International Journal for Modern Trends in Science and Technology, 7(04): 163-166, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0704026
Available online at:http://www.ijmtst.com/vol7issue04.html

Ensure Authentication with Time-Based Secure Encryption in Medical Document

Pyla Goutam[1]| Sripada Sai Praneeth[1]| Yarlagadda Sai Krishna[1] | Tanishq Ittamsetty[1] | Chava Venkata Sai[1]| Amritpal Singh[2]

[1]UG Student, Department of Computer Science, Lovely Professional University, Punjab
[2]Department of Computer Science Engineering, Lovely Professional University,Punjab

To Cite this Article
Pyla Goutam, Sripada Sai Praneeth, Yarlagadda Sai Krishna, Tanishq Ittamsetty, Chava Venkata Sai and Amritpal Singh, "Ensure Authentication with Time-Based Secure Encryption in Medical Document", *International Journal for Modern Trends in Science and Technology*, Vol. 07, Issue 04, April 2021, pp.:163-166.

Article Info
Received on 25-March-2021, Revised on 14-April-2021, Accepted on 18-April-2021, Published on 22-April-2021.

ABSTRACT

The health sector has been growing day by day in recent times. For example, to prescribe an unconventional method of medical care or to promote a new drug, it is necessary for the hospital to neglect existing medical knowledge. For a research organization. Medical knowledge is too diverse as it includes one's personal details like their name, social insurance, address, gender, and date of birth to even their debit card's expiration dates. Hence, it is only logical to protect patients' privacy after using their medical knowledge for clinical studies and data analysis. In this project, we are going to ensure a lightweight security mechanism with time-based secure encryption in medical documentation. At this point, using an encrypted cryptographic approach, users can share their data in a secure and secure manner. To tackle this, we present a versatile, secure, affordable, and secure cloud-based web page for meditation environments.

KEYWORDS: *Ensure, Cryptographic*

I. INTRODUCTION

A typical surprise in medical care in most Asian countries is the unavailability of proper human and physical assets which are in the range of foresters to provide for integrated medical services. Insights suggest that Asian countries experience high PACE side effects of medical problems such as diabetes, liver infections, and parasites, for example, schistosomiasis and malaria fever. These can be detected before medical conditions develop or their problems can be ruled out in advance. This is because of the combination of the setting, functions, and specifics of the variable. If we have a chance to beat them, it will lead to significant progress in the degree of medical services. Similarly, the absence and absence of an accessible emergency clinic data framework, which is the most exceptional programming that directly provides all specialized and formal medical services methods, guarantee that clinical organizations have their methods and have full power over perfection. The success of these high-end frameworks does not depend on the specific choice of gear and programming for efficiency. Their well-being to different clients - from medical care providers such as professionals, caregivers, professionals, and executives - may depend on what each of these classes' vision and needs are conflicting and their data should change. These are the advantages of each framework.

II. RELATED WORK

The traditional medical care data framework already used in the field of medical services was

paper-based and later suppressed by the Healthcare Information System (HIS). However, HIS was found to be unsuccessful due to some issues such as stockpiling restriction, framework combination, high work cost, and framework support. Distributed computing is another innovation that describes the production, framework, and computational steps anywhere on the Internet, anytime and anywhere. This innovation states that they can solve many problems of the medical care framework, for example, increase capacity limits and add new capabilities to the existing medical care framework. Distributed computing offers financially savvy, increment interoperability and openness, streamline assets and incorporate the medical care data frameworks. It turns into an answer for tackling the recent concerns, which lead to upgrade usefulness and highlights of the medical services data frameworks. Accordingly, the point of this examination is to investigate distributed computing innovation as an answer for medical services data framework issues. Issues like information transmission, information stockpiling, cost, and upkeep issues are introduced and portrayed. The ramifications of this investigation at that point were talked about.

