verifiable records, when you consider that we lack a machine for verifiable computation of the useful resource usage.

Relying on the prevailing server-ruled get entry to manage isn't always secure. Data proprietors who keep documents on cloud servers nonetheless need to manipulate the get entry to on their very own arms and hold the records private in opposition to the cloud issuer and malicious customers. Encryption isn't always sufficient. To upload the confidentiality guarantee, records proprietors can encrypt the documents and set a get entry to coverage in order that handiest certified customers can decrypt the document. With Cipher text-Policy Attribute-based Encryption (CP-ABE), we are able to have each fine- grained get admission to manipulate and sturdy confidentiality. However, this get admission to manipulate is most effective to be had for facts owners, which seems to be insufficient. If the cloud issuer cannot authenticate customers earlier than downloading, like in lots of current CP-ABE cloud storage systems , the cloud has to permit anybody to down load to make sure availability. This makes the storage gadget at risk of the resource-exhaustion attacks. If we solve this hassle through having facts proprietors authenticate the downloader's earlier than permitting them to download, we lose the ability of get admission to manipulate from CP-ABE. Cloud computing has been implemented to many IT environments because of its performance and availability. Moreover, cloud protection and privacy troubles had been mentioned in phrases of vital protection elements: confidentiality, integrity, authentication, access control, and so on.

In this paper, we are searching for to analyze the definition and base generation of block chain and survey the trend of research so far to speak about regions to be studied, thinking about cloud computing environments. In addition, we talk the concerns for block chain safety and stable answers in detail. This paper research the block chain technology and surveys the block chain through studying typical generation and research trends. The outcomes of this studies can function vital base records in analyzing block chain and could useful resource in information the recognized protection issues as a result far. We can foster the improvement of destiny block chain generation through information the trend of block chain protection.

Problem Statement

In projected system Associate in Nursing attribute based mostly authorization mechanism want to authorize access requesting users to access a given PHR resource supported the associated access policy whereas utilizing a proxy re-encryption theme to facilitate the approved users to decode the specified PHR files. Additionally use Multi authority attribute based mostly encoding theme. It provides the safety and confidentiality to the PHR knowledge. Using block chain in PHR can provide higher security compared to storing all data in a central database. In the data storage and management aspect, damage from attacks on a database can be prevented.

Moreover, since the block chain has an openness attribute, it can provide transparency in data.

Proposed System

The system or application is moved to cloud storage giving access to all the users such as patient and doctors to share the communications. Using a security model in the cloud using

Attribute Based Encryption a strong encryption performance wise strong and more secured. The token data for each PHR file is generated. Only through that token attribute the PHR file can be read and the doctor's suggestion to PHR file can be given. Block chain technology has the capability to appreciably regulate the manner corporations behavior commercial enterprise in addition to the manner establishments system transactions. Businesses and governments regularly function in isolation however with block chain technology contributors can have interaction in commercial enterprise transactions with customers, suppliers, regulators, doubtlessly spanning throughout geographical boundaries.

I. LITERATURE SURVEY

There have been several research works regarding the Advance Encryption Standard Based Access Control with block chain security in Personal Health Records in prevention of fraudulent activities on health care websites.

Authors of [1] shows Cloud computing represents ultra-modern maximum thrilling computing paradigm shift in records technology. However, safety and privacy are perceived as number one limitations to its extensive adoption. Here, the authors define numerous vital safety demanding situations and inspire in addition research of safety answers for a truthful public cloud environment.

Further, the authors of [2] have put forward yet another viewpoint where they have shown the usage of Public-key virtual certificates which has been broadly utilized in public-key infrastructure (PKI) to offer person public key authentication. However, the general public-key virtual certificates itself can't be used as a protection element to authenticate person. In this paper, we advise the idea of generalized virtual certificates (GDC) that may be used to offer person authentication and key agreement. A GDC includes person's public facts, along with the facts of person's virtual driver's license, the facts of a virtual start certificates, etc., and a virtual signature of the general public facts signed through a depended on certificates authority (CA). However, the GDC does now no longer include any user's public key. Since the user does now no longer have any private and public key pair, key management in the use of GDC is a great deal less difficult than the use of public-key digital certificate. The digital signature of the GDC is used as a secret token of every user in an effort to in no way be found out to any verifier. Instead, the proprietor proves to the verifier that he has the understanding of the signature with the aid of using responding to the verifier's challenge. Based on this concept, we advocate each discrete logarithm (DL)-based and integer factoring (IF)-based protocols which can attain user authentication and secret key establishment.

