iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5148

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Secure Attributes with Several Authorities for Blockchain in Electronic Health Reports

Lakshmi E S[1], Sugato Chakrabarty[2]
[1]*M. Tech,* [2]*Professor, Computer Science, CMR Institute of Technology, Bengaluru*

Abstract: ***Electronic Health Records are entirely controlled by hospitals rather than patients, which complicates the seeking medical advice from different hospitals. Patients face a problem when they need to focus on the details of their own health care and restore the management of their own medical data. The fast development of Blockchain technology promotes population attention, together with medical records furthermore as patient-related data. This technology provides patients with complete and immutable records and the access to EHRs free from service suppliers and treatment websites. The aim is to ensure the validity of encapsulated EHRs in the Blockchain, we present an attribute-based signature schema with multiple authorities, in which a patient endorses a message based on the attribute by not disclosing any information other than evidence that he testified. In addition, there are multiple authorities with no single or central generate and distribute public / private keys of the patient, which avoids the problem of blocking and complies with the mode of distributed knowledge storage of data in the Blockchain. By sharing the secret seeds of the pseudo-random function among the multiple authorities, this protocol resists a collusion attack out of N of N-1 corrupted authorities. Under the assumption of the machine additive Diffie-Hellman, we also formally demonstrate that, in terms of the accountability and perfect confidentiality of the signatory of the attribute, this attribute-based signature scheme is secure the random oracle pattern. The comparison shows the effectiveness and properties between the planned technique and strategies planned in different studies.***

Keywords: Block-Chain, Electronic Health Reports (EHRs), RSA algorithm, DES Encryption and Decryption.

I. INTRODUCTION

A. Overview

Electronic Health Reports (EHR) is a convenient health report repository service that allows traditional paper-based medical reports to be digitally accessible on the website.

This system was constructed to grant patient to monitor, generate, manage and share reports with their family, colleague, health-care providers and new authorized users. In addition, the health analyst and the provider of these services have access to these health reports, the health care solution transition plan should be implemented. However, in ongoing condition, victim disperse their electronic reports in various field during their lives, moving them from one maintenance provider database to other. As a result, the victim may give up control of actual health care information, while the maintenance provider typically provides essential management.

Patient connection to electronic reports is very finite and victim are generally unable to freely share this data with analyst or providers. Interoperability issues between various suppliers, hospitals, and analysis institutes, so on add extra barriers to high-achievement data distribution.

B. Existing System

In the existing rule, the victim may drop control of current health care information, although the maintenance provider typically produce initial management. Patient approach to health reports is very finite and victims are usually unable to freely share this information with analyst or providers. Interoperability issues between various suppliers, hospitals, analysis institutes, so on. Add extra barriers to high-achievement data distribution. Without integrated data administration and transfer, medical reports are disintegrated rather than consistent.

1) Disadvantages

a) Patient approach to digital reports is very finite and victims are generally unable to freely transfer this information with analyst or providers

b) Objection of interoperability between various suppliers, hospitals, analyst etc.

c) Less security.

C. Problem Statement

The order of problem listing in health care sector is needed to permit extra useful information swap within health care providers and in particular with victims. Paper-based format do not effort in digital status, and any pattern of problem-listing construction, like automatic listing, represent significant compliance and patient safety issues.

D. Proposed System

The blockchain is treated as an advanced technological innovation. It is a peer-to-peer scattered ledger mechanizations for recording activity, arrangements and marketing. The uses of blockchain mechanization are decentralized preservation, evidence backup in the slab arrangement, protected transport and information access, along with inviolable and tamper-proof data preservation. Leveraging these distinctive appearance of health report scheme, Blockchain helps manage authentication, accountability, and data sharing while ensuring the processing of informa-tion about privacy, preservation and facilitation of resources. For the patient, and improving the health of the populations.

1) Advantages

a) Give authentic, timely and full information about victims at the time of treatment.
b) Provide immediate access to victims reports for more integrated and effective responsibility.
c) Protected sharing of digital message with victims and doctors.
d) Support providers more adequately recognize patients, reduce medicinal failure and gives security measure.

