International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

ELECTRONIC HEALTH RECORDS

Pooja B[1], Aishwarya C[1], Divyashree S[1], Srinidhi Kulkarni[2]

[1]Dept of Computer Science and Engineering, Jyothy Institute of Technology, Bangalore, India
[2]Asst professor, Dept of Computer Science and Engineering, Jyothy Institute of Technology, Bangalore, India

---

Abstract - *Electronic health records (EHRs) are altogether constrained by medical clinics rather than patients, which confuses looking for therapeutic advice from various medical clinics. Patients face a basic need to concentrate on the subtleties of their own social insurance and re-establish the board of their own medicinal information. The quick improvement of blockchain innovation advances populace social insurance, including medicinal records as well as patient-related information. This innovation furnishes patients with exhaustive, permanent records, and access to EHRs free from specialist organizations what's more, treatment sites. In this paper, to ensure the legitimacy of EHRs epitomized in the blockchain, we present a property-based mark conspire with numerous experts, in which a patient underwrites a message as indicated by the quality while revealing no data other than the proof that he has validated 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.*

Key Words: Blockchain, ABS,

1. INTRODUCTION

1.1 Introduction to Blockchain

The blockchain is a growing list of records, called blocks, which are linked using cryptography. A cryptographic hash of the previous block, timestamp, and transaction data constitute to a single block. A blockchain is decentralized, conveyed and open computerized record that is utilized to record exchanges crosswise over numerous pcs so the record can't be modified retroactively without the adjustment of every ensuing square and the agreement of the system.

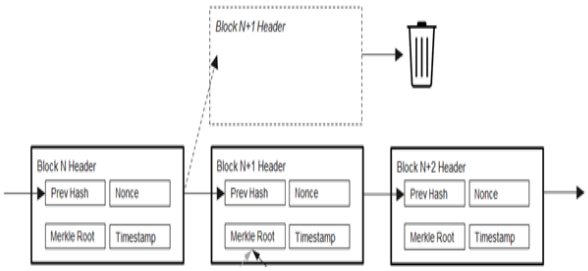

Fig -1: Structure of Blockchain

This enables the members to confirm and review exchanges in lavishly. A blockchain database is overseen self-sufficiently utilizing a shared system and a disseminated time stepping server. They are confirmed by mass coordinated effort controlled by aggregate personal matters. The outcome is a vigorous work process where members' vulnerability in regards to information security is negligible. The utilization of a blockchain evacuates the normal for unbounded reproducibility from an advanced resource. It affirms that every unit of significant worth was exchanged just once, taking care of the long-standing issue of twofold spending. Blockchain has been depicted as an esteem trade convention. This blockchain-based trade of significant worth can be finished snappier, more secure and less expensive than with conventional frameworks a blockchain can relegate title rights since when appropriately set up to detail the trade assertion, it gives a record that forces offer and acknowledgment

1.2 Introduction to Electronic Health Records

Electronic health records (EHRs) give an advantageous wellbeing record stockpiling administration, which advances customary patient medicinal records on paper to be electronically open on the web. This framework was intended to enable patients to have the control of creating, overseeing and sharing EHRs with family, companions, medicinal services suppliers, and other approved information shoppers. Besides, gave that the medicinal services specialist and suppliers of such administration get to these EHRs over the on board, the change program of social insurance arrangement is relied upon to be accomplished. However, in the present circumstance, patients dissipate their EHRs over the distinctive territories amid life occasions, making the EHRs move from one specialist co-op database to another. Along these lines, the patient may lose control of the current human services information, while the specialist organization typically keeps up the essential stewardship. Persistent get to consents to EHRs are very restricted, and patients are normally helpless to effectively share this information with scientists or suppliers. Interoperability challenges between various suppliers, clinics, investigate establishments, and so on include additional boundaries to elite information sharing. Without composed information the executives and trade, the wellbeing records are divided rather than strong. On the off chance that the quiet has the ability to oversee and sharing his EHRs safely and totally, as appeared in fig. 1, paying little mind to the inquiry about reason or the information sharing among human services suppliers, the social insurance

industry will profit enormously. Drawing support from blockchain technology, the proposed method accomplishes this goal to promote cooperation in the way of deep mutual trust between each organization.