The authors of [3] talk about besides attracting a billion dollar economy, Bit coin revolutionized the sphere of virtual currencies and inspired many adjoining areas. This additionally precipitated large medical interest. In this survey, we unroll and shape the many fold outcomes and studies directions. We begin through introducing the Bit coin protocol and its constructing blocks. From there we retain to discover the layout area through discussing current contributions and outcomes. In the process, we deduce the essential systems and insights on the middle of the Bit coin protocol and its applications. As we display and discuss, many key thoughts are like wise relevant in numerous different fields, in order that their effect reaches a ways past Bit coin itself.

However Authors of [4] suggested that Smart grids ready with bi-directional communication waft are anticipated to offer greater sophisticated intake tracking and power buying and selling. However, the troubles associated with the safety and privacy of intake and buying and selling information gift severe challenges. In this paper we cope with the trouble of offering transaction safety in decentralized clever grid power buying and selling without reliance on relied on third parties. We have applied a proof-of- idea for decentralized energy trading system using block chain technology, multi-signatures, and nameless encrypted messaging streams, permitting friends to anonymously negotiate power charges and securely carry out buying and selling transactions. We performed case research to carry out safety evaluation and over all performance assessment inside the context of the elicited safety and privacy requirements.

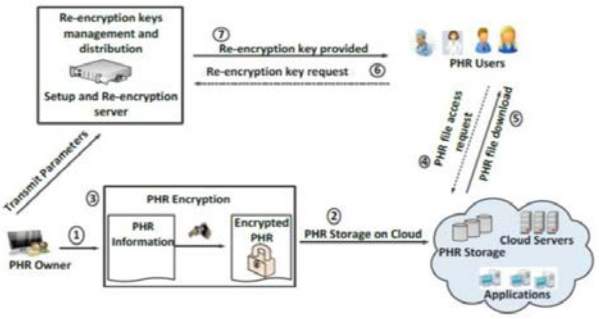
Authors of [5] demonstrated Cloud computing is arising computing paradigm wherein sources of the computing infrastructure are furnished as offerings over the Internet. As promising because it is, this paradigm additionally brings forth many new demanding situations for statistics safety and get right of entry to manipulate while users outsource touchy statistics for sharing on cloud servers, which aren't in the identical relied on area as statistics owners. To hold touchy user statistics exclusive towards un trusted servers, present answers typically observe cryptographic techniques via way of means of disclosing statistics decryption keys best to legal users. However, in doing so, those answers unavoidably introduce a heavy computation overhead at the records proprietor for key distribution and records control whilst fine-grained records get entry to manipulate is desired, and as a consequence do now no longer scale well. Our proposed scheme additionally has salient houses of user get entry to privilege confidentiality and consumer mystery key accountability. Extensive evaluation suggests that our proposed scheme is particularly green and provably steady beneathneath present security models.

The authors of[6] Attribute-primarily based totally encryption (ABE) has spread out a famous studies subject matter in cryptography during the last few years. It may be utilized in diverse circumstances, because it offers a bendy manner to behavior fine- grained records get entry to manipulate. Despite its fantastic blessings in records get entry to manipulate, present day ABE primarily based totally get entry to manipulate gadget can't fulfill the requirement properly while the gadget judges the get entry to conduct in line with characteristic comparison, such as “greater than x” or “less than x”, that are referred to as similar attributes in this paper. In this paper, based on a fixed of well-designed sub-attributes representing every similar attribute, we assemble a similar attribute-primarily based totally encryption scheme (CABE for short) to deal with the aforementioned problem. The novelty lies in that we offer an extra green production primarily based totally at the era and control of the sub-attributes with the belief of 0-encoding and1-encoding.

The authors of [7], Motivated through the recent explosion of interest around block chains, we study whether or not they make a good fit for the Internet of Things (IoT) sector. Block chains permit us to have a disbursed peer-to-peer network where non- trusting individuals can have interaction with every different without a trusted intermediary, in a verifiable way. We evaluation how this mechanism works and additionally check out clever contracts- scripts that are living at the block chain that permit for the automation of multi-step processes. We then circulate into the IoT domain, and describe how a block chain-IoT combination: 1) allows the sharing of offerings and assets main to the introduction of a market of offerings among gadgets and 2) lets in us to automate in a cryptographically verifiable way numerous existing, time-ingesting workflows.

