



A PROXY RE-ENCRYPTION APPROACH TO SECURE DATA SHARING IN CLOUD FOR DATA SECURITY

TANETI JAYA DARSHAN

Master of Computer Applications (MCA),
Dr. K.S Raju Arts & Science College(A),
Penugonda, W.G.Dt., A.P, India

B.N.S. GUPTA

Associate Professor in Computer Science,
SVKP & Dr. K.S Raju Arts & Science College(A),
Penugonda, W.G.Dt., A.P, India

Abstract: As the Internet of Things has grown, data sharing has become one of the most beneficial cloud computing applications. Even though this technology has a pleasing aesthetic, data security is still one of its difficulties because inappropriate data utilization might have a number of unfavorable impacts. In this research, we present a proxy re-encryption technique for secure data transfer in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, and authorized users can access the data through proxy re-encryption construction. Because Internet of Things devices have limited resources, an edge device acts as a proxy server to conduct computationally intensive tasks. Additionally, by utilizing information-centric networking capabilities, we successfully distribute cached content through the proxy, hence boosting the quality of service and effectively utilising the network capacity. It accomplishes fine-grained data access control and lessens centralised system bottlenecks. Our strategy for ensuring data security, confidentiality, and integrity has the potential, as shown by the security study and plan review.

1. 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 purposes in 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. 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.

Although simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. Proxy re-encryption (PRE), a notion first proposed by Blaze *et al.* [2], allows a proxy to transform a file computed under a delegator's public key into an encryption intended for a delegatee. Let the data owner be the delegator and the data user be the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a trusted third party generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the cipher text before sending the new cipher text 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. Data disclosures can be minimized through the use of encryption since only users delegated by the data owner can effectively access the outsourced data.

2. LITERATURE SURVEY

A. PRE Data Sharing

Yu et al. [15] combined key-policy ABE (KP-ABE) and PRE to propose a system for data sharing in the cloud. The data was encrypted using KP-ABE which meant that only an appropriate collection of the attribute secret keys can make decryption possible. Besides the encrypted data, the cloud also managed all attribute secret keys except one special secret key in order to handle revocation of users. When users are revoked, new keys were distributed to the remaining users by the data owner and the encrypted data had to be re-encrypted. Although the scheme was efficient, the re-encryption was performed in a lazy way, and, therefore, the security of the scheme was weakened. Park [16] provided a modification to the scheme in [15], where collusion between the service provider and revoked users is avoided. Their scheme was to basically replace the service provider with a trusted third party, which implies that there should be reliance on stronger trust assumption. Other schemes [17]–[19] have made similar approaches but utilized ciphertext-policy ABE (CP-ABE) rather, in which the access policy is associated with the ciphertext instead of the secret keys. Liu et al. [20] also proposed a time-constrained access control scheme based on PRE and ABE. ABE was used to design time-based access control policies while PRE was used to update the time attributes. Although these schemes have their advantages, they are not suitable in the context of IoT due to the heavy computations on encryption and decryption.

B. Blockchain-Based Access Control and Data Sharing

Zyskind et al. [27] used blockchain to provide distributed personal data management and ensure privacy as well. The blockchain was utilized as an automatic access control manager, and, hence, no third party was required. Only the data address was stored on the blockchain

and a distributed hash table was used as the implementation of the data storage. This reduced the risk of data leakage. However, no specific access control model was proposed in their scheme. Maesa et al. [28] proposed a blockchain-based access control scheme where the data owner defines policies on the data and stores them on the blockchain. The policies are then assigned to the users as access rights.

