A Proxy Re-Encryption Approach to Secure Data Sharing the Internet of Things Based on Blockchain

Anbuvizhli[1], Raja Rajan L[2], Ragul A[3], Noor Mohamed[4]
[1]Assistant professor, Dept of Information Technology
[2, 3, 4]Dept of Information Technology
[1, 2, 3, 4] Jeppiaar Engineering College,

Abstract- *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. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations.*

Keywords- Access control, blockchain, data security, identity-based proxy re-encryption, information-centric network (ICN), Internet of Things (IoT).

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposesin applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others [1]. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data.

A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. 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.

II. PROPOSED SYSTEM

This system proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology.

In the proposed system, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. We propose a secure access control framework to realize data confidentiality, and fine-grained access to data is achieved. This will also guarantee data owners' complete control over their data.

We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.

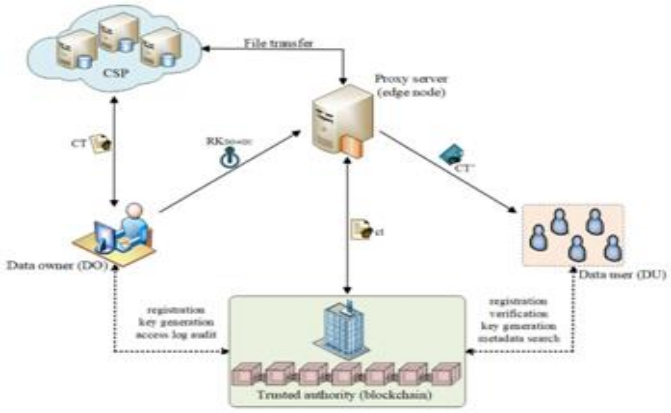
In the proposed system, the data is divided into 3 different blocks and stored in the cloud for the enhanced security model and then the proxy re-encryption approach is made for securing the data in the cloud.

PRE, together with IBE and the features of ICN and blockchain, will enhance security and privacy in data-sharing systems.

PREand IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data.

The blockchain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network.

