IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Based Safe Electronic Medical Records

Priyanka Jaiswal[a], Dr. Sudhir Agarwal(HOD)[b]

[a]*BIT, Gorakhpur, Uttar Pradesh* [b]*BIT, Gorakhpur, Uttar Pradesh*

Keywords:

Blockchain, Electronic health records, Attribute based signature.

Corresponding author:

Dr. Sudhir Agarwal(HOD)

[a]*BIT, Gorakhpur, Uttar Pradesh*

E-mail: sagarwal22@gmail.com

ABSTRACT

Electronic health records (EHRs) are only handled by hospitals and not patients, rendering medical advice in several hospitals more difficult. Patients ought to rely on their own healthcare information and restore their own patient records control. The exponential advancement of blockchain technologies facilitates wellness for the General population, medical records and patient knowledge included. This technology provides treatment professionals and websites patients with detailed and unchanging details and access to EHRs free of charge. In this article, we introduce an attribute-based signature scheme with several authorities to ensure that the blockchain-encapsulated EHRs are legitimate, where a patient endorses an attribute message and does not share details other than the proof he has attested to them. In addition, many authorities may manufacture and spread public / private keys of a patient without a trustworthy single or central mechanism, thereby avoiding the issue of escrow and adhering to the blockchain distributed data management mode. By swapping the hidden pseudorandom feature seeds between the authorities, the protocol resists N-1 deceptive authorities to attack conspiracies. We also formally show that this attribute-based signature approach is protected in a random oracle paradigm by imperfection and absolute privacy in the presumptions of bilinear Diffie-Hellman. The association indicates the effectiveness and properties of the methods proposed in other studies.

1. INTRODUCTION

Healthcare provides medical record archiving services that promote traditional medical records of paper patients for electronic access to the web. The system is designed to help patients control the creation and management of electronic medical records with family, friends, healthcare professionals and other consumers of official data. Additionally, if a healthcare researcher and these service providers are entering these EHRs worldwide, the healthcare transformation program must be completed. However, in the current scenario, patients disperse their EHR in diverse areas of life events, moving the EHR from one database of service providers to another. As a consequence, the consumer will lose tolerance to traditional clinical data while the service provider continues primary administration. Patients have restricted access to EHR and these details cannot be readily exchanged with researchers or suppliers. Interaction trials among diverse suppliers, hospitals and research institutes. Add additional barriers to sharing better-performance data. Without synchronized organization and data transfer, medical records are more fragmented than stable.

During encryption, patient information is securely encrypted and stored in the specified registry. The private key and the public key will generate the keys. With the private key, the patient will be capable to access his particular registry column and, when accessing the registry, the EHR will be decoded using a decryption algorithm and a private key. The main goal of the project is to use the blockchain concept so that multiple selected EHR columns can be encrypted and decrypted. Hospitalized patients are identified and treated and these diagnoses and treatments are documented for future use in the hospital's electronic medical record (EHR) system. This registration must be protected by third parties at all costs. The key aim of the project is data encryption and decryption of patients using DES and AES electronically. The system will be safe if only the authorized person has the private key required to download the encrypted patient data. The system does not provide any security when an unauthorized user knows the private key.

2. LITERATURE SURVEY

1. Survey on "Escrow Free Attribute-Based Signature with Self-Revealability":

A significant drawback of rudimentary cryptographic functionality is that a private user key is generated by an AA on behalf of this user to sign or decrypt messages. In this connection, we use the key extraction protocol to substitute the ATBS key generation algorithm, in which the Key Generation Center (KGC) does not produce an attribute-dependent private key in the name of a legal individual instead of the current technique to mitigate the key scrow issue for several AAs. Furthermore, if the ABS signer considers it difficult (if necessary) for a signer to give the verifier proof of a signature produced by a user under the signing key, especially if the user knows only his private key, we attach a signer disclosure protocol to our ABS system to enable a user to affirm or deny his/her identity. In addition, we describe a formal model for the construction of the ABS system known as scrow-free ABS and the provision of concrete buildings that are self-revealing.

