ISSN: 2348-2079

International Journal of Intellectual Advancements and Research in Engineering Computations (IJIAREC)

IJIAREC |Vol. 11 | Issue 4 | Oct - Dec -2023

www.ijiarec.com

DOI : https://doi.org/10.61096/ijiarec.v11.iss4.2023.18-22

Review

An Efficient And Secure Electronic Health Record Systems Using Block Authentication Code Mechanism

M. Bharathi[1], P.Sathya.,M.Tech[2]

[1]PG Students, Department of C.S.E, Sri Shanmugha College Of Engineering And Technology, [Salem], Tamilnadu, India.
[2]Assistant Professor,Departmentof C.S.E, Sri ShanmughaCollege Of Engineering And Technology, [Salem],Tamilnadu, India.

*Author for Correspondence: M. Bharathi
Email: yokeshshanmuga@gmail.com

Published on: 30 Dec 2023

Published by:
DrSriram Publications

Abstract

Electronic Health Record systems (EHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. Electronic Health Record systems (EHR) are increasingly being deployed within healthcare institutions to reduce the problems and limitations of the paper-based approach but its deployment has been slow due to high investment and maintenance cost. Cloud Computing has been widely recognized as the next generation's computing infrastructure and it offers several advantages to its users. In this study, an Enterprise Electronic Cloud-Based Health Record System was designed, implemented and tested for recording, retrieving, archiving and updating of patients and other medical records. The Cloud database acts as the unified data bank for all the collaborating hospitals, the middleware provides a common platform for all the EHR systems between remote hospitals while an authentication server grants access to authorized users and denies unauthorized users access to records or resources on the system. An e-web portal serves as the front end of the system and it links the application with the cloud. We Proposed Block Authentication Code Mechanism (BAC) techniques to encrypt each patient's EHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed

simultaneously by exploiting multi-authority EHR. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Keywords: Electronic Health Record systems (EHR), Block Authentication Code Mechanism (BAC).

INTRODUCTION

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization.

Cloud computing is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users.

For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

EXISTING SYSTEM

The cloud computing paradigm brings many benefits, there are many unavoidable security problems caused by its inherent characteristics such as the dynamic complexity of the cloud computing environment, the openness of the cloud platform and the high concentration of resources. One of the important problems is how to ensure the security of user data. Security problems, such as data security and privacy protection in cloud computing, have become serious obstacles which, if not appropriately addressed. Secure sharing of data plays an important role in cloud computing. Attribute-based access control can realize data confidentiality in the untrusted environment of server-end, fine-grained access control and large-scale dynamic authorization which are the difficult problems to solve the traditional access control.

DISADVANTAGES

Attribute-based access control can realize data confidentiality in the untrusted environment of server-end, fine-grained access control and large-scale dynamic authorization which are the difficult problems to solve the traditional access control.

PROPOSED SYSTEM

This project proposes a Block Authentication Code(BAC) Mechanism access control scheme with constant-size ciphertext that can realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing. The proposed scheme adopts BAC with constant ciphertextsize and maintains the size of ciphertext and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage, data transmission and computation. Second, we design

a hierarchical access control system. This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, we prove our scheme has indistinguishable security under an adaptive chosen ciphertext attack and we analyze the performance of our scheme.

Advantages

- Shows our scheme has good adaptability and scalability in cloud computing.
- Making the Block Authentication Code(BAC) simpler and more efficient along with making it evenmore suitable for access control in a cloud environment.

SYSTEM SPECIFICATION

The purpose of system requirement specification is to produce the specification analysis of the task and also to establish complete information about the requirement, behavior and other constraints such as functional performance and so on. The goal of system requirement specification is to completely specify the technical requirements for the product in a concise and unambiguous manner.

IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULES

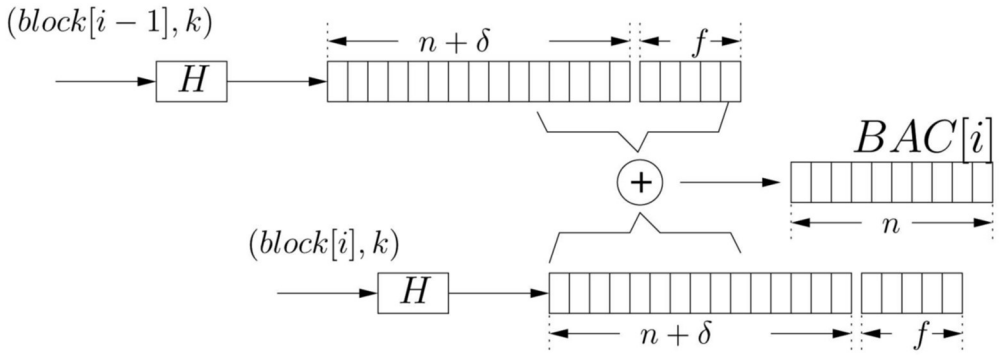
A module is a part of a program. Programs are composed of one or more independently developed modules that are not combined until the program is linked. A single module can contain one or several routines.

