IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 404-408

DOI: 10.17148/IARJSET.2023.10756

Electronic Encryption

Yashaswini Y[1], Sharath K[2]

Student, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[2]

Abstract: Data sharing has emerged as one of Internet of Things' most advantageous cloud computing applications as it has developed. Even if the evolution of technology has been visually appealing, data security is still one of its challenges because improper usage of data can result in a variety of negative effects. We provide a proxy re-encryption method in this paper for safe data exchange in cloud contexts. Identity-based encryption enables data owners to outsource their protected information to the cloud, while proxy reset encryption construction allows authorized users to access the data. Due to the limited resources of Internet of Things devices, an edge device serves as an intermediary in order to handle demanding calculations.

Additionally, we successfully distribute cached material in the proxy by using information-centric networking capabilities, hence enhancing the quality of service by making efficient use of the network capacity. Additionally, the foundation of our system concept is blockchain, a ground-breaking technology that permits decentralised data sharing. It achieves very fine regulation of access to data and reduces inefficiencies in centralised systems. The security study along with the assessment of our plan demonstrate the potential of our strategy for guaranteeing data security, confidentiality, and integrity

Keywords: security,integrity, ground breaking technology.

I. INTRODUCTION

Information security as it relates to networked devices is referred to as computer security, sometimes known as digital safety or IT security. The field includes all procedures and systems used to guard against unauthorised or unintentional access to, alteration of, or destruction of computer-based tools, data, and services. Security for computers also includes defence against unforeseen circumstances like natural calamities. Aside from that, in the computer sector, the term security -- or the phrase "computer security" -- refers to methods used to make sure that data stored in computers cannot be viewed or compromised by anybody without authorisation. Data encryption and keys are used in the majority of computer security procedures.

Your work computer and all information stored on it are at risk because you don't take simple precautions to protect them. You might endanger the functionality of other computers connected to the network of your company, or possibly the company as a whole.

A. Technical security measures, such as anti-virus software and login passwords, are crucial. (More on those items below) However, the first and most crucial line of defence is a safe physical environment.

Is the location where you maintain your work computer safe enough to guard against theft or unauthorised access while while you're away? Even though the Medical Centre is covered by the Security Department, it just takes a few seconds to steal a personal computer, especially a portable one like a laptop or PDA. When you are not around, your gadget should be protected just like any other important item.

Threats from humans are not the sole issue. The environment (such as water or coffee) or physical stress can impair computers.Credentials for login (user-IDs and passwords) are a part of the protection for the University's networked and shared information systems. In most cases, access usernames are a crucial component of personal computer security. Since offices are typically open, communal spaces, it is difficult to completely monitor who has physical access to which computers.

If the software allows it, you should think about creating passwords for any particularly sensitive programmes installed on your computer (such as data analysis software) in order to secure it.

II. LITERATURE SURVEY

An analysis of underlying technologies, protocols, and applications for the Internet of Things[1]

The worldwide Web of Things (IoT) is discussed in general terms in this paper, with a focus on enabling technology, protocols, and application-related challenges. The most recent advancements in RFID, a technology digital sensors, wireless communication, and Internet protocols enable the Internet of Things. The fundamental idea is to create a new class of gadgets by having smart sensors work together directly without human intervention. The present Internet, mobile,

ISO 3297:2007 Certified

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 404-408

DOI: 10.17148/IARJSET.2023.10756

and machine-to-machine (M2M) technology boom can be viewed as the beginning of the Internet of Things. The Internet of Things (IoT) is anticipated to connect physical things to enhance intelligent decision-making in the next years, bridging various technologies to open up new application

The use of atomic proxy cryptography and flexible protocols[2]In contrast to the pre-existing notion, which is a linguistic feature (see Okamoto, Ohta [OO90]), we first introduce an idea of divertibility as a protocol attribute. In the context of interactive zero-knowledge proofs, we provide a description of protocol divertibility that is applicable to any two-party protocol and is consistent with Okamoto and Ohta's concept. Blind signature techniques are another significant example that fits the new criteria. We put forth a divertibility sufficiency criterion that many existing protocols already meet and which, surprisingly, generalises to include numerous protocols that aren't often associated with divertibility (like Diffie-Hellman key exchange).