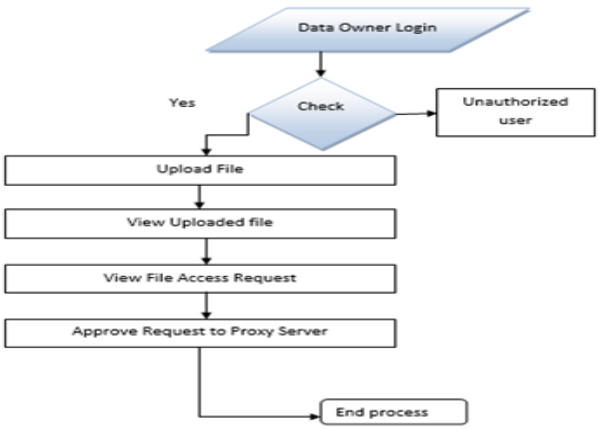
III. ARCHITECTURE DIAGRAM



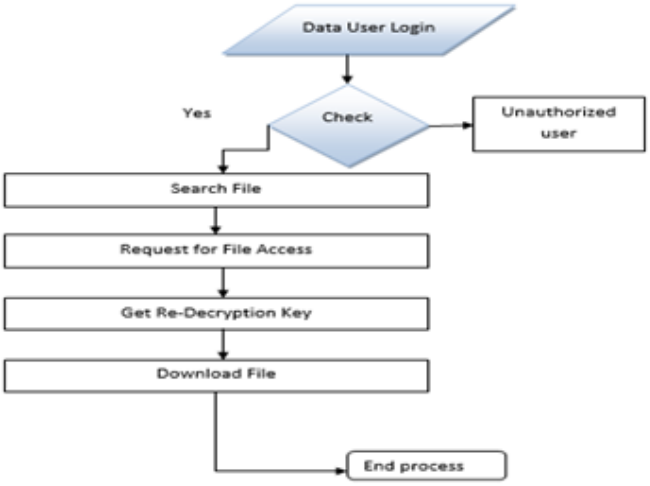
IV. DATA FLOW DIAGRAM

- Data Flow Diagram- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

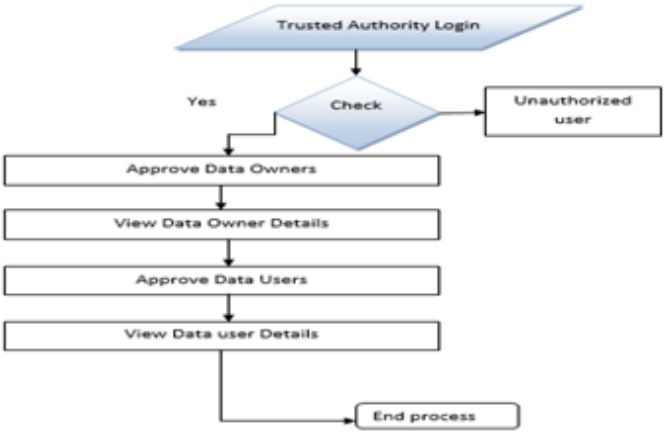
Data Owner:



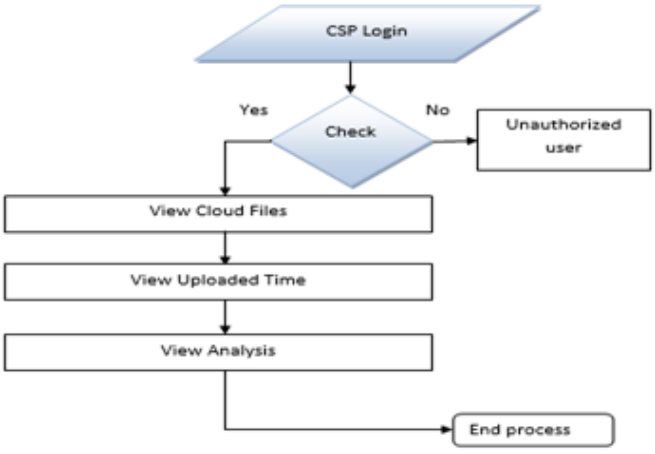
Data User:



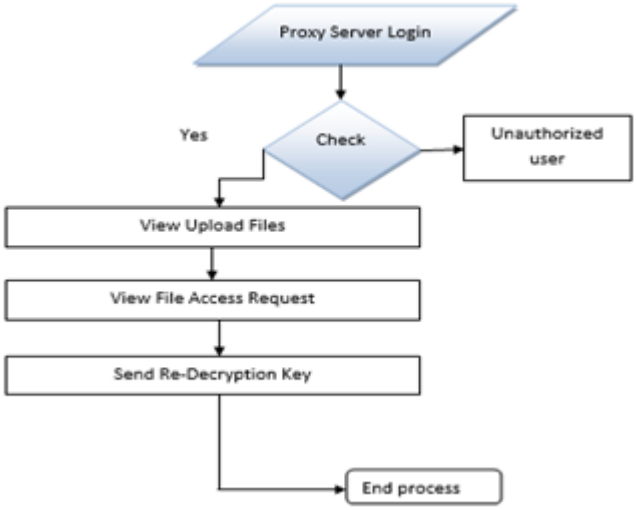
Trusted Authority:



CSP:



Proxy Server:



V. UML DIAGRAMS

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

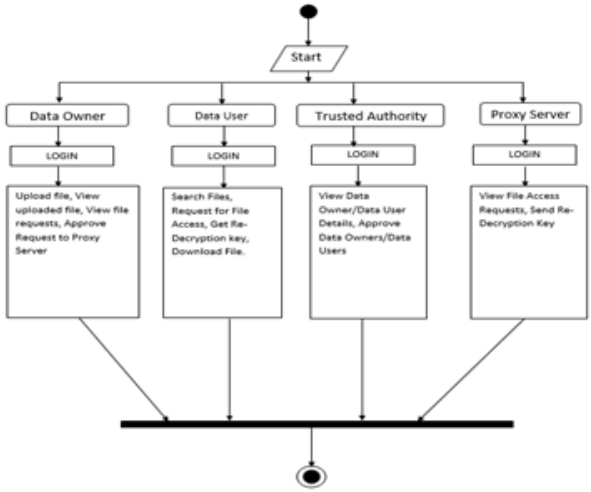
GOALS:

The Primary goals in the design of the UML are as follows:

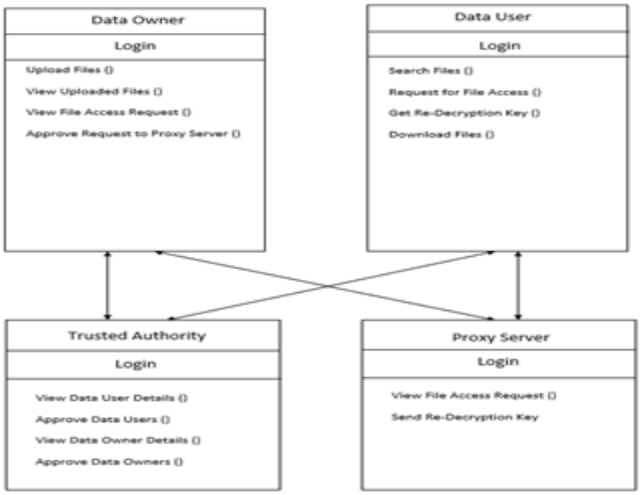
1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM

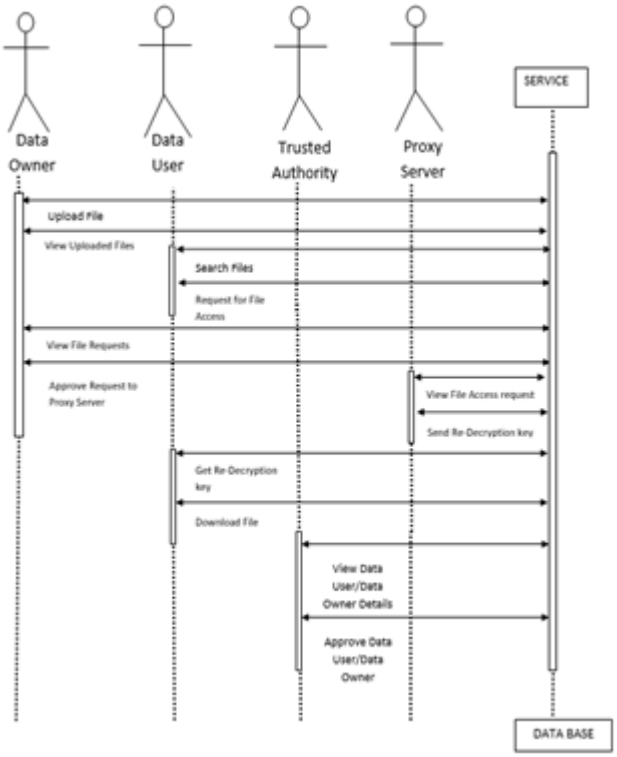
CLASS DIAGRAM



SEQUENCE DIAGRAM



ACTIVITY DIAGRAM:



HARDWARE REQUIREMENTS

- System : Pentium i3 Processor
- Hard Disk : 500 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 2 GB

SOFTWARE REQUIREMENTS

- Operating system : Windows 10.
- Coding Language : JAVA.
- Tool : NetBeans 8.2
- Database : MYSQL

VI. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, we propose a secure identity-based PRE-data-sharing scheme in a cloud computing environment. Secure data sharing is realized with IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations. The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth. Then, we present a blockchain-based system model that allows for flexible authorization on encrypted data. Fine-grained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing scheme.

REFERENCES

[1] Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, and Jianbin Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain", IEEE SYSTEMS JOURNAL, VOL. 16, NO. 1, MARCH 2022.

[2] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.

[3] T. Koponen et al., "A data-oriented (and beyond) network architecture," in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181–192.

[4] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to pursuit," in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13.

[5] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops,2010, pp. 1–6.

[6] Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.