II. LITERATURE SURVEY

The following works were carried out by specific persons in the area of Block-chain and EHR:

1) Medical records of patients are usually fragmented several treatment sites, posing an obstacle to efforts in clinical care, research and public health. Electronic medical records and the Internet provide a technical infrastructure on which to build longitudinal medical records that can be integrated into the sites of care. Choices regarding the structure and ownership of these recordings will have a profound impact on the accessibility and confidentiality of patient information. Already, alarming trends are obvious as property online Medical records systems are developed and deployed. Promising technology to unify the current market disparate elements of a patient's medical record may actually threaten the accessibility of information and compromising the privacy of patients. In this article, propose two doctrines and six desirable characteristics to guide the development of the online medical record systems. We describe how such systems could be developed and used clinically.

2) This paper presents a fully secure attribute-based signature scheme in the standard model. The security of the proposed ABS system is proven by standard assumptions, the linear decision-making hypothesis and the existence of collision-resistant hash functions. The permissible predicates of the proposed ABS scheme are more general than those of existing ABS schemes. The proposed ABS schema is the first to support general non-monotonic predicates, which can be expressed using NOT gates as well as AND, OR, and Threshold operators. Gates, while existing ABS schemes only support monotonic predicates. The proposed ABS scheme is as effective as one of the most efficient ABS schemes, which has been proven safe in the generic group model.

3) Data privacy is about ensuring that users retain control over access to information, while data accessibility is about ensuring that access to information is not limited. It is natural that conflicts between privacy and accessibility of data are occurring and health care is an area in which they are particularly relevant. In this article, we discuss how blockchain technology and smart contracts could help in some typical scenarios related to data access, data management, and data interoperability for the specific domain Health care. We then propose the implementation of a large-scale information architecture to access electronic health records (EHRs) based on smart contracts as information mediators. Our main contribution is the definition of privacy and data accessibility issues in the health sector and the proposal of an integrated blockchain architecture.

III. THEORETICAL BACKGROUND

A. Block-Chain

A Blockchain is a growing list of records called Blocks. That are linked using cryptography function. Each block contain a cryptographic hash of the previous block, timestamp, transaction data, signature and nonce. A blockchain is resistant to changing the data. It is an open and distributed large book capable of recording transactions between two parties in an efficient, permanent and verifiable manner. It is used as a distributed ledger, a blockchain is generally managed by a peer-to-peer network that collectively adheres to a protocol for inter-node communication and validation of new blocks. Once recorded, the data of a given block cannot be modified retroactively without modification of all the previous blocks, which requires a consensus of the majority of the network. Although blockchain records are not unalterable, they can be considered secure by design.

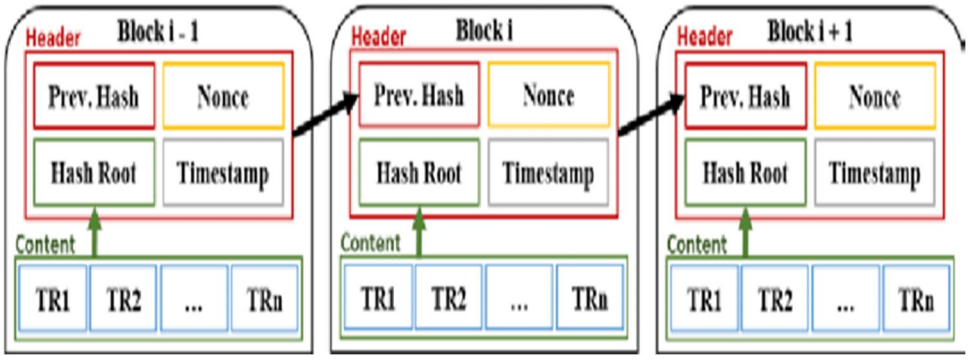


Fig. 1 Blockchain

Blockchain technology was previously developed for Bitcoin cryptocurrency and was first introduced in the Nakamoto bitcoin white paper in 2008. Since blockchain technology has been seen as a new technological revolution, like the invention of the steam engine or the Internet.

Typical block metadata contains:

1) *Version* - The current version of the block structure
2) *Previous block header hash* - The reference of the main block of this block
3) *Root hash:* A cryptographic hash of all the transactions included in this block.
4) *Time* - the time this block was created
5) *n-Bits:* The current difficulty that was used to create this block
6) *Nonce ("number used once")* - A random value that the creator of a block can manipulate.