II. RESEARCH METHODOLOGY

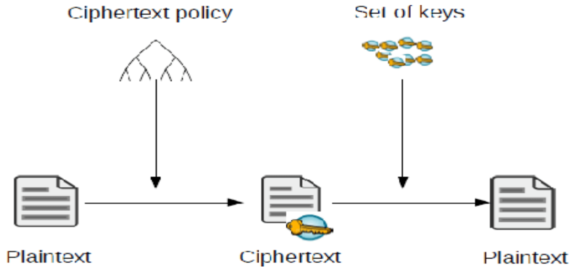
We present a methodology called Secure Sharing of PHRs in the Cloud (SeSPHR) to administer the PHR access control mechanism managed by patients themselves. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. Generally, there are two types of PHR users in the proposed approach, namely: (a) the patients or PHR owners and(b)the users of the PHRs other than the owners, such as the family members or friends of patients, doctors and physicians, health insurance companies’ representatives, pharmacists, and researchers. The patients as the owners of the PHRs are permitted to upload the encrypted PHRs on the cloud by selectively granting the access to users over different portions of the PHRs. Each member of the group of users of later type is granted access to the PHRs by the PHR owners to a certain level depending upon the role of the user. The levels of access granted to various categories of users are de-fined in the Access Control List (ACL) by the PHR owner. For example, the family members or friends of the patients may be given full access over the PHRs by the owner. Similarly, the representatives of the insurance company may only be able to access the portions of PHRs containing information about the health insurance claims while the other confidential medical information, such as medical history of the patient is restricted for such users.



III. METHODOLOGIES USED

A. Cipher Text Attribute Based Encryption

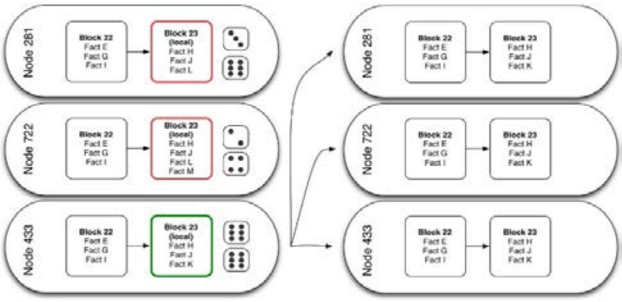
Attribute-based encoding can also be a kind of public-key cryptography amongst that the key of a user and moreover the cipher text square measure established upon attributes (e.g. the country where in he lives, or the sort of subscription he has). In any such system, the secret writing of a cipher text is viable imparting the set of attributes of the user key suits the attributes of the cipher text. There square measure primarily two sorts of attribute-based cryptography schemes: Key policy attribute-based cryptography (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE).



B. Block Chain Technology

A block chain, originally block chain, is a growing list of records, referred to as blocks, which can be related the usage of cryptography. Each block carries a cryptographic hash of the preceding block, a timestamp, and transaction information (typically represented as a merkle tree root hash). By design, a block chain is proof against modification of the information. It is "an open, dispensed ledger which could document transactions among events effectively and in a verifiable and everlasting way". For useasa dispensed ledger, a block chain is usually controlled through a peer-to-peer network together adhering to a protocol for inter-node comm. unique and validating new blocks. Once recorded, the information in any given block cannot be altered retroactively without alteration of all next blocks, which calls for consensus of the network majority. Although block chain records aren't unalterable, block chains can be taken into consideration steady through design and exemplify a dispensed computing system with excessive Byzantine fault tolerance.

Decentralized consensus has consequently been claimed with a block chain.



C. Token Generation System

Computer cryptography makes use of integers for keys. In a few instances keys are randomly generated using a random number generator (RNG) or pseudorandom number generator (PRNG). A PRNG is a computer algorithm that produces data that looks random below analysis. PRNGs that use system entropy to seed data usually produce higher results, due to the fact that this makes the preliminary situations of the PRNG a lot greater tough for an attacker to guess. Another manner to generate randomness is to make use of information outside the system. VeraCrypt(a disk encryption software) makes use of user mouse moves to generate specific seeds, wherein users are endorsed to move their mouse sporadically. In different situations, the key is derived deterministically the usage of a passphrase and a key derivation function.