Blockchain innovation was earlier produced for the cryptographic money bitcoin furthermore, was first displayed in the bit-coin whitepaper by Nakamoto in 2008. Since blockchain innovation showed up, it has been praised as another innovative upset simply like the creation of the steam motor or the web as a result of its immense impaction on society. Beforehand, numerous limitations have been set on sharing enormous EHRs in view of the dangers to information security or spillage of private patient data amid information trade. Furthermore, current EHRs are Blockchain innovation was earlier produced for the cryptographic money bitcoin furthermore, was first displayed in the bit-coin whitepaper by Nakamoto in 2008. Since blockchain innovation showed up, it has been praised as another innovative upset simply like the creation of the steam motor or the web as a result of its immense impaction on society. Beforehand, numerous limitations have been set on sharing enormous EHRs in view of the dangers to information security or spillage of private patient data amid information trade. Furthermore, current EHRs are managed by hospitals and providers, whereas patients are deprived of the right to freely control their own EHRs. Through utilizing blockchain technology, standards for recording data and managing identity are established, and the blockchain of EHRs is constructed. In addition, this technology records the auditing traces of all transactions in an immutable distributed ledger, which guarantees responsibility and transparency in the procession of data exchange. Therefore, the patient has the ability to record healthcare and diagnostic information from doctors in their own EHRs, thus reducing the number of medical accidents and preserving patient privacy.

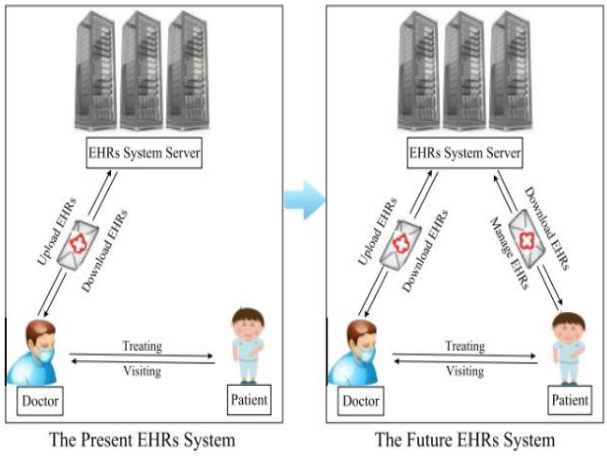

Fig – 2: Ehrs system in the present and future. The patient should have right to access his ehrs for managing and sharing them independently.

2. LITERATURE SURVEY

2.1 Attribute-based signatures: achieving attribute-privacy and collusion-resistance

Attribute-based signature (abs) is a latest and versatile cryptographic primitive. The signature is linked with the attributes of the users instead of the identity of the user.

Abs offers:

- A solid unforgeability ensures for the verifier, that the mark was created by a solitary gathering whose traits fulfill the case being made; i.e., not by an agreement of people who pooled their properties together.

- Solid security ensures for the endorser, that the mark uncovers nothing about the personality or characteristics of the underwriter past what is expressly uncovered by the case being made. Formally the security prerequisites of abs were characterized as a cryptographic crude, and after that portray a productive abs development dependent on gatherings with bilinear pairings. We demonstrate that our development is secure in the nonexclusive gathering model. At long last, we outline a few utilizations attribute-based signature (abs) is a latest and versatile cryptographic primitive. The signature is linked with the attributes of the users instead of the identity of the user. Abs offers: • a solid unforgeability ensures for the verifier, that the mark was created by a solitary gathering whose traits fulfill the case being made; i.e., not by an agreement of people who pooled their properties together. • Solid security ensures for the endorser, that the mark uncovers nothing about the personality or characteristics of the underwriter past what is expressly uncovered by the case being made. Formally the security prerequisites of abs were characterized as a cryptographic crude, and after that portray a productive abs development dependent on gatherings with bilinear pairings. We demonstrate that our development is secure in the non-exclusive gathering model. At long last, we outline a few utilization of this new device; specifically, abs fills a basic security necessity in quality based informing (ABM) systems.[1] the multi-authority setting is a special feature in which users can claim their own combination of attributes issued by independent and mutually distrusting authorities. Attribute-based systems depend on the combination of attributes respective users possess. In such systems, the users obtain multiple attributes from one or more attribute authorities, and a user's capabilities in the depend on their attributes. While offering several advantages, attribute-based systems also present fundamental cryptographic challenges. For instance, to provide end-to-end secure communication in an attribute-based messaging system, it must be possible to encrypt a message using attribute-keys (rather than individual users' keys). Recently cryptographic tools have emerged to tackle some of these challenges for encryption [2]. The sort of