B. Blockchain in EHR

The concept of applying blockchain in health care systems for the purpose of security and interoperability in health care. With the evolution of internet of things and the abundance of health devices and mobile health apps, a tremendous amount of health data is being recorded and transferred each day. This data traffic requires management in terms of privacy and security. Blockchain technology can provide a solution that not only helps in secure the registration and sharing of medical reports, but also ensures the privacy of each patient's record by giving patients ownership of their medical record. In addition to the benefits of blockchain for health care management, its challenges need to be addressed in advanced.

Previously, there were many restrictions on sharing health records electronically because of the risks to data security or the leakage of private information from the patient during the data exchange. In addition, current EHRs are managed by providers and hospitals, while patients are denied the right to freely control their own health records electronically. Using blockchain technology, data logging and identity management are established and the blockchain of EHRs is built. Furthermore, this technology records audit trails of all transactions in an immutable distributed ledger, ensuring accountability and transparency in the processing of data exchanges. As a result, the patient has the ability to record health care and diagnostic information from physicians in their own health records, thereby reducing the number of medical accidents and providing the patient's privacy.

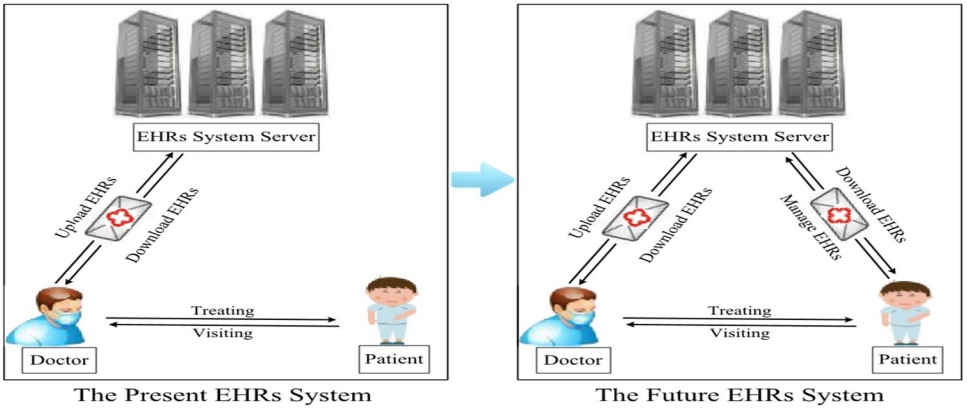


Fig. 2 Present and Future system of Electronic health reports

Benefits of Electronic Health Report:

1) EHRs reduce your administrative tasks
2) EHRs put your information accurately in the hands of people who need it
3) EHRs help your doctors coordinate your care and protect your safety
4) EHRs reduce unnecessary tests and procedures
5) EHRs give you direct access to your health records

IV. SYSTEM REQUIREMENTS

A. Hardware Requirements

1) System : Pentium IV 2.4 GHz
2) Hard Disk : 500 GB
3) Ram : 4 GB
4) Keyboard : Standard keyboard

B. Software Requirements

1) OS : Windows XP/7
2) IDE : Eclipse Galileo
3) Coding : Java (Jdk 1.7)
4) Web Technology: Servlet, JSP
5) Web Server : TomCat6.0
6) Database : MySQL5.0

V. SYSTEM ANALYSIS

A. System Architecture

The system architecture shows the structure and behaviour of the system. Fig 3 shows the structure of Blockchain process in EHRs. In a cloud storage platform, the system EHR consists of certain departments, such as hospitals, pharmaceutical departments, insurance departments, research departments, and so on. All departments can provide patient services together and limit the rights of each department to prevent the misuse of EHRs. Thus, an EHR system with a blockchain structure is designed. Suppose that each patient has only one health care chain. After being treated in a hospital, all information, including EHRs, consumption records, insurance records, etc., is encapsulated in a block. Patient treatments at different times will be generated in different blocks. Then, a series of blocks is generated based on the time sequence and a chain of health care of that patient is constructed.