- Data Owners
- Users
- Key Authority
- Key Authentication
- Cloud Service Provider

METHOGOLOGY

It is the manager of cloud servers and also a semi-trusted entity which provides many services such as data storage, computation and transmission.

ALGORTHM
BAC(BLOCK AUTHENTICATION CODE)ALGORTHM



To present our scheme, we use the following notations

1. The stream packets are clustered to blocks, denoted as block[i], with b packets in each block, where 0 < i <$[total - packet - number/b]$. Padding is used when necessary to generate the last block.
2. The length (in terms of bits) of the BAC for each data block is n.
3. A hash function, denoted as H(X), is a one-way hash, using an algorithm such as MD5 or SHA.
4. X, Y represents the concatenation of X with Y.
5. A secret key k is only known to the communicating parties.
6. The origin of the data stream can be identified by a flag, which is f bits, where $0 \leq f \leq n$.

CONCLUSION

The proposed scheme adopts Block Authentication code Mechanism with constant-size ciphertext that solves the problem oftheciphertext size depending linearly on the number of attributes. Our scheme can maintain the size of ciphertext and the computation of encryption and decryption at a constant value. Therefore, the scheme can improve the efficiency of the system. We have performed some numerical simulation and the testing results are coincident with the theoretical analysis. In addition, we prove the scheme is of CCA2 security under the decision-al q-Bilinear Diffie-Hellman Exponent assumption. Final-ly, we also demonstrate an application model in a Hadoop distributed cloud environment. This shows our scheme has good adaptability and scalability in cloud computing. In further research, we intend to focus on making the Block Authentication Code (BAC) simpler and more efficient along with making it even more suitable for access control in a cloud environment.

REFERENCES

1. Vawdrey DK, Sundelin TL, Seamons KE, Knutson CD.Trust negotiation for authentication and authorization in healthcare information systems. Proceeding of 25th Annual International Conference IEEE;2003.doi: 10.1109/IEMBS.2003.1279579.
2. Shenai S, Aramudhan M.Cloud computing framework to securely share health and medical records among federations of healthcare information systems.BiomedRes.2018 [Special Issue:S133-6];2018. doi: 10.4066/biomedicalresearch.29-17-823.
3. Kester Q, Nana L, Pascu AC, Gire S, Eghan JM, Quaynor NN.'A cryptographic technique for security of medical images in health information system' Second International Symposium on Computer Vision and Internet (VisionNet'15): signalprocessing, Image processing and Pattern Recognition (SIPR'15), Procedia.ComputSci. 2015;58:538-43.
4. Haux R.Reinhold, Health information systems – past, present, future.IntJ MedInform. 2006;75(3-4):268-81. doi: 10.1016/j.ijmedinf.2005.08.002, PMID 16169771.
5. Centers for Medicare & Medicaid Services. Electronic healthrecords [definition];2016.Reterive.[accessed onJan 31, 2020].Available from:https://www.cms.gov/e healthrecords/.
6. Burk D."A Framework for SharingPersonalMedicalInformationSecurely and EfficientlyAcrossPublic/PrivateInstitutions".Cisco:Internet Business Solutions Group (IBSG);2010. Available from:http://tools.cisco.com.
7. Poissant L, Pereira J, Tamblyn R, Kawasumi Y.The impact of electronichealthrecords on timeefficiency of physicians and nurses: A systematicreview.J AmMedInformAssoc. 2005;12(5):505-16. doi: 10.1197/jamia.M1700, PMID 15905487.
8. Zhang J, Patel V.'Electronic Health Records – A Human Project',e-health and medicalITsolutions.Vols. 35-36;2006.
9. Harris T.'Cloud computing – An overview',white paper, TorryHarris Business Solutions;2010.
10. Huth A, Cebula J.'The basics of cloud computing'Carnegie Mellon University, Produced for US-CERT;2011.
11. Deng M, Nalin M, Schlehahn E, Abbadi I.'Trust model for cloud applications and first application architecture',Seventh Framework Programme, Technical report D3.1.1/1.0; 2010. p. 1-152.
12. Wang X.'Application of cloud computing in the health information system', Computer Application and System Modeling (ICCASM);2010.
13. Mirza H, El-Masri S.Cloud computing system for integrated electronic health records.British Computer SocietyHealth Level 7 (HL7); 2005.PHCSG.Available from: http://www.hl7.org/.

14. Cho I, Kim J, Kim JH, Kim HY, Kim Y.Design and implementation of a standards-based interoperable clinical decision support architecture in the context of the Korean EHR. IntJ MedInform. 2010;79(9):611-22. doi: 10.1016/j.ijmedinf.2010.06.002, PMID 20620098.
15. Saif S, Wani S, Khan S.A Network engineering solution for data sharing across healthcare providers and protecting patients' health data privacy using EHR System.J GlobRes ComputSci. 2010;2(8).