As medical care administration costs increase and medical care specialists become less and less vague, medical service associations will inevitably consider achieving the Health Data Innovation (HIT) framework. To support health communities more effectively and practically, HIT allows them to streamline their cycles in greater numbers. Innovations like Cloud Computing(CC) provide a framework and real empowerment for HIT administrators on the internet. Requests of the medical service industry can be met by the use of 'e-Health cloud' by its compensation. Despite its exceptional capabilities, HIT is not widely written as a CC model. There is no clear structure that reveals every appropriate planning and interaction between HIT and CC. Understanding the scheme's effectiveness and its isolation is accordingly important. Discussing the multi-component introductory idea of 'E-health cloud', and a large number of difficulties in building the e-Health climate and managing its success is the main theme of the paper. Looking for unconventional answers to address security concerns and protection issues is also a part of it.

III. PROPOSED MECHANISM

In this project. We are going to ensure a lightweight secure mechanism with time-based secure encryption in medical documents. At this point, using an encrypted cryptographic approach, users can share their data a while. In this application, we implement a strong authentication policy to prevent unauthorized login and malicious operation in medical applications. We have also implemented a strong encryption policy to securely manage data in this application. . We propose a versatile, secure, cost-effective, and privacy-protected cloud-based framework for meditation environments.

IV. ALGORITHM

In addition to secure knowledge security in cloud computing, the main goal of the design is to achieve properly accessible access management and climate user withdrawal. In particular, we need to shift our goals to the following points:

Ala Scalability: The information owner is offline in user editing mode.

Ine Fine-grinded access control: The data owner can specify an express access structure for each data.

Privacy Data Privacy: Cloud service providers and malicious users will not be able to retrieve information and will not be allowed to own information.

Efficiency Cost Efficiency: The value of re-encryption at the cloud service provider is very low.

For scalability, each user's access should be automatically disabled after a predetermined period; For precise access control, we must adopt an encryption system that supports feature-based access structures such as CP-ABE and KP-ABE; For data privacy, we must always allow users with features that satisfy the access structure and have access rights over a period of time to retrieve data; For the price possible, we need to implement Lazy Re-encryption (LRE) on the private release encryption theme at that time, so the cloud service provider will only encrypt data after receiving access requests from customers.

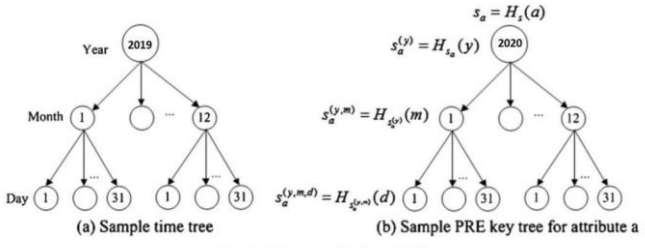
V. TIME PRIVATE RELEASE ENCRYPTION SCHEME

The main idea of the Time Private Release Provider Scheme is to combine the concept of time with the hub and private release encryption. Of course, each user is characterized by a collection of

features and an effective duration, but this is reflected over a longer period of time. The consumer is entitled to these features, i.e. the valid amount of consumer rights. Information accessed by users AN attribute-based access structure AND is related to the time interval. The structure of access is maintained by the data owner, but the time interval is updated by the time the cloud service provider receives the AN access request. Information can only be retrieved by users whose features satisfy the access structure and whose access rights are effective during the class time period. We have a tendency to mechanically change the cloud service provider to update the time period, as the initial specific real-time time tree. The top of the time tree is modified to support reconnection. For easy presentation, we have a tendency to reflect only on the three-layer time tree at the time of this paper, because the time of day is the optimal time, so the time tree is classified into 3 layers: year. , Month and day. We use (y, m, d), (y, m), and (y) to denote a specific day, month, and year. For example, (2019, 4,5) the Gregorian calendar represents month five, 2012. The information-related time interval corresponds to a leaf node in the time tree and therefore to the collection of effective time periods associated with it by the user. Nodes in the time tree. If a node recalls a good basic size that recalls (or equals) the time period later, the user's capture will be executed at the appropriate time interval.