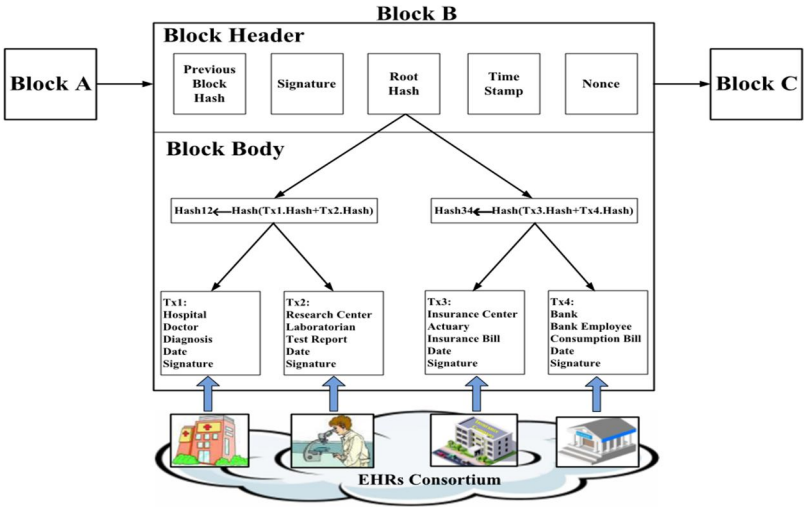


Fig. 3 System architecture of blockchain in EHRs

To meet the distributed structure requirement in the EHR system, we use an attribute-based signature with multiple authorities to process the above application. An MA-ABS system is a protocol by which a signature attests not to the identity of the patient who endorsed a message, but rather to a claim about the delegated attributes of certain authorities that they possess.

VI. IMPLEMENTATION

A. Modules

1) *Admin Module:* The administrator must login with username and password. Once logged in admin can view his profile, can edit and change password, he will add the details of data owner, auditor, department, designation and he can also edit the details and gets logged out.
2) *Data Owner (Doctor):* The Data owner must login with username and password. Once logged in he can view his profile can edit also. Here he will add the user details and upload the file. While uploading file, have to generate the hashtag, which we considering as current hashtag then have to take previous file current hashtag for this current file genius hashtag /previous hashtag and timestamp and nonce. Nonce is nothing random number generation.

Previous hashtag + current hashtag +timestamp + nonce = concatenating these parameter have to generate the confidential key. This is the header part of block chain.

File we are considering as Body part which is giving body part of 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. After this he set the access control option Data Owner can set access control for multiple users.

3) *User*: The user must login with username and password. Once logged in user can view his details and has right to download the file. while downloading, based on file id this system is picking the block id 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.

   After downloading complete he can view the transaction details and send request to auditor to verify the file.
4) Auditor: The auditor gets login and he verify the file when he gets request from user. During verification the file has to get downloaded from cloud then has to get unzip after unzip using 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.

B. Algorithms

1) *RSA Algorithm:* The RSA algorithm is the foundation of a cryptographic system - a suite of cryptographic algorithms used for specific security services or objectives - that enables public-key encryption and is widely used to secure sensitive data, particularly when they are sent via an insecure server network such as the Internet.

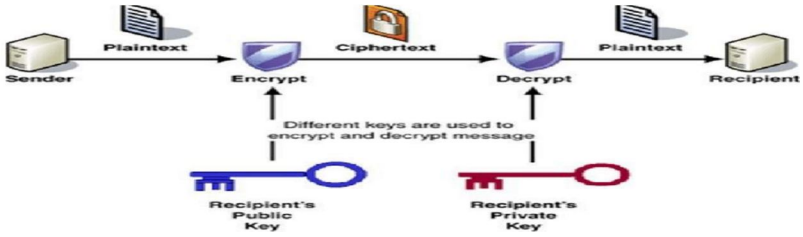


Fig. 4 Generating Public and Private Keys

Public key cryptography, also known as asymmetric cryptography, uses two distinct but mathematically related keys, one public and the other private. The public key can be shared with everyone, while the private key must remain secret.