verification required in a trait-based framework varies from that offered by computerized marks, similarly, open key encryption does not possess all the necessary qualities for property-based encryption. A property-based arrangement requires a more extravagant semantics, including security necessities, like later mark variations like gathering signatures [3], ring signatures [4], and mesh signatures [5].

2.2 Attribute-based group signature with revocation

In real life, every signature possesses specific attributes. Signature is necessary to meet certain criteria that are correspondent to attributes. Group signatures where any member of a team can be behalf for any another member of a team. For an instance, if Alice wants a signature from an employee of Bob's company and if the necessary person is absent, in any other person from the bob's company can sign in this way abgs works. In this scheme removal of a member from a group is enabled or removal of some of the user's attributes is possible. Previously [6], ABGS came into existence but it could not revoke. ABGS was introduced to include attributes in a group signature scheme [7].

2.3 Attribute-based signatures

ABS is an adaptable primitive that lets a user sign a message with keen control over identifying information. The signer who wishes to sign in abs must possess a set of attributes and must sign a message with a predicate that completely agrees with their attributes. Signature confirms the user consisting of attributes who satisfies all attributes is attested to message.

Attributes that identify information about signer is hidden by signature. Users using ring signatures cannot endorse message as it involves a large number of people and everyone are not known to users. Group signatures also cannot be used to endorse as people required by the user may not belong to the group. Mesh signatures also have many disadvantages to endorse. But ABS provide basic cryptographic challenges. The sort of validation required in a quality-based framework contrasts from that offered by digital signatures, similarly, public-key encryption does not possess all the necessary qualities for trait attribute-based encryption. A quality-based arrangement requires a more extravagant semantics, including namelessness prerequisites, like mark variations like group signatures, ring signatures, and mesh signatures. The regular topic in all these mark natives is that they give a certification of unforgettability and endorser namelessness. A substantial signature must be created in specific ways; however, the signature does not uncover any additional data about which of those ways was really used to create it. [8]

2.4 Study and performance analysis of RSA algorithm

Few applications require real-time security. Few applications which need security are complicated and deeply involve cryptographic concepts. RSA algorithm enhances security. Algorithm and key are two basic components required for encryption of data. An algorithm is generally known by everyone and the key is the secret component. RSA is an asymmetric key algorithm implying key used for encryption and key used for decryption are different. Keys are public key and private key. Public key can be shared with anyone but Private Key is a mystery. It's only known to authorized person.

RSA Encryption

In the RSA encryption scheme, the sender must obtain receivers public key pair to encrypt the message. The sender sends ciphertext to the receiver.

RSA Decryption

The private key of the receiver and modules computation is enough to decrypt the text [9].

3. PROPOSED SYSTEM

The blockchain is considered as another innovative upset that was presented. It is a shared appropriated record innovation to record exchanges, assertions, and deals. The advantages of the blockchain innovation are decentralized support, information sparing in the square the chain structure, secure transporting and getting to of information just as hostile to alter and evident information security. Exploiting these distinctive highlights above in an EHRs framework, blockchain empowers the administration of verification, classification, responsibility, and information sharing while at the same time taking care of data identified with security, medicinal asset sparing and encouraging for the patient, and making populace human services more astute. Expecting that there is an EHRs framework in a distributed storage stage, which comprises of a few divisions, for example, emergency clinics, pharmaceutical offices, protection offices, malady explore offices, etc, EHRs frameworks can be mutually overseen. All divisions can offer administrations for patients together and confine the privileges of every office to avert EHRs misuse. In this manner, an EHRs framework with a blockchain structure is planned. Assume that each patient possesses one blockchain of medicinal services alone. In the wake of being treated in a clinic, all the data including EHRs, utilization records, protection records, and so forth is epitomized in one square. Tolerant medicines at various occasions will be produced in various blocks. At that point, a progression of the block is created by the time grouping and a social insurance blockchain of this patient is built. The approved substance may investigate the wellbeing records of this patient by methods for his blockchain, and has feeble to alter the information in a setup square, (for example, medicate sensitivity and measurement). At the point when the patient goes to be treated in other clinical offices or emergency clinics next time, the new element needs to distinguish this patient and validate his accessible blockchain, which could