D. Advanced Encryption Standard algorithm (AES)

The AES algorithm makes use of a substitution-permutation, or SP network, with more than one rounds to provide cipher text. The number of rounds relies upon on the key length being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds. Each of those rounds calls for a round key, however when you consider that simplest one key is inputted into the algorithm, this key desires to be extended to get keys for every round, together with round 0.

IV. RESULTS ANDTESTING

Name of the test	Integration Of all Unit Testing
Test Description	File Upload, Key generation, Encryption & Decryption.
Sample Input	File
Expected Output	Successful operations
Actual result/Remarks	As expected.
Passed (?)	Successful

Table: Integration Of all Unit Testing

Unit Testing of System, Integration Testing of System, Functional Testing of system, System Testing, White-Box Testing of System, Black-Box Testing of System, Acceptance Testing: all the trails said above passes effectively. No deformities experienced.

V. RESULTEVALUATION

Advantages of the Proposed System:

More Secured, ABE is fast in performance, application on cloud is more secured, proper access is shared through the token, resources not required, transaction is secured using block chain

VI. CONCLUSION

We have planned a secure and flexible attribute primarily based PHR sharing theme mistreatment cloud computing that satisfies the supposed security and privacy needs. To verify patient-centric PHR sharing, PHR owners have to have complete control of outsourced non-public PHR data Thus, it is important to save PHR records in an encrypted format in third-party cloud platforms. As soon as the PHR data square measure keep in an encrypted format, attaining fine-grained get entry to is kind of difficult. Most extremely good existing cloud primarily based PHR schemes have used ABE schemes to modify fine grained PHR access.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, no. 1, pp. 69–73,2017.

[2] L.HarnandJ.Ren,“ Generalized digital certificate for user authenti-cation and key establishment for secure communications,” IEEE Trans-actions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379,2017.

[3] Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 2015, 18,2084–2123.

[4] Aitzhan, N.Z.; Davor, S. Security and Privacy in Decentralized Energy Trading through Multi- signatures, Block chain and Anonymous Messaging Streams. IEEE Trans. Dependable Secur. Comput. 2016,99.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in The 29th IEEE International Conference on Computer Communications (IEEE INFOCOM 2010). IEEE, 2010, pp.1–9.

[6] K.Xue,J.Hong,Y.Xue,D.S.Wei,N.Yu,andP. Hong, “CABE: A new comparable at tribute-based encryption construction with 0-encoding and 1- encoding,” IEEE Transactions on Computers,vol. 66, no. 9, pp. 1491–1503,2017.

[7] Christidis, K.; Michael, D. Block chains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4,2292–2303.

[8] Analyzing the performance of a block chain-based personal health record implementation Alex Roehrs, Cristiano Andréda Costa, Rodrigoda Rosa Righia,Valter Ferreirada Silva,José Roberto Goldim,DouglasC.Schmidt.

[9] Generating design knowledge for block chain- based access control to personal health records Pascal Meier,Jan Heinrich Beinke,Christian Fitte, Jan Schulte to Brinke & Frank Teuteberg Information Systems and e-Business Management volume 19, pages13–41(2021).

[10]An Architecture and Management Platform for Block chain-Based Personal Health Record Exchange: Development and Usability Study An Architecture and Management Platform for Block chain-Based Personal Health Record Exchange: Development and Usability Study Authors of this article: Hsiu-An Lee 1, 2, 3, 4, 5 Author Orcid Image ; Hsin- Hua Kung 2, 3, 4, 5 Author Orcid Image ; Jai Ganesh Udayasankaran 3, 4, 6 Author Orcid Image; Boonchai Kijsanayotin 3, 4, 7 Author Orcid Image ; Alvin B Marcelo 3, 4, 8 Author Orcid Image ; Louis R Chao 1 Author Orcid Image ; Chien-Yeh Hsu 2, 3, 4, 5, 9.

[11]PHR System using Block chain Technology December 2019International Journal of Advanced Trends in Computer Science and Engineering 8(6):3188-3193 from Sang Young Lee.

[12]Block chain Technology in Healthcare: A Comprehensive Review and Directions for Future Research by SeyednimaKhezr1, MdMoniruzzaman 1,Abdulsalam Yassine 2 and RachidBenlamri2.

[13]Electronic health records in a Block chain: A systematic review André Henrique Mayer, Cristiano Andréda Costa, Rodrigoda Rosa Righi.