2. Survey on "Multi-authority Attribute-Based Signature"

ABS is a new primitive cryptographic function where a symbol with its attributes will sign a message and the checker can only state whether the signator has attributes that conform to his policy. ABS is a cryptographic function that is primitive. In addition, no person with characteristics that do not comply with the regulation can counterfeit a signature. ABS presents a range of applications, such as anonymous mechanisms of identification and sharing of attributes. These systems can, however, enable a user to obtain attributes from multiple authorities involving a multi-authority ABS scheme. In comparison, in place of a particular attribute authority, such authorities can delegate trust to all authorities. This paper proposes a multi-agency system of ABS that incorporates complex processes, criteria of AND, OR and threshold. To ensure that a client receives attribute keys from distinct authorities, we use a central authority. To prevent partnership attacks so that a user combines his attribute keys and identities, we follow a single global identity (GID). And a hidden key from the central authority enables the identification of the person to be affirmed. Therefore, our system will satisfy the specifications of true applications and therefore transmit trust to any machine authority.

3. Survey on "Blockchain-based System for Secure Data Storage with Private Keyword Search "

Traditional cloud computing relies almost entirely on massive storage networks that, like trusted third parties, transfer and maintain data. A variety of hurdles emerge from this paradigm, including access to data, high operating costs and data protection. In this paper, we suggest a framework that uses blockchain technologies to provide keyword search services with secure distributed data storage. The application enables the user to use encryption technology to upload their data in encrypted form, distribute data knowledge into cloud nodes, and preserve data access. It also provides the data owner with the right to search for anyone's details. Via the safe dataset, the frame enables private keyword searches.

4. Survey on "A New Approach to Threshold Attribute Based Signatures"

Improvements in threshold-based signatures have recently been created, powered by improvements in attribute-based encryption and signature (t-ABS). We suggest a new way of producing ring-influenced threshold signatures in this work. Threshold-dependent attribute, centered on a (t, n total) threshold, guarantees that the signing company retains at least t in a number of n è l attributes for the audit. Another way to do this is that, as a combination of attributes, the signer has at least 1 of n x t. A new t-ABS solution is then to allow a signatory from each conceived n-to-t package to choose any n 0 sets of t attributes and to show that he(s) has at least one n 0.0. For this approach, we have a multi-faceted ABS threshold system. We also indicate that our system is secured at random.

5. Survey on "Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model"

This paper presents a fully-protected (adaptive-pronounceable and private) ATR system (ABS) in the standard model. In the regular projections, the decisional linear (DLIN) inference and the presence of collision-resistant (CR) hazh functions, the protection of the suggested ABS Scheme is seen. In other words, a generalized non-monotone predicate that can be represented by NOT, AND, OR and Threshold Gates was adopted by the new ABS system, although the current ABS schemes only support monotone predicates. The proposed ABS architecture is as powerful as one of the most common (several times worse) ABS structures in the generic community model and has been shown to be stable.

3. PROPOSED METHODOLOGY

MODULES:

EHRs Server:

The EHR server is the same as a cloud computing server that stores and transmits EHRs.

Authorities:

N agencies comprise of different organizations that identify and exchange patient information, such as clinics, health care companies, medical research institutes, etc.

Patient and Data Verifier:

Patients can build, monitor, control, sign and identify their own EHRs, while data verificators can access and validate the accuracy of this signature.

Application needs Non-Functional Requisites

Expanded System admin security: Oversight to prevent PC violence should be incredibly safe and accessible.

Compactness: The presentation of this program is easy to use, such that the consumer can understand and respond to the identical equivalent.

Unwavering quality: And the features available in this sub-implementation structure's is very likely to convey the necessary inquiries to us.

Time take for Reaction: It is very easy to take the time needed by the order to finish a business given by the customer.

Multifariousness: Our functionality may be generalized to include the benefits of software that is already available to maximize the product's performance. This is suggested implicitly in the upcoming work on the proposal.

Vigor: The project is respectful to responsibility for unauthorized customer/beneficiary data outlets. Blunder controls were performed on the platforms to avoid deception of platforms.

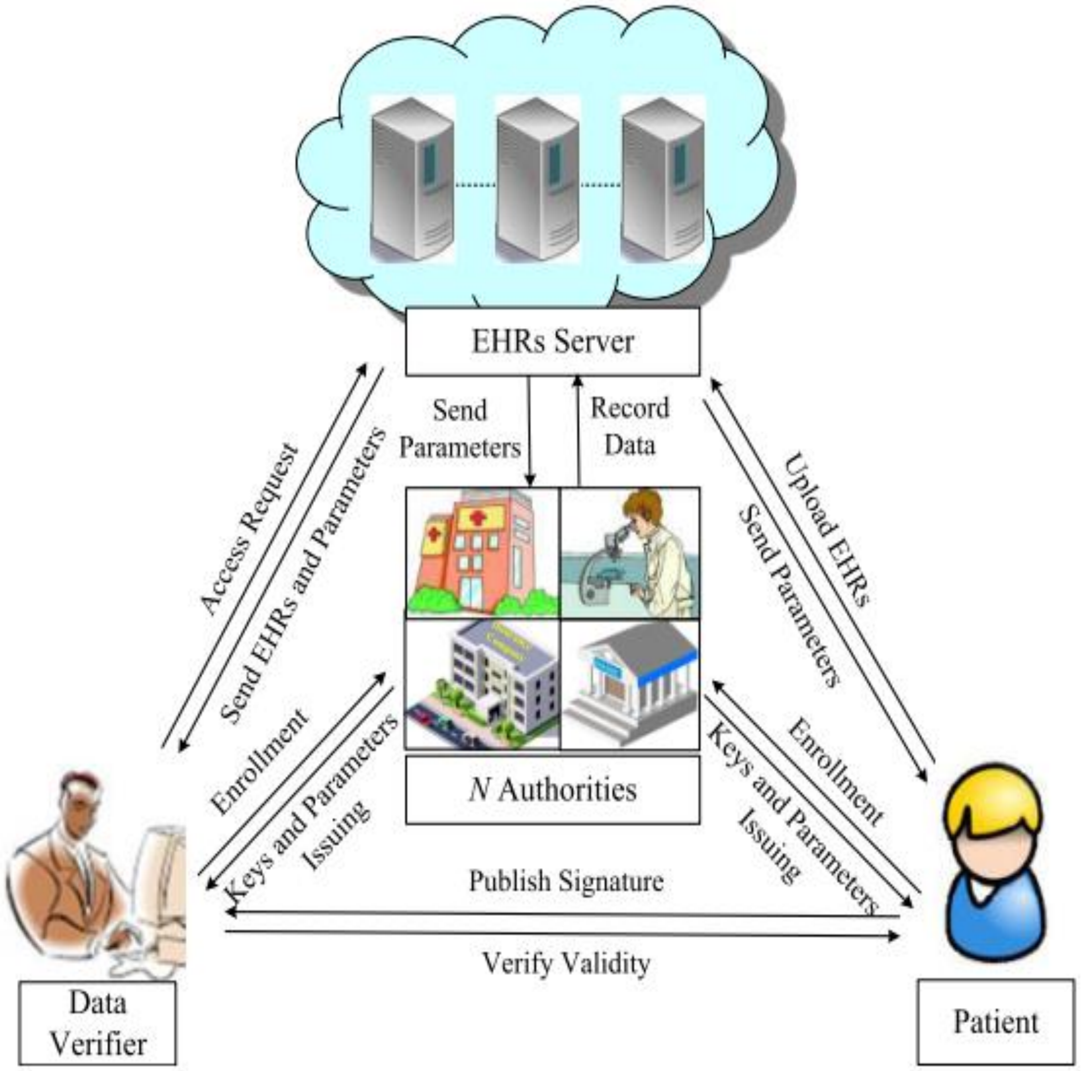
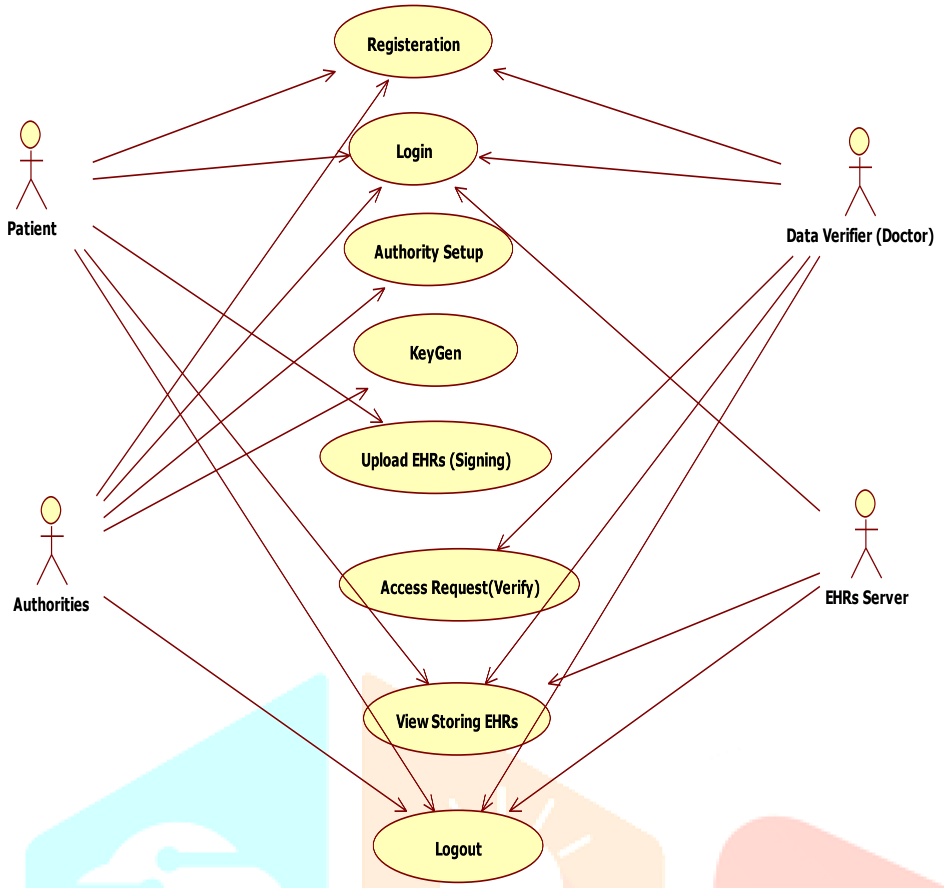


Fig.1. Project Architecture diagram

4. SYSTEM DESIGN

Description:

Star (UML) may be a kind of static framework architecture that delineates the structure of a system by showing its resources, attributes, operations and even grouping relationships. A class plot in the Hierarchical Modeling Language used in our Project Creation. It states that the class includes data.



Our Total Application on Use Case

Fig.2. Project User Case

Description:

Star (UML) can be a type of behavioral map that is displayed and created within the Cohesive Modeling Vocabulary we used in our Project Development using a use-case analysis. It is influenced by the graphical visualization of the mind offered by a system by the degree to which experts function, their aims (addressed as use cases) and any criteria are present. The most popular reason behind a case diagram is to illustrate the structural limitations of the character in the display. Sections of the entertainers are seen in the framework.

User Sequence:

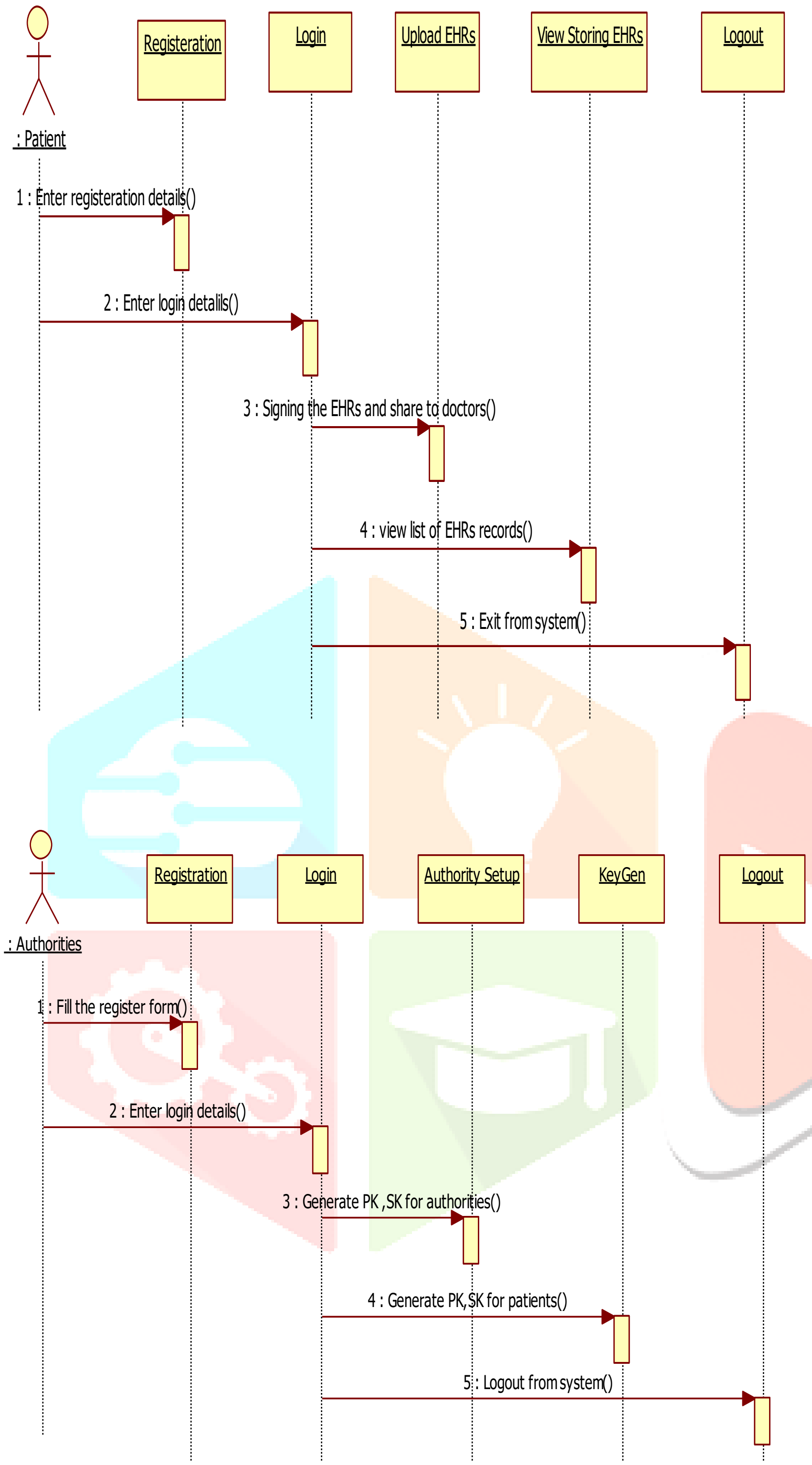

: Patient
Registeration
Login
Upload EHRs
View Storing EHRs
Logout
1 : Enter registeration details()
2 : Enter login details()
3 : Signing the EHRs and share to doctors()
4 : view list of EHRs records()
5 : Exit from system()
: Authorities
Registration
Login
Authority Setup
KeyGen
Logout
1 : Fill the register form()
2 : Enter login details()
3 : Generate PK ,SK for authorities()
4 : Generate PK,SK for patients()
5 : Logout from system()

Fig.3. Project User Sequence

Description:

The Star (UML) gathering schema in our Centralized Modeling Language may be a sensible association chart, but frames function together and demonstrate in what master mind. It's a message sequence map formation. Progress maps are also classified as case charts, situation dynamics and short-term approaches.

5. CONCLUSION

In order to protect patient anonymity in an EHR framework on blockchain, many authorities have been adopted and built into ABS an MAABS scheme that satisfies the specifications of the blockchain mechanism and guarantees that knowledge is confidential and immutable. PRF seeds are needed by the authorities, patient private keys must be mounted, N-1 compromised authorities may not succeed in collusion attacks. The security of the protocol is eventually proved in terms of unforgiveness and perfect protection under the CBDH presumption. The comparison study reveals that the protocol's efficiency and expense improves simultaneously with the amount of administrations and patient characteristics. Many distributed machine implementations may use a non-monotone predicate, which improves the representation of the predicate. The direction of potential work in blockchain technologies is to embrace general non-monotonic predicates.

REFERENCES

[1] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). Who Owns Medical Records: 50 State Comparison.[Online]. Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medicalrecords-50-state-comparisonVOLUME 6, 2018 11685R. Guo et al.: Secure ABS Scheme With Multiple Authorities for Blockchain in EHRs

[2] K.D.Mandl,P.Szolovits,andI.S.Kohane,‘‘Publicstandardsandpatients’ control: How to keep electronic medical records accessible but private,’’ BMJ, vol. 322, no. 7281, pp. 283–287, Feb. 2001.

[3] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] World Economic Forum. (Sep. 9, 2015). Deep Shift: Technology Tipping Points and Societal Impact. [Online]. Available: http://www3.weforum. org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[5] (Dec. 12, 2016). Healthcare Rallies for Blockchains: Keeping Patients at the Center. [Online]. Available: http://www.ibm.biz/blockchainhealth

[6] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O’Reilly Media, 2015, pp. 53–68.

[7] G.Prisco.(Apr.26,2016).TheBlockchainforHealthcare:GemLaunches Gem Health Network With Philips Blockchain Lab. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gemlaunches-gem-health-network-with-philips-blockchain-lab-1461674938

[8] U.S. White House. 104th Congress. (Aug. 21, 1996). Public Health Insurance Portability and Accountability Act.[Online]. Available: https://en. wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_ Act

[9] P. Taylor. (Apr. 27, 2016). Applying Blockchain Technology to Medicine Traceability.[Online]. Available: https://www.securingindustry. com/pharmaceuticals/applying-blockchain-technology-to-medicinetraceability/s40/a2766/#.V5mxL_mLTIV

[10] P. B. Nichol. (Mar. 17, 2016). Blockchain Applications for Healthcare: Blockchain Opportunities are Changing Healthcare Globally-Innovative Leaders See the Change. [Online].Available: http://www.cio.com/article/3042603/innovation/blockchain-applicationsfor-healthcare.html

[11] G. Irving and J. Holden, ‘‘How blockchain-timestamped protocols could improve the trustworthiness of medical science,’’ F1000Research, vol. 5, p. 222, May 2016.

[12] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, ‘‘Searchain: Blockchainbased private keyword search in decentralized storage,’’ Future Generat. Comput. Syst., 2017, doi: 10.1016/j.future.2017.08.036.

[13] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, ‘‘Medical JPEG image steganography based on preserving inter-block dependencies,’’ Comput. Electr. Eng., 2017, doi: 10.1016/j.compeleceng.2017.08.020.

[14] H. K. Maji, M. Prabhakaran, and M. Rosulek, ‘‘Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,’’ in Proc. IACR Cryptol. ePrint Arch., Apr. 2008, pp. 1–23. [Online]. Available: https://eprint.iacr.org/2008/328.pdf

[15] A. Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in Proc. EUROCRYPT, Aarhus, Denmark, 2005, pp. 457–473.

[16] D. Khader, ‘‘Attribute based group signature with revocation,’’ in Proc. IACR Cryptol. ePrint Arch., Jun. 2007, pp. 1–19. [Online]. Available: https://eprint.iacr.org/2007/241.pdf