spare the medicinal assets and maintain a strategic distance from the rehashed recognition.

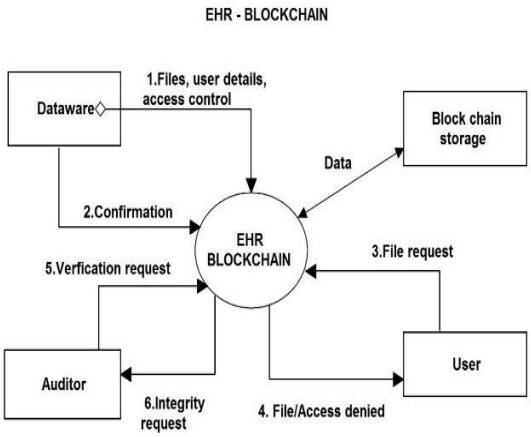

Fig – 3: Context Analysis

3.1 Favorable circumstances of the proposed system

• Providing precise, exceptional, and complete data about patients at the purpose of consideration

• Enabling speedy access to persistent records for increasingly organized, productive consideration

• Securely imparting electronic data to patients and different clinicians

• Helping suppliers all the more successfully analyze patients, diminish restorative blunders, and give more secure consideration

• Improving patient and supplier association and correspondence, just as social insurance accommodation

• Enabling more secure, progressively dependable recommending.

3.2 Block creation process

Step 1: Transaction data

Step 2: Chaining the blocks (with a hash)

Step 3: Hash is created using SHA-1

Step 4: The Block is created with a previous block hashtag

Step 5: Block Header is generated.

Step 6: Block is encrypted

Step 7: Block is compressed and stored.

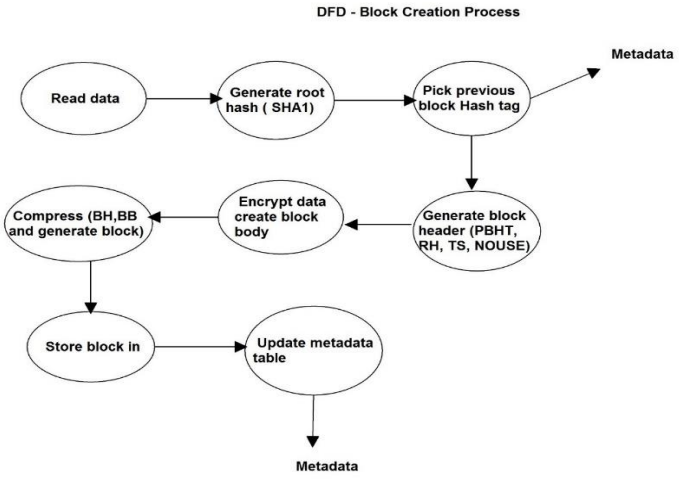

Fig – 4: Creation of Block

3.3 File download process

The user has to first select the file to be downloaded and keys must be inputted to gain the access. If keys are valid, access is granted else notifies the user to enter proper keys. If access is gained, block id and metadata are obtained from the file. Then the block is downloaded from the cloud and uncompressed as blocks are compressed and stored in the cloud. The uncompressed block is decrypted and the file gets downloaded in the user's system. Once the download is completed, a confirmation message gets displayed.