After that, we have a tendency to let the information owner so the Cloud Service Provider shares the root private key in advance, so the Cloud Service Provider will calculate the required Secret Encryption keys that support their time and rewrite the corresponding text on the machine.

.Specifically, at any time, all attributes a are related to one of the first public keys PKa, and 3 public time keys: public key based on the day PKa (y, m, d), public key based on the month PKa (y, m) , and the public key based on the year PKa (y), all of which means the public key during a specific day (y, m, d), month (y, m), and year (y).



Three-level time tree and attribute a's PRE key tree.

The first public key symbols within the access building. Upon receipt of the invitation, the Cloud Service Provider uses the basic secret key S to calculate the Private Encryption keys for all attributes within the access point based on its time, and thus use these private encryption keys to rewrite the original text by switching the first public keys of all attributes within the framework of access to time-based public keys.

We use sa (y), sa (y, m), and sa (y, m, d) to identify the encryption keys for encrypted encryption in the adjective (y), (y, m), and (y, m, d), which can be used to reset the first PKa public key to the time-generated public keys PKa (y), PK a (y, m), and PKa (y, m, d), respectively. Since the Secret Encryption key used in our theme comes from the root private key and therefore the current time period, we have a tendency to use completely different notifications such as, for all attributes a period and the following figures:

Sa(y)= HSa(y)
Sa(y, m)= H Sa (y)(m)
Sa(y, m, d)= H Sa(y, m)(d).

VI. CONCLUSION

Already the data framework for medical care used in the medical services environment was based on paper and was later replaced by the Healthcare Information System (HIS). However HIS has been found to be ineffective due to a number of issues such as storage limit, framework combination, high operating costs and framework support. Distributed computer is one of the new products that transmits the product, framework and component of the computer as a help to the Internet anywhere and anytime. These innovations are said to address many of the problems of the medical care framework, for example, to increase capacity and add new capabilities to the current medical care framework. In this project we will use a lightweight and secure method of Verifying Time Based Secure Encryption in Medical Document. By using this encrypted Time encryption method users can share their information in a secure and secure way. We propose a flexible, secure, cost-effective, and confidential cloud-based framework for environmental health care.

REFERENCES

[1] Masrom, Maslin, and Ailar Rahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.

[2] HUCÍKOVÁ, Anežka, and Ankica Babic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." Transforming Healthcare with the Internet of Things (2016): 122.
[3] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.
[4] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583–592.
[5] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).
[6] How to Improve Healthcare with Cloud Computing , By Hitachi Data Systems, white paper, (2012).
[7] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.
[8] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." Procedia Engineering 15 (2011): 2852–2856.
[9] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485–490.
[10] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).
[11] Omachonu, Vincent K., and Norman G. Einspruch. "Innovation in healthcare delivery systems: a conceptual framework." The Innovation Journal: The Public Sector Innovation Journal 15, no. 1 (2010): 1–20.
[12] Reddy, B. Eswara, TV Suresh Kumar, and Gandikota Ramu. "An efficient cloud framework for health care monitoring system." In Cloud and Services Computing (ISCOS), 2012 International Symposium on, pp. 113-117. IEEE, 2012.
[13] Parekh, Maulik, and B. Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis." Procedia Computer Science 50 (2015): 537–542.
[14] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684– 700.
[15] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78,(2018):964–975.
[16] Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguo Lian and Athanasios V. Vasilakos, A novel watermarking method for software protection in the cloud, SOFTWARE – PRACTICE AND EXPERIENCE, 42:409–430, 2012.
[17] https://www.yesser.gov.sa/en/Pages/default.aspx
[18] Huang, Jie, Mohamed Sharaf, and Chin-Tser Huang. "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud." In Parallel Processing Workshops (ICPPW), 2012 41st International Conference on, pp. 279–287. IEEE, 2012.
[19] Huang, Qinlong, Yixian Yang, and Mansuo Shen. "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing." Future Generation Computer Systems72 (2017): 239–249.
[20] Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98. Acm, 2006.