Proxy Re-Encryption Method for Secure Data Sharing In Blockchain Using Internet of Things

[1]Amutha.C, [2]K.Vijayprabakaran, [3]M.S. Sabari, [4]Dr.R.Umamaheswari
[1,2,3,4]*Department of Computer Science and Engineering, Gnanamani College of Technology,Namakkal*

ABSTRACT- The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. It uses proxy authorization and verification to upload medical data over cloud-based M-CPS. the best method is Advanced Encryption Standard method (AES). There are many types of AES that can be used but the most effective is AES-128. So, the aim of this study is to design image cryptographic application using the AES-128 method. Process of design applications with this method is through several stages, such as process of encryption, decryption, key generation and testing of the methods used. The attacks test is given by cropping, blurring, and enhancing the ciphertext image. To reduce the storage problem in Cloud we have split the image and file into different block and get stored, so storage problem get rectified. The proposed scheme needs to reduce the computation cost on the end-user as much as possible.

I. INTRODUCTION

With the rapid development of communication technology and computing power, people are facing increasing amounts of data. Maintaining this data requires large amounts of storage space and powerful computing power, which has become a challenge for DO. Fortunately, cloud computing technology has also evolved rapidly in the past few years to provide flexible computing and storage resources for DO. Therefore, more and more individuals/organizations tend to store their data in cloud server (CS) to reduce the overhead of local computing and storage resources. However, once DO deletes the local copies of the files after uploading the files to CS, he/she will not control the files. In this case, it's difficult for DO to confirm the integrity of outsourced data by using traditional data integrity checking schemes. In addition, due to the particularity of the cloud environment, CS is not only subject to malicious attacks from external adversaries, but also suffers from internal software errors or hardware failures. In these cases, DO's files are vulnerable to tampering, corruption, and loss. Besides, CS is an semi-trusted entity which may deliberately delete files that DO never or rarely accesses and conceals data errors caused by unexpected events. In summary, although cloud computing technology brings a lot of convenience, it also raises many security issues [3], [4]. Hence, many experts and scholars have made plenty of efforts to tackle these security problems.

II. LITERATURE SURVEY

In the current work, the infrastructure of the cyber-physical systems (CPS) are reviewed and discussed[4]. This article enriched the researches of the networked Medical Device (MD) systems to increase the efficiency and safety of the healthcare. It also can assist the specialists of medical device to overcome crucial issues related to medical devices, and the challenges facing the design of the medical device's network. The concept of the social networking and its security along with the concept of the wireless sensor networks (WSNs) are addressed.

Afterward, the CPS systems and platforms have been established, where more focus was directed toward CPS-based healthcare. The big data framework of CPSs is also included. Data collaboration in cloud computing is more and more popular nowadays, and proxy deployment schemes are employed to realize cross- cloud data collaboration[5]. However, data security and privacy are the most serious issues that would raise great concerns from users when they adopt cloud systems to handle data collaboration. Different cryptographic techniques are deployed in different cloud service providers, which makes cross-cloud data collaboration to be a deeper challenge.

In this paper, we propose an adaptive secure cross-cloud data collaboration scheme with identity-based cryptography (IBC) and proxy re-encryption (PRE) techniques. We first present a secure cross-cloud data collaboration framework, which protects data confidentiality with IBC technique and transfers the collaborated data in an encrypted form by deploying a proxy close to the clouds. We then provide an adaptive conditional PRE protocol with the designed full identity-based broadcast conditional PRE algorithm, which can achieve flexible and conditional data re- encryption among ciphertexts encrypted in identity-based encryption manner and ciphertexts encrypted in identity-based broadcast encryption manner. The extensive analysis and experimental evaluations

demonstrate the well security and performance of our scheme, which meets the secure data collaboration requirements in cross-cloud scenarios.

III. EXISTING SYSTEM

In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible.
The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users A proxy runs the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no idea of the data owner's secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data-sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties.