2) *MD5 (Message Digest 5)*

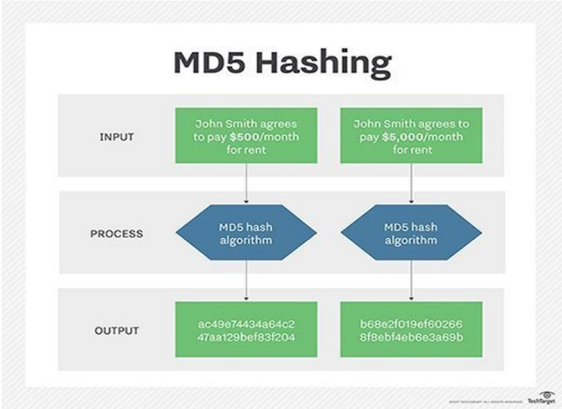


Fig. 5 MD5 Hashing

The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any input length and returns a fixed-length summary value to be used for authentication of the original message. The MD5 hash function was originally designed to be used as a secure cryptographic hash algorithm for authentication of digital signatures. MD5 is not recommended for uses other than as a non-cryptographic checksum to verify the integrity of data and to detect unintentional data corruption.

3) *DES Algorithm:* DES works by using the same key to encrypt and decrypt a message, so the sender and recipient must know and use the same private key. The data encryption standard is a block cipher, which means that a cryptographic key and an algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a message in plain text, DES the group into 64-bit blocks. Each block is encrypted using the secret key in a 64-bit encrypted text by means of permutation and substitution. The process involves 16 rounds and can run in four different modes, encrypting the blocks individually or making each encrypted block dependent on all previous blocks. Decryption is simply the opposite of encryption.

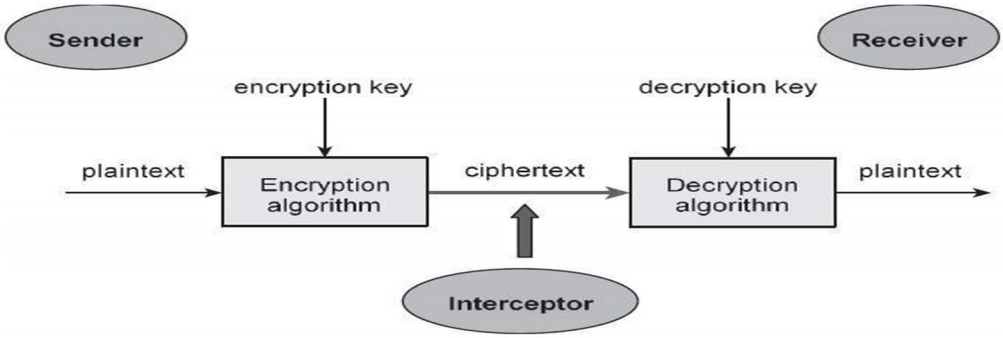


Fig. 6 DES Encryption and Decryption

VII. RESULTS

The following snapshots define the results or outputs that are obtained after step by step execution of all modules of the system.

1) *Admin Login:* Fig 7 shows the login process to admin page of Electronic health report system.
2) *Admin profile details:* Fig 8 shows the admin profile information, in which admin can edit profile and even can change password.
3) *Auditor Details:* Fig 9 shows auditor details added by the admin . here admin can view and update the auditor details. Where auditor details include name, user id, address, email and contact number.
4) *Data Owner Details:* In fig 10 we can see the data owner details added by the admin. Where admin can view and update the data owner details.
5) *Key Generation:* Fig 11 shows the key is updated successfully. When key is updated it means internally it has generated the private key.