C. Access Control Schemes for ICN

In order to control content in ICN frameworks, several centralized and decentralized access control mechanisms have been proposed in literature. Silva and Zorzo [31] presented an access control system for named data networking which relied on an ABE scheme and a proxy server. Before a content is published, the data owner encrypts the content and generates an access policy that binds it. The encrypted data is stored in the immediate routers while the access policy is stored on the server. When a user wants to access content, the user retrieves the content from the router, obtains the access policy from the proxy server, and then decrypts the data. Their scheme enables user revocation; however, it suffers from a single point of failure if a proxy server fails to work because the proxy server takes part in each content access. Li et al. [32] designed a privacy enhancing scheme using ABE for access control in ICN, and a trusted third party is deployed to manage attributes. A content publisher generates an access policy based on the attributes defined by the third party and uses a random symmetric key to encrypt the data. The publisher then hides the random key and the access policy in the content name and only authorized users can gain access to the content. The proposed scheme achieves privacy by hiding the access policy in the content name, but user revocation is not guaranteed.

3. EXISTING SYSTEM

Park [16] provided a modification to the scheme in [15], where collusion between the service provider and revoked users is avoided. Their scheme was to basically replace the service provider with a trusted third party, which implies that there should be reliance on stronger trust assumption. Other schemes [17]–[19] have made similar approaches but utilized ciphertext-policy ABE (CP-ABE) rather, in which the access policy is associated with the ciphertext instead of the secret keys. Liu *et al.* [20] also proposed a time-constrained access control scheme based on PRE and ABE. ABE was used to design time-based access control policies while PRE was used to update the time attributes. Although these schemes have their advantages, they are not suitable in the context of IoT due to the heavy computations on encryption and decryption.

An IBE PRE scheme suitable for data sharing was presented by Han *et al.* in [21]. The re-encryption keys were not only bound to the users' identities but also to a specific ciphertext. This implied that the data owner had to create a different reencryption key for each pair of data user and shared file. A similar idea was proposed by Lin *et al.* [22] where they used a hierarchical PRE instead of an identity-based PRE. These two schemes tend to be inefficient when multiple and complex data pieces are considered. An identity-based broadcast encryption (IBBE) combined with PRE was proposed by Zhou *et al.* in [23] for data sharing. Their scheme was a hybrid one that allowed the conversion to be done between the two protocols without leaking any sensitive information. Wang *et al.* [24] also designed an identity-based PRE (IBPRE) scheme for accessing health records. The scheme achieved coarse-grained access control.

If a proxy receives the re-encryption key from the data owner, either all the ciphertexts can be re-encrypted and accessible to the intended users or none at all. On that note, Shao *et al.* [25] proposed an IBEPRE scheme that is based on conditions. In their proposal, the proxy could transform a subset of ciphertexts under an identity to other ciphertexts under another identity. However, decryption rights to a group of users could not be authorized. In addition to the above, PRE has been used to mitigate security problems in IoT [26].

Zyskind *et al.* [27] used blockchain to provide distributed personal data management and ensure privacy as well. The blockchain was utilized as an automatic access control manager, and, hence, no third party was required. Only the data address was stored on the blockchain and a distributed hash table was used as the implementation of the data storage. This reduced the risk of data leakage.

Fan *et al.* [29] designed a similar model to [28] where the encrypted data is uploaded to the cloud and access policies on the data are stored on the blockchain as transactions. Although these two schemes achieve tamper-proof systems and easy auditing, there is a leakage of access policies since the blockchains used are public ones and are thus visible to everyone. Singh and Kim [30] presented a blockchain-based model for sharing data in vehicular networks and also enable secure communication among vehicles. However, the use of a public blockchain does not work well in peer-to-peer (P2P) data sharing among vehicles due to the high cost involved in establishing a public blockchain in resource-constrained vehicles.

Disadvantages

- 1) The system was not implemented Attribute Based Encryption Method which leads less security on outsourced data.
- 2) The system is less security due to lack of Identity-Based Encryption.

4. PROPOSED SYSTEM

The system proposes a secure access control framework to realize data confidentiality, and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data.

The system gives a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.

To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking.

The security analysis of our scheme is presented, and we also test and compare its performance with existing schemes.

Advantages

- 1) The proposed system is secure against man-in-the-middle (MITM) attacks. MITM attacks get to the certificate authority (CA) to provide the user with forged public keys.
- 2) The proposed system finds Data Tampering and blocks when hackers compromise a system, they inject their own versions of the data into the system.