IV. PROPOSED SYSTEM

We measure the privacy disclosure of our scheme by the attacker's confidence in the success of an attack. Our proposed scheme, and show that the security and privacy goals have been achieved. Provided a proxy re-encryption functionality for cloud-data storage services. Unfortunately, this storage feature consumes more computation cost, and thus cannot be applied in the use of M-CPS. However, it consumes more computation costs for cloud-based M-CPS. the protection of the decryption key and reduces the burden on data owners. t the algorithm proposed by Ahn et al. can simultaneously ensure both efficiency and accuracy. Based on this algorithm, we present an efficient scheme. our proposed scheme obviously meets the security requirements. It protects the secrecy and privacy of data as well as the user's input query while simultaneously hiding data access patterns. the best method is Advanced Encryption Standard method (AES).

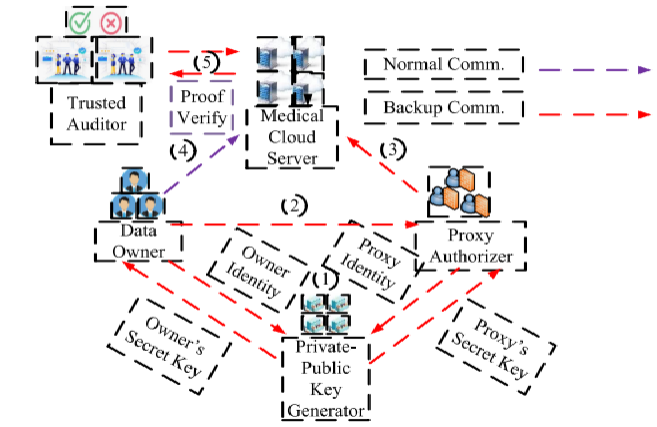

Fig 1 Proposed system

Software Model Waterfall Mode:
The Waterfall Model is a linear sequential flow. In which progress is seen as flowing steadily downwards (like a waterfall) through the phases of software implementation. This means that any phase in the development process begins only if the previous phase is complete. The waterfall approach does not define the process to go back to the previous phase to handle changes in requirement. In this article, we will discuss the advantages and disadvantages of the waterfall, should we avoid it? when to use it? and the waterfall model pitfall, and why I see it as the father of the SDLC models.
Waterfall Model Phases
Waterfall Model contains the main phases similarly to other process models, you can read this article for more information about phases definitions.

Use of Waterfall Model

Due to the nature of the waterfall model, it is hard to get back to the previous phase once completed. Although, this is can be very rigid in some software projects which need some flexibility, while, this model can be essential or the most suitable model for other software projects' contexts.

The usage of the waterfall model can fall under the projects which do not focus on changing the requirements, for example:

1. Projects initiated from a request for proposal (RFP), the customer has a very clear documented requirements
2. Mission Critical projects, for example, in a Space shuttle
3. Embedded systems.

We can notice some similarities of these types of projects that they cannot be delivered in iterative, incremental, or agile manner, for example, in embedded systems for the elevator, you cannot deliver an elevator who can go up only without going down, or handling only users requests from inside and ignore outside calls for the elevator.

Validation and Verification Model –V-Model

V-Model is mostly known as the validation and verification software development process model (The Vee Model), and It is one of the most know software development methodology. Although it is considered as an improvement to the waterfall model and it has some similarities as the process also based on sequential steps moving down in a linear way, it differs from the waterfall model as the steps move upwards after the coding phase to form the typical V shape. This V shape demonstrates the relationships between each phase of the development life cycle and its associated phase of testing. This means that any phase in the development process begins only if the previous phase is complete and has a correspondence related testing phase which is performed against this phase completion. Similar to the Waterfall model, the V- Model does not define the process to go back to the previous phase to handle changes in requirement.

The technical aspect of the project cycle is considered as a V shape starting with the business needs on the upper left and ending with the user acceptance testing on the upper right.

V-Model Model Phases

The V-Model Model contains the main phases similarly to other process models, you can read this article for more information about SDLC phases definitions. Moreover, it breaks down the testing phase into detailed steps to ensure the validation and verification process. So, it contains the below testing phases: Unit Testing The Unit testing is the testing at the code level and helps eliminate issues at an early stage, mainly the developer is responsible to perform the unit test for his code while not all the defects cannot be discovered at the unit testing.