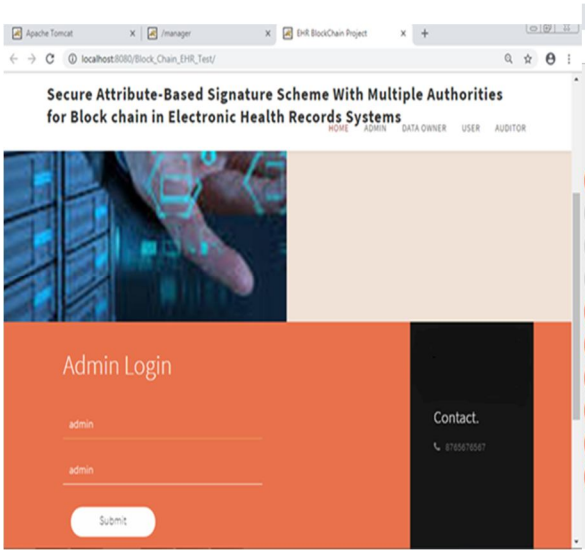


Fig.7 Admin Login

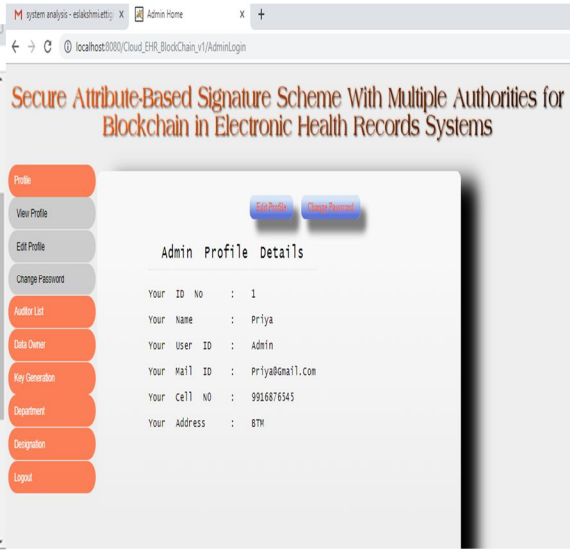


Fig. 8 Admin Profile details

Fig. 9 Auditor details

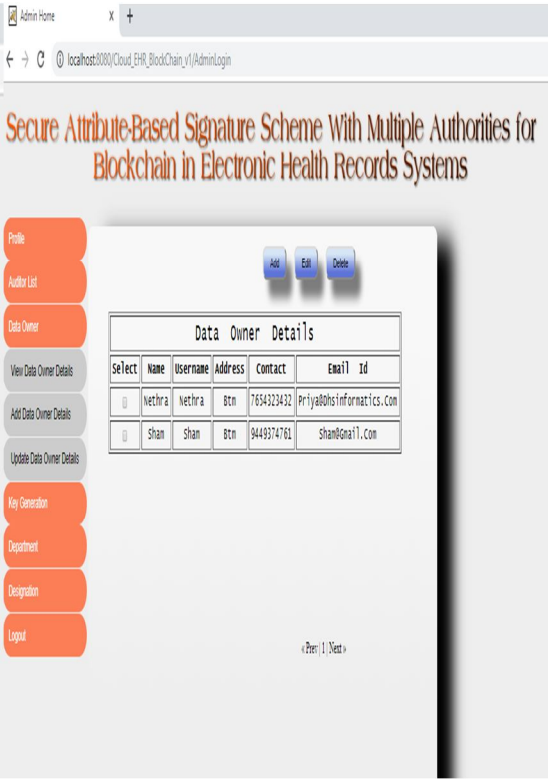


Fig. 10 Data Owner details

6) *File Upload:* Fig 12 shows the file upload process. Here we upload the file in .txt format . File means patient report.
7) *File Upload Acknowledgement:* In fig 13 we can see the file upload acknowlegement message, which contain information like user name, in which cloud our file is uplaoded, file name with date and time.
8) *Available File to Download:* Fig 14 shows the data owner uploaded file is available to download for the patient. Where this block contain the upload time and date information.
9) *File Download Acknowledgement:* Fig 15 shows the file download acknowledgement . Which contains the details like file name with date and time.