Identity-based encryption technologies and signature protocols[3] We offer a novel sort of cryptographic system in this work that allows any set of users to exchange information effectively and to verify each other's signatures without exchanging either their public or private keys, without maintaining key directory listings, and without enlisting the help of a third party. The plan presupposes the presence of trusted key extraction facilities, whose primary function is to issue each user a unique smart card upon their initial network enrollment. Regardless of who the other party is, the user is able to sign and encrypt messages that are sent as well as decode and verify messages that are received using the information encoded in this card.

Key search for public key encryption

[4]We research the issue of searching encrypted data using a common key scheme. Think about user Bob sending user Alice an email that is encrypted with Alice's public key. Whether the email message contains the word "urgent" will be checked by an email gateway so that the communication can be forwarded appropriately. Alice, upon the other hand, is unwilling to let the gateway access to all of her messages' encryption keys. Without discovering anything additional about the email, we develop and build a system that enables Alice to give the gateway a key that enables the gateway to check whether the term "urgent" is a keyword in the email. This system is known as public key encryption.

constructing a searchable, encrypted audit log[5] Any safe system must include audit logs, which must be thoughtfully created in order to accurately reflect previous system activity. This is particularly true if there are enemies around who might try to manipulate with the scrutiny logs. Although it is crucial that auditors have access to audit logs so they can evaluate previous system activity, the information contained in an audit log may be sensitive and should be kept secure from unauthorised access.

Problem: Authorised auditors must be able to efficiently examine audit log contents while keeping them secure from unauthorised parties (by encrypting them).

III. EXISTING WORK

The idea of proxy re-encryption (PRE), first put out by Blaze et al., enables a proxy to convert a file computed using a delegator's public key onto an encryption meant for a delegatee. Let the user of the data be the delegate and the owner of the data be the delegator. In such a plan, the data owner is able to give the user temporary encrypted messages without disclosing his secret key.

The re-encryption key is created by the data owner or a reliable third party. Before providing the updated ciphertext to the user, a proxy does the re-encryption algorithm employing the key. Because it is unaware of the data owner's secret key, the proxy in a PRE scheme cannot be entirely trusted. This is viewed as the best option for securely granting others access to encrypted data, which is essential in any scenario involving data sharing.

The previous system's significant decryption overhead is a drawback. Since thin devices in the IoT ecosystem have various limitations, including computational resource, battery life, and bandwidth cost, ABE cannot be directly used to healthcare IoT networks.

Traditional encryption techniques need intricate key management mechanisms, making them inappropriate for data sharing.

In the current system as well, the re-encryption was carried out inefficiently, which reduced the scheme's security.

Due to the complex computations involved in encryption and decryption, they are not appropriate for use in the IoT context.

IV. PROPOSED METHODOLOGY

By combining Por with security based on identity (IBE), information-centric routing (ICN), and blockchain technology, this method suggests an improvement in IoT data exchange.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 404-408

DOI: 10.17148/IARJSET.2023.10756

 The data possessor extends an access control list that is kept on the blockchain in the proposed system. The data is only accessible to authorised users. To achieve data security and very fine access to data, we provide a safe access control system. Additionally, this will ensure that data owners have total authority regarding their data.
 We provide a thorough explanation of our PRE system and the implementation of a comprehensive protocol that ensures data security and privacy.
 For the suggested system's increased security model, the data is split into three separate units and maintained in the cloud. Next, a proxy re-encryption strategy is developed to protect the data in the online.

PRE will improve security and private in data-sharing systems along with IBE, ICN, and blockchain technologies.
PRE and IBE will guarantee very fine, data access control, yet the idea of ICN assures a suitable level of service for data delivery since in-network caching enables effective data distribution.
The blockchain is designed to minimise storage and data-sharing costs and to promote trust among network participants.

V. IMPLEMENTATION

A. Trusted Authority

The organisation that authorises a new data Provider or data user in the system is acknowledged as the trusted authority. The trustworthy authority (TA) that starts the system parameters is the blockchain. Additionally, the TA offers secret keys that are linked to the identities of the users. Utilising this distributed ledger improves the security plus privacy of data by achieving authenticity, candour, and verifiability inside the network. Owners of data can properly manage their data as a result. The data owner(s) as user(s) are registered on the blockchain network, and membership keys are distributed to them. The owner creates a re-encryption key using the user's identity and transmits it to the proxy server whenever a user wants access to data.