Functional Testing

Functional testing is associated with the low-level design phase which ensures that collections of codes and units are working together probably to execute new function or service.

Integration Testing

Integration testing is associated with the high-level design phase. Integration testing ensures the integration between all system modules after adding any new functions or updates.

System Testing

System testing is associated with the system requirements and design phase. It combines the software, hardware, and the integration of this system with the other external systems.

User Acceptance Testing

User Acceptance testing is associated with the business and operations analysis phase. The customer users are the main performers of this testing based on test cases and scenarios that cover the business requirements to ensure that they have delivered the right software as per the specifications.

CLOUD COMPUTING :

Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user—it's just somewhere up in the nebulous "cloud" that the Internet represents.

DATA SECURITY

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and

privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements

Cloud computing can be considered as a new computing archetype that can provide services on demand at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities.

CLOUD SERVICES

Cloud computing will enable services to be consumed easily on demand. Cloud computing has the characteristics such as on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. These merits of cloud computing have attracted substantial interests from both the industrial world and the academic research world. Cloud computing technology is currently changing the way to do business in the world.Data security has consistently been a major issue in IT.

Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks

Data Confidentiality

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness .

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

Hybrid Technique

A hybrid technique is proposed for data confidentiality and integrity , which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

Data Availability

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively. Privacy has the following elements.

VI. CONCLUSION

In this project propose to define a specialized access policy for each data attribute in the Company, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute. To preserve the access pattern of the data attributes in the, we construct a blind data retrieving protocol based on the Paillier encryption. provides the encryption module for the re-encryption and also time privileges for accessing particular file. we present a blockchain-based system model that allows for flexible authorization on encrypted data.When the pixel value of the encrypted image is changed, the decryption process have been successful, but it cannot restore the plaintext imagewe presented a secure and efficient scheme to locate the exact nearest neighbor over encrypted medical images stored.To over come storage problem we split storage space into different way we have created multiple folders. The Advanced Encryption Standard (AES) algorithm was successfully applied to encrypt an image. In the decryption process, this method can restore plaintext as clear as before. Attack test is given on the ciphertext by cropping, blurring, and enhancing. It is found that this method can recognize plaintext clearly for cropping attacks. The performance of our scheme is evaluated using real-world medical images.

REFERENCES

[1] B.Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino, ''Materials, structures, mechanical systems, and manufacturing roadmap,'' NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.

[2] H. Laaki, Y. Miche, and K. Tammi, ''Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,'' IEEE Access, vol. 7, pp. 20325–20336, 2019.

[3] H. Wang and J. Zhang, ''Blockchain based data integrity verification for large-scale IoT data,'' IEEE Access, vol. 7, pp. 164996–165006, 2019.

[4] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[5] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[7] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[8] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[10] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[11] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[12] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[13] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[14] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[15] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ''Blockchain data-based cloud data integrity protection mechanism,'' Future Gener. Comput. Syst., vol. 102, pp. 902–911, Jan. 2020.

[16] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, ''Blockchain based data integrity service framework for IoT data,'' in Proc. IEEE Int. Conf. Web Services (ICWS), Jun. 2017, pp. 468–475.

[17] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, ''On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain,'' IEEE Access, vol. 10, pp. 75365–75375, 2022.

[18] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, ''An enhanced pairing-based authentication scheme for smart grid communications,'' J. Ambient Intell. Humanized Comput., vol. 2021, pp. 1–13, Jan. 2021.

[19] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, ''Privacypreserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment,'' IEEE Access, vol. 7, pp.

[20] A. Sengupta, A. Singh, P. Kumar, and T. Dhar, ''A secure and improved two factor authentication scheme using elliptic curve and bilinear pairing for cyber physical systems,''

[21] H. S. Grover and D. Kumar, ''Cryptanalysis and improvement of a threefactor user authentication scheme for smart grid environment,'' J. Reliable Intell. Environ., vol. 6, no. 4, pp. 249–260, Dec. 2020.