5. SYSTEM DESIGN

The importance can be stated with a single word “Quality”. Design is the place where quality is fostered in software development. Design provides us with representations of software that can assess for quality. Design is the only way that we can accurately translate a customer’s view into a finished software product or system. Software design serves as a foundation for all the software engineering. Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area of application. Design is the first step in the development phase for any engineered product or system. The designer’s goal is to produce a model or representation of an entity that will later be built. Beginning, once system requirements have been specified and analyzed, system design is the first of the three technical activities -design, code and test that is required to build and verify software.

Without a strong design we risk building an unstable system – one that will be difficult to test, one whose quality cannot be assessed until the last stage.

During design, progressive refinement of data structure, program structure, and procedural details are developed, reviewed and documented. System design can be viewed from either technical or project management perspective. From the technical point of view, design is comprised of four activities – architectural design, data structure design, interface design and procedural design.

5.2 UML DIAGRAMS

The Unified Modeling Language (UML) is used to specify, visualize, modify, construct and document the artifacts of an object-oriented software intensive system under development. UML offers a standard way to visualize a system's architectural blueprints, including elements such as:

- Actors
- Business processes
- (logical) components
- Activities
- programming language statements
- database schemas, and
- Reusable software components.

USE CASE DIAGRAM

A Use Case Model describes the proposed functionality of a new system. A Use Case represents a discrete unit of interaction between a user (human or machine) and the system. This interaction is a single unit of meaningful work, such as Create Account or View Account Details.

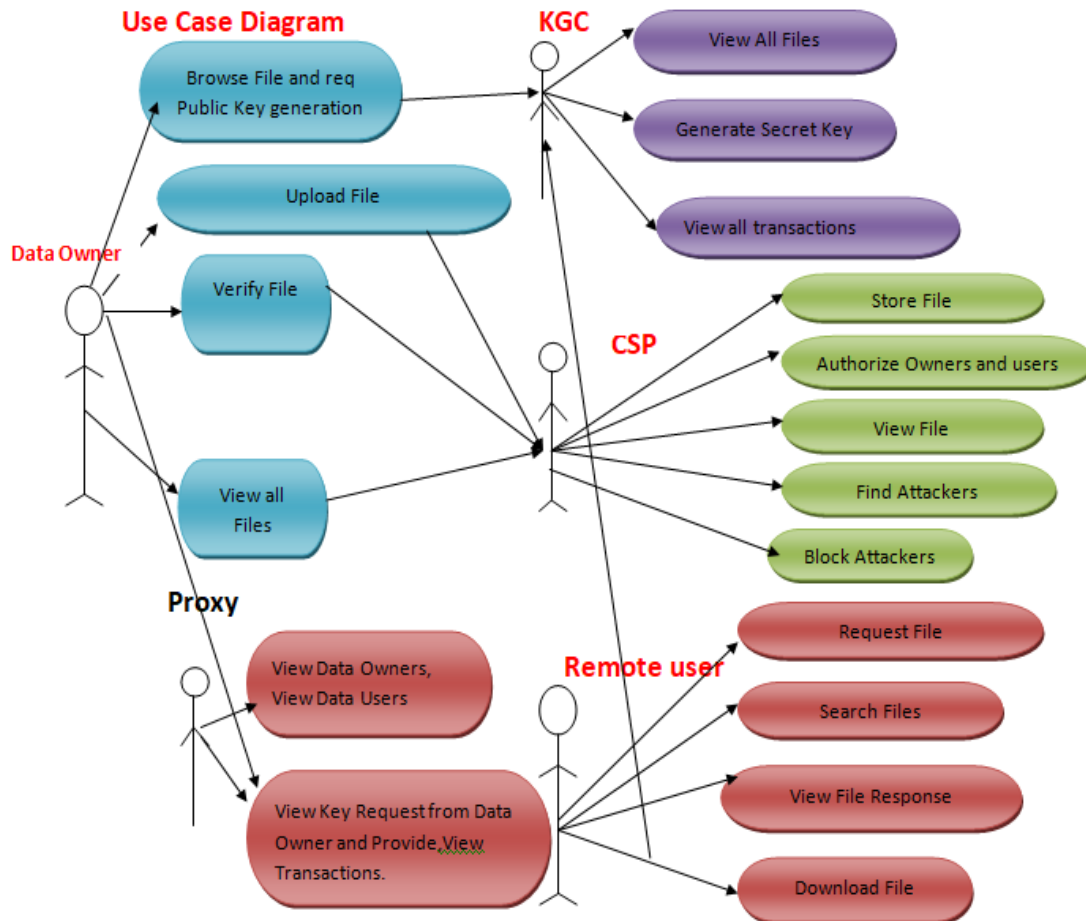
Each Use Case describes the functionality to be built in the proposed system, which can include another Use Case's functionality or extend another Use Case with its own behavior.