B. Data Owner

Users who are in possession of confidential communication and want to safely distribute them are represented by the Data Owner module. Using cryptographic techniques and the relevant keys obtained from the KGC, the Info Owner encrypts the messages. The ciphertexts—also referred to as encrypted messages—are subsequently uploaded onto a the cloud A server (CS) for distribution and storage. Data Owners (DOs) are a group of individuals who have uploaded private messages to CS in order to distribute them securely to DUs.

C. Data user

Individuals with permission and proper authorization obtained from the KGC are considered Data Users. Each Data User aims to securely access and decrypt the encrypted text despite having constrained resources for data storage and computing. The Data User asks the CS for the encrypted data and the ES for the required transformation keys. The Data User executes the decryption process using these keys, which depending on the security measures strategy employed may include partial or full decryption. To maintain data security, data users must make sure they have the proper authorizations and adhere to the decryption procedure.

D. Proxy Server

The Proxy server is implemented in this module. Using his own public key, a user can encrypt a file using proxy re-encryption, and the ciphertext is subsequently stored on a trustworthy yet untrustworthy server. When the recipient is chosen, the sender can designate the server to serve as a proxy for a re-encryption key related to the recipient. The initial ciphertext is then re-encrypted by the proxy and sent to the appropriate recipient. Finally, the recipient can use her private key to decrypt the generated ciphertext. The security of PRE typically ensures that (1) no the server/proxy nor unintended recipients may discover any valuable data about the (re-)encrypted file and (2) the proxy cannot meaningfully reconfigure the encryption the initial ciphertext before obtaining the re-encryption key.

E. CSP

We create Cloud Service Providers (CSP) in this module. We use DriveHQ as our cloud service provider to implement cloud storage, and the files that the data owner uploads are stored there as blocks and pieces. Furthermore, there is a very little chance that an attacker will discover fragments on every node if they are unsure of the positions of the fragments. In order to prevent an attacker from obtaining the data file, we fragment the information that was given file and upload it to the cloud. In cloud systems, there is substantially less chance for an attacker to access a sizable amount of data. The system will require more time to retrieve the data if each fragment is entered only once.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023, Pages 404-408

DOI: 10.17148/IARJSET.2023.10756

VI. CONCLUSION

Data sharing has become one of the IoT's most well-known uses as a result of its development. In a setting that utilises the cloud, we provide a secure identity-based Precondition data-sharing mechanism to ensure integrity, security, and privacy. The IBPRE technology enables secure data sharing and enables data owners to effectively share their encrypted data with authorised users while storing it in the cloud. An edge device acts as a proxy to manage the intense calculations due to resource limitations. The plan also makes use of ICN's capabilities to effectively serve cached information, enhancing service quality and optimising network bandwidth.

BIOGRAPHIES

I **Yashaswini Y** from Department of MCA of Bangalore Institute Of Technology would like to express my sincere appreciation to the following individuals and organizations who have contributed to the completion of this research:

Dr.T Vijaya Kumar, Head of MCA Department, Bangalore Institute Of Technology. For their valuable guidance and insightful suggestions throughout the research process.

Prof. K Sharath, Department of MCA, Bangalore Institute Of Technology. For their assistance in conducting experiments and collecting data.

REFERENCES

[1] "Internet of Things: A survey encompassing enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorial, vol. 17, no. 4, october/december 2015, pp. 2347-2376.
[2] "Divertible protocols via atomic proxy cryptography," Prog. Int. Conf. Theory Am. Cryptographic Techn., Springer, May 18, 1998, pp. 127–144.
[3] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Workshop Theory Appl. Cryptographic Techn., Springer, August 1984, pp. 47–53.
[4] "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506-522. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano.
[5] "Building an encrypted and searchable audit log," in NDSS, vol. 4. Citeseer, February 2004, pp. 5–6. B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters.
[6] D. Balfanz et al., "Secret embraces from pairing-based key agreements," in Proc. IEEE, Symp.
[7] "Chosen-ciphertext security from identity-based encryption," Proc. Int. Conf. The theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.
[8] T. Koponen and colleagues, "A data-oriented (and beyond) network architecture," Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., August 2007, pp. 181–192.
[9] "Developing information networking further: From PSIRP to pursuit," in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13. N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos.
[10] "Secure naming for a network of information," in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops, 2010, pp. 1-6. C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren.
[11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," Proc. IEEE INFOCOM 2004, vol. 2, 2004, p. 918–928.