Fig. 11 Key Generation

Fig. 12 Upload File

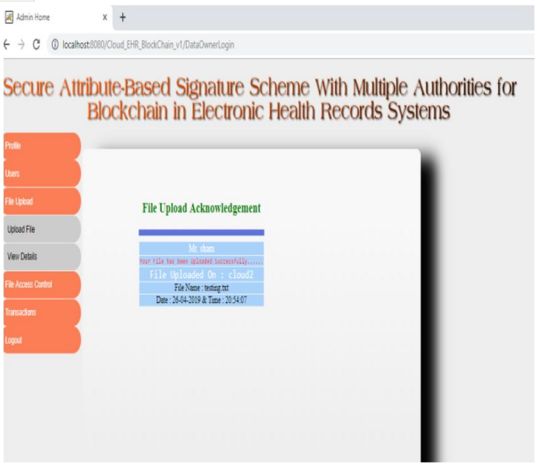


Fig. 13 Upload File Acknowledgement

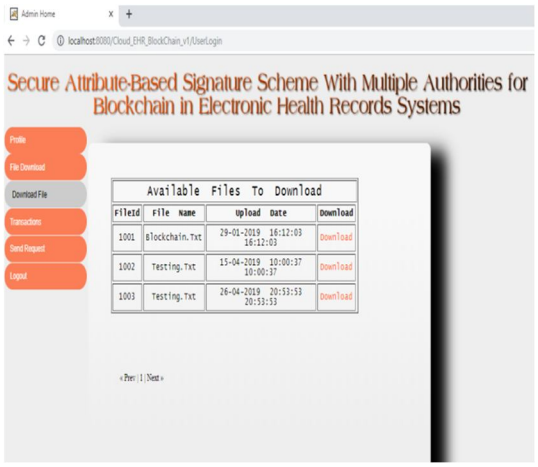


Fig. 14 Available file to Download

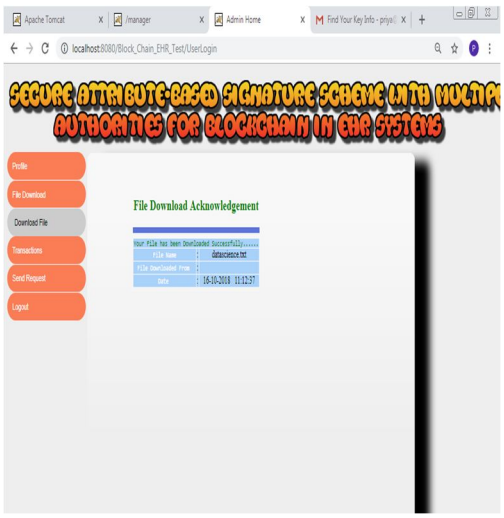


Fig. 15 Download Acknowledgement

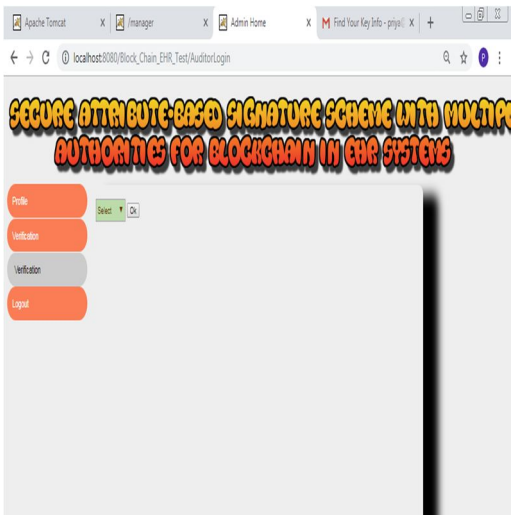


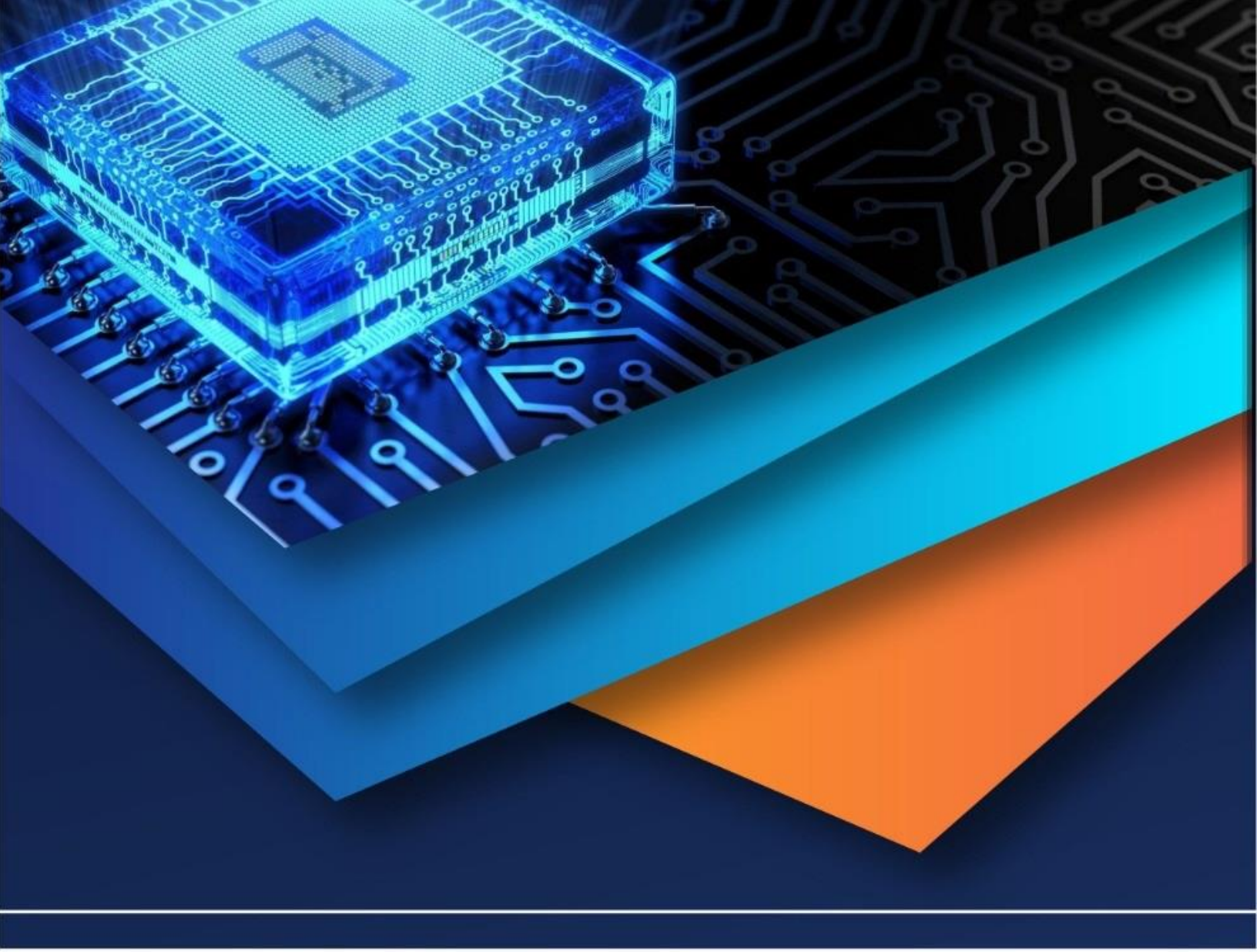
Fig. 16 Verification

VIII. CONCLUSION

Aim to preserve the privacy of patients in an EHR system on Blockchain, several authorities are introduced in the ABS and present an MA-ABS system that meets the need of the structure of the Blockchain, as well as the guarantee of anonymity and unchangingness of information. PRF seeds are needed between the authorities and the private keys of the patient must be built, N-1 corrupt authorities can't succeed in collusion attacks. Finally, the protection of protocol is proved under the CBDH hypothesis in terms of impregnation and excellent privacy. Comparison analysis demonstrates the performance and cost of this protocol increases linearly with the number of authorities and patients attributes as well. A non-monotonic predicate could be used in several distributed system applications that enriches the illustration of the predicate. Non monotonic general support predicates in Blockchain technology is that the direction of the future work.

REFERENCES

[1] H. K. Maji, M. Prabhakaran, and M. Rosulek, ''Attribute-based signatures,'' in Proc. CT-RSA, San Francisco, CA, USA, 2011, pp. 376–392.
[2] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, ''Attribute-based signature and its Application '' in Proc. ASIACCS, Beijing, China, 2010, pp. 60–69.
[3] J. Herranz, F. Laguillaumie, B. Libert, and C. Ràfols, ''Short attribute-based signatures for threshold predicates,'' in Proc. CT-RSA, San Francisco, CA, USA, 2012, pp. 51– 67.
[4] T. Okamoto and K. Takashima,'' Efficient attribute-based signatures for non-monotone predicates in the standard model,'' in Proc. PKC, Taormina, Italy, 2011, pp. 35–52.
[5] C. Chen et al.,'' Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures,'' in Proc. CT-RSA, San Francisco, CA, USA, 2013, pp. 50–67.
[6] Y. S. Rao and R. Dutta, '' Efficient attribute-based signature and signcryption realizing expressive access structures,'' Int. J. Inf. Secur., vol. 15, no. 1, pp. 81–109, Feb. 2016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY