International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET207461

Block chain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors

V. Sujatha*, V. Sai Sameera , P. Yuvasri, K. Akhil Verma, G. Sankar Naveen
Department of CSE, BITS VIZAG, Visakhapatnam, Andhra Pradesh, India

Article Info
Volume 7 Issue 4
Page Number: 224-230
Publication Issue :
July-August-2020

Article History
Accepted : 05 Aug 2020
Published : 12 Aug 2020

ABSTRACT

The main objective of this project is securely store and maintain the patient records in the health care. Headrest is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily. The block chain technology is used to protect the Headrest data hosted within the cloud. The block that contain the medical data and the time stamp. Cloud computing will connect different health care providers. It allows health care provider to access the patient details more securely from anywhere. It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The health care provider have to decrypt the data prior to download.

Keywords: Decrypt, Health Care, Cloud Computing

I. INTRODUCTION

Cloud computing offers an opportunity for individuals and companies to offload to powerful servers the burden of managing large amounts of data and performing computationally demanding operations. Due to the increasing popularity of cloud computing, more and more Data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. Data owners offer services to a large number of businesses and companies, they stick to high security standards to improve data security by following a layered approach that includes data encryption, key management, strong access controls, and security intelligence. Headrest is a data-intensive domain where a large amount of data is created,disseminated, stored, and accessed daily. It is clear that technology can play a significant role in enhancing the quality of care for patients (e.g. leveraging data analytic to make informed medical decisions) and potentially reduce costs by more efficiently allocating resources in terms of personnel, equipment, etc. Generally, Electronic Medical Records (Em Rs) contain medical and clinical data related to a given patient and stored by the responsible Headrest provider. This facilitates the retrieval and analysis of Headrest data. To better support the management of Em Rs, early generations of Health Information Systems (HIS) are designed with the capability to create new EMR instances, store them, and query and retrieve stored Em Rs of interest.2 HIS can be relatively simple solutions, which can be schematically described as a graphical user interface or a web service. These are generally the front-end with a database15at the back-end, in a centralized or distributed, implementation. With patient mobility (both internally and externally to a

given country) being increasingly the norm in today's society, it became evident that multiple stand-alone EMR solutions must be made interoperable to facilitate sharing of Headrest data among different providers, even across national borders, as needed. For example, in medical tourism hubs such as Singapore, the need for real-time Headrest data sharing between different providers and across nations becomes more pronounced.

To facilitate data sharing or even patient data portability, there is a need for Em Rs to formalize their data structure and the design of HIS. Electronic Health Records (E Hrs), for example, are designed to allow patient medical history to move with the patient or be made available to multiple Headrest providers (e.g. from a rural hospital to a hospital in the capital city of the country, before the patient seeks medical attention at another hospital in a different country).3 E Hrs have a richer data structure than Em Rs. There have also been initiatives to develop HIS and infrastructures that are able to scale and support future needs, as evidenced by the various national and international initiatives such as the Fascicle Humanitarian Electron (FSE) project in Italy, the pesos project in Europe, and an ongoing project to standardize sharing of E Hrs. Recently, the pervasiveness of smart devices (e.g. Android and i OS devices and wearable devices) has also resulted in a paradigm shift within health industry. Such devices can be user-owned or installed by the Headrest provider to measure the well- being of the users (e.g.patients) and inform/facilitate medical treatment and monitoring of patients. For example, there is a wide range of mobile applications (apps) in health, fitness,weight-loss, and other Headrest related categories. These apps mainly function as a tracking tool, such as registering user exercises/workouts, keeping the count of consumed calories, and other statistics (e.g. number of steps-taken), and so on. 16There are also devices with embedded sensors for more advanced medical tasks, such as bracelets to measure heartbeat during workouts, or devices for self testing of glucose. The data (e.g. user's vital signs) can be continuously gathered and sent in real- time to a smart device, before being sent to a remote Headrest cloud for further analysis. Another example is Ambient Assisted Living solutions for Headrest designed to realize innovative healthful and tele medicine services, in order to provide remote personal health monitoring. These developments have paved the way for Personal Health Records (PHR), where patients are more involved in their data collection, monitoring of their health conditions, etc, using their smart phones or wearable devices (e.g. smart shirts and smart socks). block chain was originally designed to record transaction data, which is relatively small in size and linear. In other words, one only concerns itself about whether the current transaction can be traced backwards to the original "deal".

II. MEHTHOD AND MATERIAL

Problem Definition:

1. The main objective of this project is securely store and maintain the patient records in the Headrest.
2. Headrest is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily.
3. The block chain technology is used to protect the Headrest data hosted within the cloud.
4. The block that contain the medical data and the timestamp.
5. It allows Headrest provider to access the patient details more securely from anywhere.

6. It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud.
7. The Headrest provider have to decrypt the data prior to download.

III. EXISTING SYSTEM

Existing system doesn't maintain and process the data securely. It doesn't provides the more accurate search result. Incorrect and misleading of data will produce the wrong analysis result. Low search Efficiency. The search delay of the scheme is proportional to the size of the database. It is not suitable for the large scale databases.

DISADVANTAGES

1. Low search Efficiency
2. The search delay of the scheme is proportional to the size of the database.
3. It is not suitable for the large scale databases.
4. Doesn't support verification upon file update.
5. Data Integrity attacks.

IV. RESULT AND DISCUSSION

PROPOSED SYSTEM

1. To overcome the security problems that are occurred in the existing system and effectively store the data over the cloud we introduce this system.
2. The data user outsources the encrypted documents to the cloud.

ADVANTAGES

1. Efficient Search Result.
2. Prevents data freshness attacks and data integrity attacks.
3. It provides High Security.

MODULES

Registration

It is a process of enrolling or being enrolled into the cloud. To utilize the cloud documents, every Headrest provider should enroll. During this process your basic information like email, contacts etc., are collected and stored in the Cloud. The cloud id for a particular user will get automatically generated during the registration.

Cloud ID

Every user should create a Cloud ID and use it to identify something with near certainty that the identifier does not duplicate one that has already been, or will be, created to identify something else. Information labelled with Cloud ID by independent parties can therefore be later combined into a single database, or transmitted on the same channel, without needing to resolve conflicts between Identifiers.

Headrest Provider

1. Load patient Records
2. Key Generation
3. Encrypt patient Records
4. Block Creation
5. Upload and Download Patient Records

Data Selection and Loading

In this process, the health provider choose patient Headrest records for uploading and maintaining the dataset in the cloud.

Key Generation

The secret key is generated using cryptographic algorithm. This key is used for encrypting the dataset.

Encrypt Patient Records

The data is encrypted for secure maintenance. So that the unauthorized person cannot be able to access the data that are presented in the cloud.

Block Creation

1. Each block contain patient record and timestamp.
2. A block chain, originally block is a growing list of records called blocks.

Upload and Download Patient Records

After creating the block, the Headrest provider will upload the records into the cloud. Suppose, if they want to retrieve an record from cloud, first the Headrest provider search the record. Based on the search it will show the results. After getting an approval and key from the cloud service provider the Headrest provider can download the data.

Cloud Service Provider

The cloud service provider maintain all the patient records and also they can provide a permission to the user to access the data.

The Cloud Service Provider can view all the uploaded and downloaded documents in the Cloud. The CSP receives the document request from the Data User, verifies the authentication before granting permission. Then the CSP executes the query and returns the encrypted document according to the search token. And also returns an additional proof with the document, to verify the search result.

Public Verification Key

Public verification key is a security measure designed to make sure that your document outsourced in cloud doesn't get hacked. By verifying public key, the Data Owner and the Data User adding another layer of protection to the documents or files in the cloud by confirming each other's identities.

User Training

To achieve the objectives and benefits expected from the proposed system it is essential for the people who will be involved to be confident of their role in the new system. As system becomes more complex, the need for education and training is more and more important. Education is complementary to training. It brings life to formal training by explaining the background to the resources for them. Education involves creating the right atmosphere and motivating user staff. Education information can make training more interesting and more understandable.

Training on the Application Software

After providing the necessary basic training on the computer awareness, the users will have to be trained on the new application software. This will give the underlying philosophy of the use of the new system such as the screen flow, screen design, type of help on the screen, type of errors while entering the data, the corresponding validation check at each entry and the ways to correct the data entered. This training may be different across different user groups and across different levels of hierarchy.

Operational Documentation

Once the implementation plan is decided, it is essential that the user of the system is made familiar and comfortable with the environment. A documentation providing the whole operations of the system is being developed. Useful tips and guidance is given inside the application itself to the user. The system is developed user friendly so that the user can work the system from the tips given in the application itself.

System Maintenance

The maintenance phase of the software cycle is the time in which software performs useful work. After a system is successfully implemented, it should be maintained in a proper manner. System maintenance is an important aspect in the software development life cycle. The need for system maintenance is to make adaptable to the changes in the system environment. There may be social, technical and other environmental changes, which affect a system which is being implemented. Software product enhancements may involve providing new functional capabilities, improving user displays and mode of interaction, upgrading the performance characteristics of the system. So only thru proper system maintenance procedures, the system can be adapted to cope up with these changes. Software maintenance is of course, far more than “finding mistakes”.

Corrective Maintenance

The first maintenance activity occurs because it is unreasonable to assume that software testing will uncover all latent errors in a large software system. During the use of any large program, errors will occur and be reported to the developer. The process that includes the diagnosis and correction of one or more errors is called Corrective Maintenance.

Adaptive Maintenance

The second activity that contributes to a definition of maintenance occurs because of the rapid change that is encountered in every aspect of computing. Therefore Adaptive maintenance termed as an activity that modifies software to properly interfere with a changing environment is both necessary and commonplace.

Perceptive Maintenance

The third activity that may be applied to a definition of maintenance occurs when a software package is successful. As the software is used, recommendations for new capabilities, modifications to existing functions, and general enhancement are received from users. To satisfy requests in this category, Perceptive maintenance is performed. This activity accounts for the majority of all efforts expended on software maintenance.

Preventive Maintenance

The fourth maintenance activity occurs when software is changed to improve future maintainability or reliability, or to provide a better basis for future enhancements. Often called preventive maintenance, this activity is characterized by reverse engineering and re-engineering technique.

V. CONCLUSION

It's more securely maintain all the patient records and it will be easily accessible by any Headrest providers.

By building block chain, it provides efficient search result verification, while preventing data freshness attacks and data integrity attacks in SSE.

VI. FUTURE ENHANCEMENT

Data Classification based on Security: A cloud computing data center can store data from various users. To provide the level of security based on the importance of data, classification of data can be done. This classification scheme should consider various aspects like access frequency, update frequency and access by various entities etc. based on the type of data. Once the data is classified and tagged, then level of security associated with this specific tagged data element can be applied. Level of security includes confidentiality, encryption, integrity and storage etc. that are selected based on the type of data.

VII.REFERENCES

[1]. Yunru Zhang, Debiao He, and Kim-Kwang Raymond Choo, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT," Wireless Commu. and Mobile Comput., 2018.

[2]. Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, and Yan Zhang "block chain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things J., 2018.

[3]. Oscar Novo, "block chain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things J., vol. 5, pp. 1184-1195, 2018.

[4]. Kuo TT, Kim HE, and Ohno-Machado L, "block chain distributed ledger technologies for biomedical and health care applications," Ame. Medi. Infor. Assoc. J., vol. 6, pp. 1211-1220, 2017.

[5]. Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher, "Towards Using block chain Technology for eHealth Data Access Management,"in Proc. IEEE on Advances in Bio. Engi., Oct. 2017.

[6]. S.H. Han et al., "Implementation of Medical Information Exchange System Based on EHR Standard" 2010.

[7]. D. He et al., "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Headrest Social Network," IEEE Transactions on Dependable and Secure Computing,

[8]. F.Y. Leu et al., "A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data," Computers and Electrical Engineering, 2017.

[9]. M. Memon et al., "Ambient Assisted Living Headrest Frameworks, Platforms, Standards, and Quality Attributes", 2014.

[10]. P.C. Tang et al., "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption" 2006.

[11]. S. Marceglia et al., "A Standards-Based Architecture Proposal for Integrating PatientHealth Apps to Electronic Health Record Systems" Applied Clinical Informatics, 2015.

[12]. A. Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve

Health Care Services" Journal of Medical Internet Research, 2011.

[13].V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities" IEEE Cloud Computing, 2016.

[14].S. Nepal et al., "Trustworthy Processing of Headrest Big Data in Hybrid Clouds" IEEE Cloud Computing, 2015.5

[15].G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges" 201

Cite this article as :

V. Sujatha, V. Sai Sameera , P. Yuvasri, K. Akhil Verma, G. Sankar Naveen, " Block chain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 7, Issue 4, pp.224-230, July-August-2020. Available at doi : https://doi.org/10.32628/IJSRSET207461
Journal URL : http://ijsrset.com/IJSRSET207461