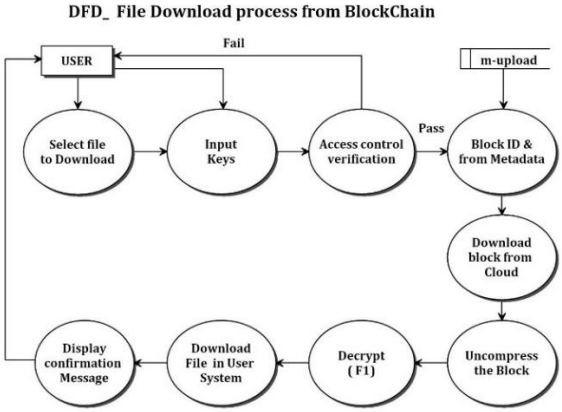

Fig - 5: File Download Process.

3.4 File corruption detection process

Block_ID is taken as input. With the help of block_ID block, content is obtained. Block content is unzipped and the root hash is calculated.as root hash is obtained details of the next block can be obtained. Therefore fetch the next block and extract previous hash code. If previous hash and root hash are the same, then the block is not corrupted.

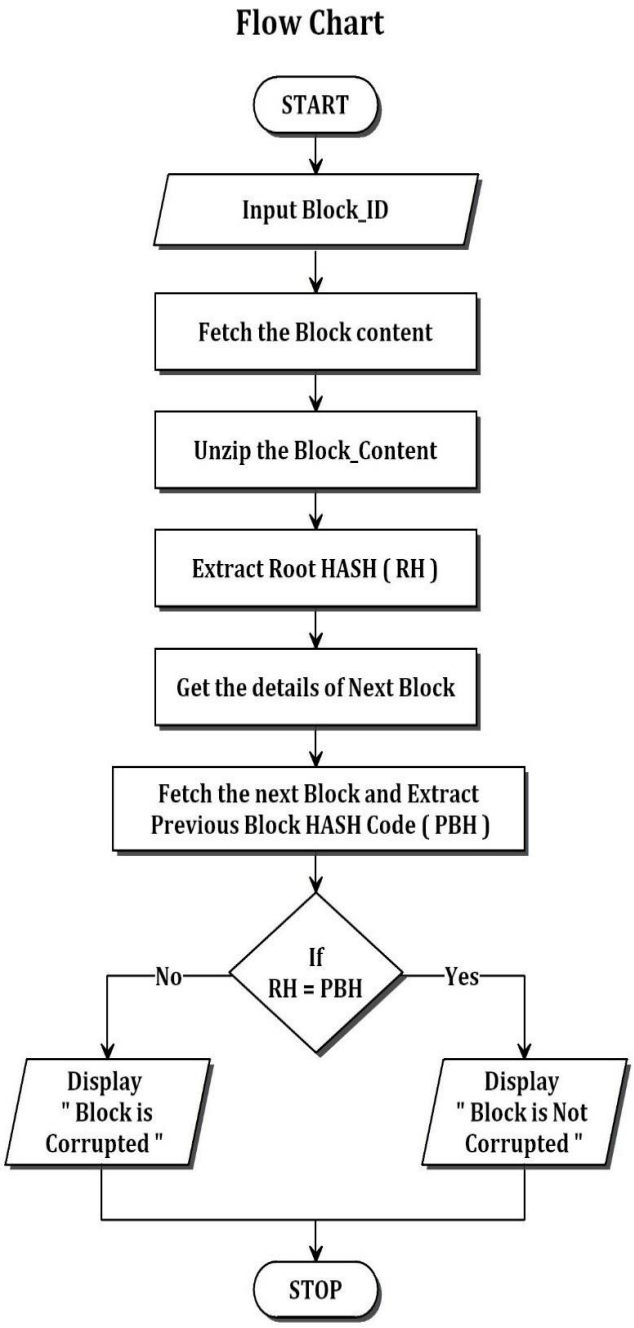

Fig – 6: Block Corruption Check Process

4. USERS IN EHRS

There can be 4 users in EHRs

a) Patient
b) Auditor
c) Data owner
d) Admin

5 SYSTEM DESIGN

5.1 Admin

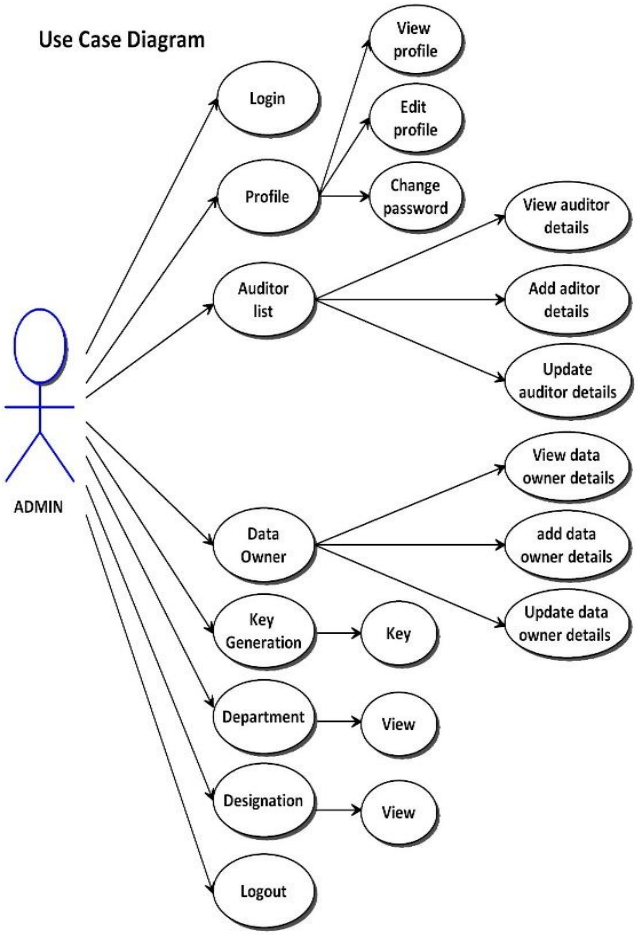

Fig – 7: Admin User Case

- Login
- Profile
  - View profile
  - Edit profile
  - Change password
- Auditor list
  - View auditor
  - Add auditor
  - Update auditor
- Data owner
  - View data owner
  - Add data owner
  - Update data owner
- Key generation
- Department(attribute i)