Use-Case diagram

A use case illustrates a unit of functionality provided by the system. The main purpose of the use-case diagram is to help development teams visualize the functional requirements of a system,

including the relationship of "actors" (human beings who will interact with the system) to essential processes, as well as the relationships among different use cases.

Use-case diagrams generally show groups of use cases — either all use cases for the complete system, or a breakout of a particular group of use cases with related functionality (e.g., all security administration-related use cases).



6. IMPLEMENTATION

Implementation is the process of converting a new or revised system design into operational one. There are three types of Implementation:

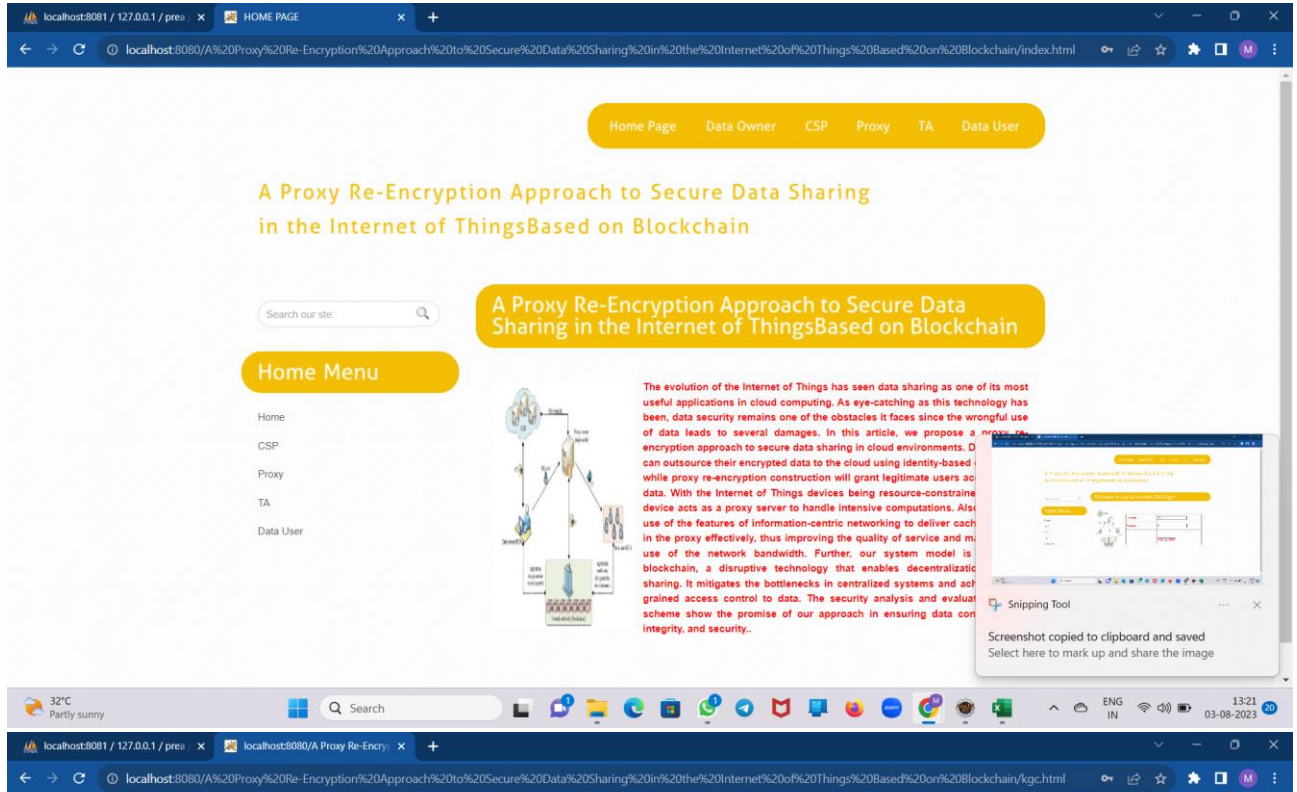
Implementation of a computer system to replace a manual system. The problems encountered are converting files, training users, and verifying printouts for integrity.

Implementation of a new computer system to replace an existing one. This is usually a difficult conversion. If not properly planned there can be many problems.

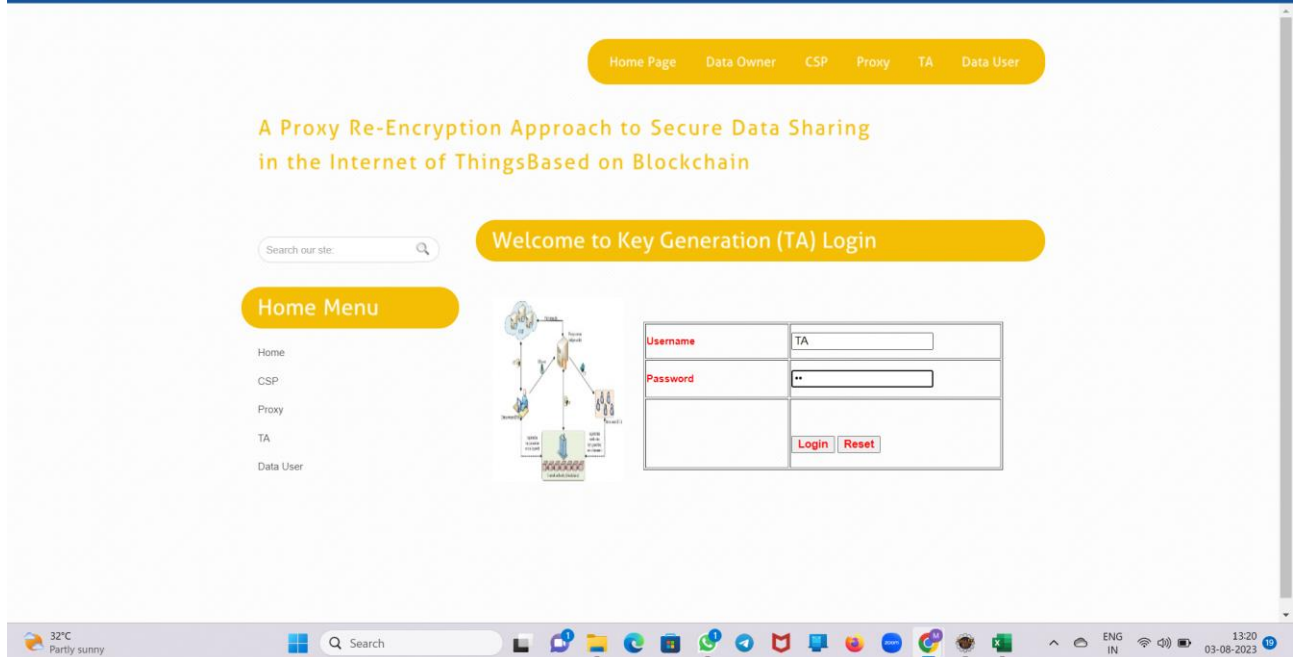
Implementation of a modified application to replace an existing one using the same computer. This type of conversion is relatively easy to handle, provided there are no major changes in the files.

Implementation in Generic tool project is done in all modules. In the first module User level identification is done. In this module every user is identified whether they are genuine one or not to access the database and also generates the session for the user. Illegal use of any form is strictly avoided.

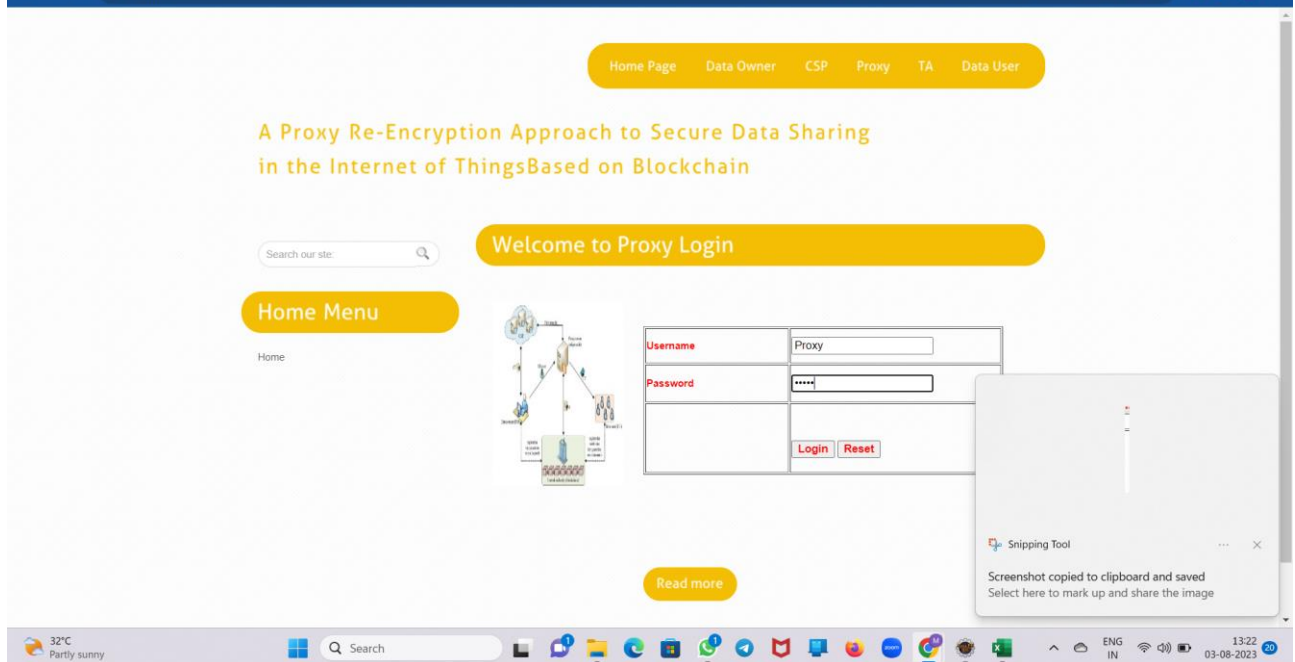
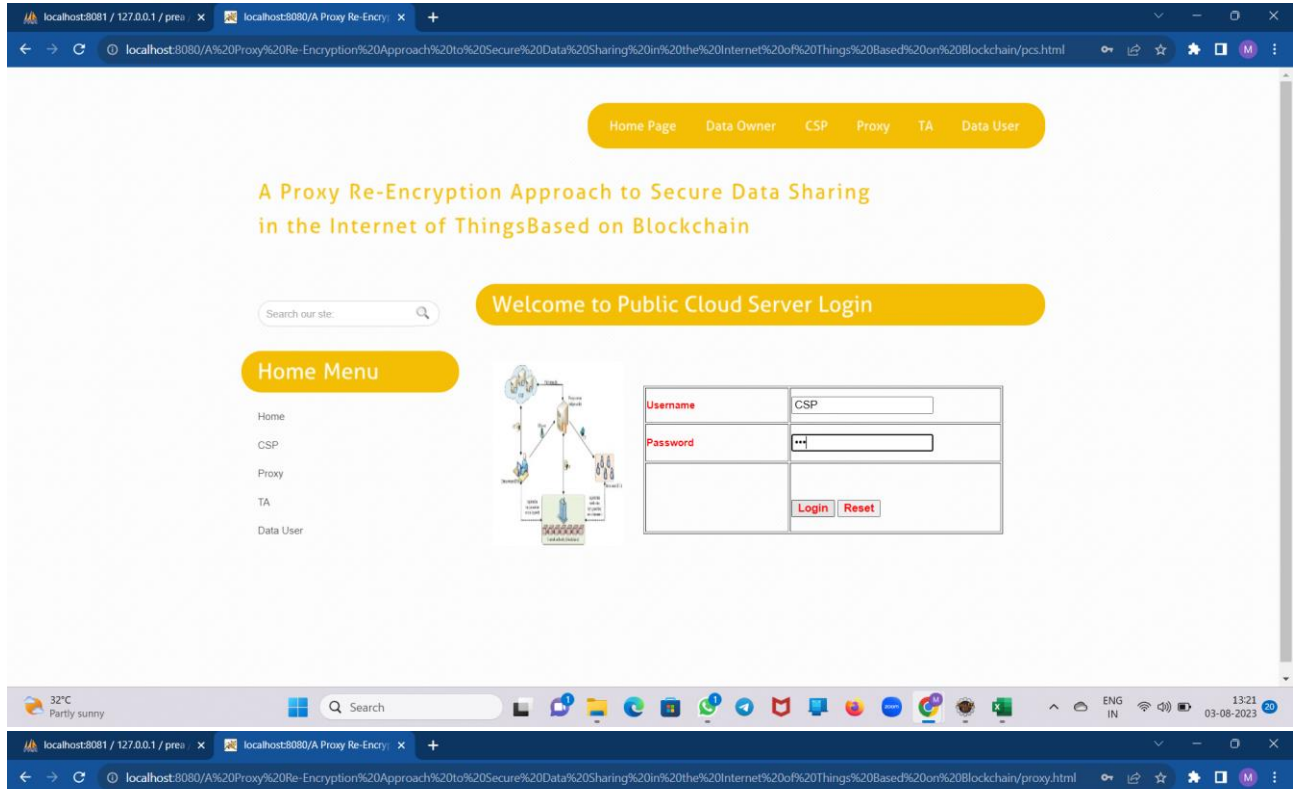
SCREENS



The screenshot shows the application's home page. At the top, there is a navigation bar with links for Home Page, Data Owner, CSP, Proxy, TA, and Data User. The main heading is "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of ThingsBased on Blockchain". Below this, there is a search bar and a "Home Menu" section with links to Home, CSP, Proxy, TA, and Data User. A central text block describes the evolution of the Internet of Things and the challenges of data security, followed by a diagram of the system architecture. A "Snipping Tool" notification is visible in the bottom right corner.



The screenshot shows the application's TA login page. The navigation bar and main heading are identical to the home page. The central text block says "Welcome to Key Generation (TA) Login". Below this, there is a "Home Menu" section with links to Home, CSP, Proxy, TA, and Data User. A central diagram of the system architecture is shown. To the right of the diagram is a login form with fields for Username (containing "TA") and Password (masked with asterisks), and buttons for "Login" and "Reset".



7. CONCLUSION AND FUTURE ENHANCEMENT

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. Finegrained 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 schemes

8. BIBLIOGRAPHY

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tut.*, vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.
- [2] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, May 1998, pp. 127–144.
- [3] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, Springer, Aug. 1984, pp. 47–53.
- [4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Springer, May 2004, pp. 506–522.
- [5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in *NDSS*, vol. 4. Citeseer, Feb. 2004, pp. 5–6.
- [6] D. Balfanz et al., "Secret handshakes from pairing-based key agreements," in *Proc. IEEE, Symp. Secur. Privacy*, 2003, pp. 180–196.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.