- Designation(attribute ii)
  - Logout

5.2 Data owner (doctor)

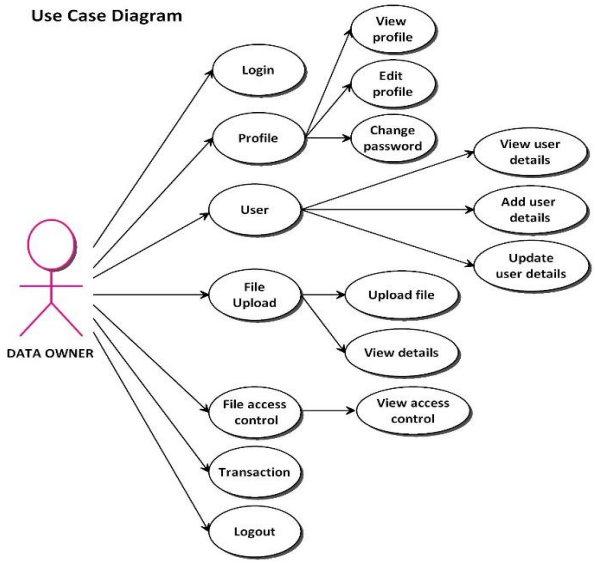

Fig – 8: Data Owner Use Cases

- Login
- Profile
  - View profile
  - Edit profile
  - Change password
- Users
  - View data owner
  - Add data owner
  - Update data owner
- File upload
  - Upload file

    While uploading a file, have to generate the hashtag, which we consider as current hashtag then have to take previous file current hashtag for this current file genius hashtag /previous hashtag and timestamp and nonce. A nonce is nothing random number generation.

Previous_hashtag+current hashtag+timestamp+nonce = concatenating these parameters have to generate the confidential key. This is the header part of the blockchain.

The file we are considering a body part which is giving body part of the blockchain concept. So, to secure this data our system is encrypting and merging the body and header part file and making the zip part like. Boo1.zip

Then store it in to cloud storage.

  - View details
- File access control
  Control file access control
  View file access control

  File access control data owner can set access control for multiple users.
- Transaction
- Layout

5.3 User (patient)

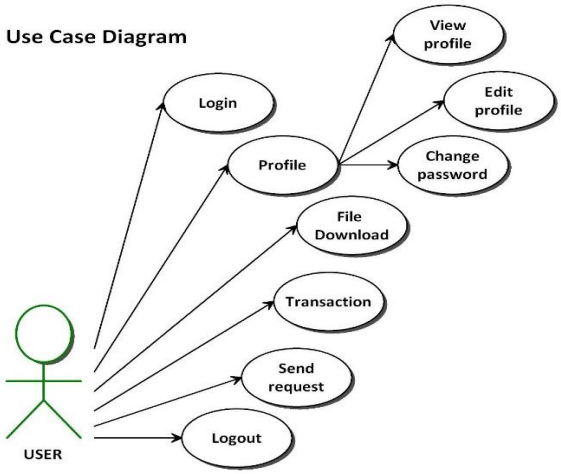

Fig – 9: Patient Use Cases

- Login
- Profile
  - View profile
  - Edit profile
  - Change password
- File download

  While downloading, based on file_id this system is picking the blocked of that specific file and using block id file has to downloaded from cloud then the file has to get unzip after unzip body file has to get decrypt and give it to the user.
- Transaction
- Send request
- Logout

5.4 Auditor

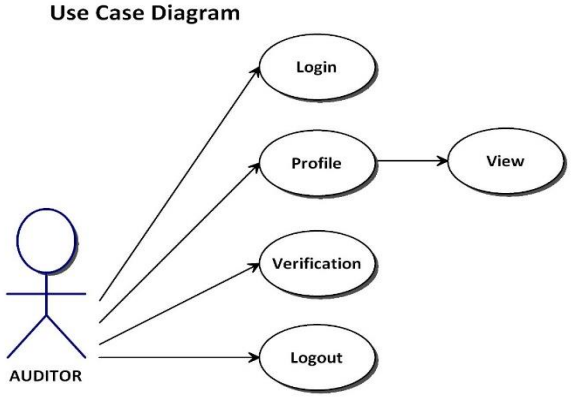

Fig – 10: Auditor Use Cases

- Profile
  - View profile
- Verification

  During verification the file has to get downloaded from cloud then has to get unzip after unzip using the confidential key the verification process will be happening and user getting the verification mail from auditor whether the file has been verified successful or modified
- Logout

6. CONCLUSION

Blockchain empowers the administration of verification, classification and information sharing while at the same time giving data identified with protection, therapeutic asset sparing and encouraging for the patient and making populace social insurance smarter. Taking the preferred standpoint of this method, it accomplishes ideal security saving for the patient.

REFERENCES

1. H. K. Maji, m. Prabhakaran, and m. Rosulek, "attribute-based signatures: achieving attribute-privacy and collision resistance," in Proc. Iacr cryptol. Eprint arch., apr. 2008, pp. 1–23. [online]. Available: https://eprint.iacr.org/2008/328.pdf

2. V. Goyal, o. Pandey, a. Sahai, and b. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In a. Juels, r. N. Wright, and s. D. C. Di vimercati, editors,acm conference on computer and communications security, pages 89–98. Acm, 2006.

3. D. Chaum and e. Van heyst. Group signatures. In eurocrypt, pages 257– 265, 1991.

4. R. L. Rivest, a. Shamir, and y. Tauman. How to leak a secret. In c. Boyd, editor, asi-acrypt, volume 2248 of lecture notes in computer science, pages 552– 565. Springer, 2001.

5. X. Boyen. Mesh signatures. In m. Naor, editor, eurocrypt, volume 4515 of lecture notes in computer science, pages 210–227. Springer, 2007.

6. D. Khader. Attribute based group signature scheme. Cryptology eprint archive, report 2007/159, 2007. Http://eprint.iacr.org/.

7. 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

8. H. K. Maji, m. Prabhakaran, and m. Rosulek, "attribute-based signatures," in proc. Ct-rsa, san francisco, ca, usa, 2011, pp. 376–392.

9. M. Preetha, m. Nithya," a study and performance analysis of RSA algorithm", in ijcsmc, vol. 2, issue. 6, June 2013, pg.126 – 139. Available: https://www.ijcsmc.com/docs/papers/june2013/v2i6201330.pdf