**A BLOCKCHAIN-BASED PROXY RE-ENCRYPTION APPROACH FOR SECURE DATA EXCHANGE IN THE NET OF THINGS**

*1 Mateti Meghana , 2 Pendam Yashonath, 3Vanga Vishwa Teja, 4Pendli Mahendher, 5N. Shiva Prasad*

# *1,2,3,4bachelor Degree, Cse,* *Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

*5Mr N.Shiva Prasad, Assistant Professor, bachelor Degree, Cse, Jayamukhi Institute Of Technological Sciences Narsampet, Warangal.*

**ABSTRACT**

Data sharing has emerged as one of the Internet of Things' most advantageous cloud computing applications as it has developed.

Even if this technology has been visually appealing, data security is still one of its challenges since 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 encrypted data to the cloud, while proxy re-encryption construction allows authorised users to access the data. Due to the limited resources of Internet of Things devices, an edge device serves as a proxy server to perform demanding calculations.

Effectively delivering cached material over the proxy will increase service quality and make efficient use of available network bandwidth. Additionally, the foundation of our system concept is blockchain, a ground-breaking technology that permits decentralised data exchange. It achieves fine-grained access control to data and reduces bottlenecks in centralised systems. The security study and evaluation of our plan demonstrate the potential of our strategy for guaranteeing data security, confidentiality, and integrity.

**INTRODUCTION**

The Internet of Things (IoT) has evolved as a technology with significant global impact, and as a result of its use, network traffic levels have increased significantly over time. In the next years, many more gadgets are anticipated to become linked. The IoT paradigm places a premium on data since the information gathered may be used for a variety of things.

in a variety of applications, including those related to industry, transportation networks, smart cities, and healthcare [1]. For all parties concerned, the sensors measure a wide range of characteristics that are highly helpful. So, despite how alluring the Internet of Things may appear, it has created new security and privacy issues. IoT must be protected from attacks that prevent it from offering the necessary services and those that endanger the confidentiality, integrity, and privacy of data.

Encrypting the data before outsourcing to cloud servers is a workable method. Attackers can only access encrypted data when conventional security measures are unsuccessful. Any information that is shared must be encrypted at the source and only be decoded by approved users in order to maintain its security.

The decryption key can be shared by all the data users chosen by the data owner when using conventional encryption techniques. The use of symmetric encryption means that the data owner and users share the same key, or at the very least that the participants have agreed upon a key. This answer is quite ineffective.

The encrypted data must first be decrypted and then re-encrypted with a key that is known to both the data owner and the users since the data owners do not always know who the intended data users are. The data owner would need to remain online constantly with this decrypt-and-encrypt approach, which is virtually impossible. When there are several data sets and various data owners and consumers, the issue gets more complicated.

Although straightforward, standard encryption techniques need intricate key management methods and are thus inappropriate for data sharing. Blaze et al. [2] initially presented the idea of proxy re-encryption (PRE), which enables a proxy to convert a file calculated using a delegator's public key into 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 communications without disclosing his secret key. The re-encryption key is created by the data owner or a reliable third party.

This answer is quite ineffective.

The encrypted data must first be decrypted and then re-encrypted with a key that is known to both the data owner and the users since the data owners do not always know who the intended data users are. The data owner would need to remain online constantly with this decrypt-and-encrypt approach, which is virtually impossible. When there are several data sets and various data owners and consumers, the issue gets more complicated.

Although straightforward, standard encryption techniques need intricate key management methods and are thus inappropriate for data sharing. Blaze et al. [2] initially presented the idea of re-encryption by proxy (PRE), which enables a proxy to convert a file calculated using a delegator's secret key into a secret key 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 communications 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 executes the re-encryption algorithm using 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 regarded as a top choice for securely granting access to encrypted data, which is an essential element in any data-sharing scenario. Additionally, PRE enables the sharing of encrypted cloud data with authorised users while protecting its privacy from unauthorised individuals.

Since only individuals authorised by the data owner may successfully access the outsourcing data, data leaks can be reduced by the use of encryption.

**RELATED WORKS**

This section examines some of the ways that the technologies mentioned in this article may be applied to cloud access control and data sharing.

Pre-Data Sharing in A

Key-policy ABE (KP-ABE) and PRE were coupled by Yu et al. [15] to provide a solution for cloud data sharing. KP-ABE encryption was used to encrypt the data, making decryption feasible only with the right set of attribute secret keys. In addition to managing the encrypted data, the cloud also controlled all attribute secret keys with the exception of one unique secret key for user revocation. The encrypted data had to be re-encrypted when users were revoked since new keys required to be provided by the data owner to the remaining users.

Despite being effective, the scheme's security was compromised since the re-encryption was carried out carelessly. A revision to the plan in [15] by Park [16] prevents collaboration between the service provider and users whose access has been revoked. Their plan essentially consisted of substituting a reliable third party for the service provider, which suggests that a higher level of confidence should be assumed. Similar methods were used by other techniques [17]–[19], although they did so using ciphertext-policy ABE (CP-ABE), in which the access policy is linked to the ciphertext rather than the secret keys.

A time-constrained access control strategy based on PRE and ABE was also presented by Liu et al. [20]. While PRE was used to update the time characteristics, ABE was utilised to establish time-based access control policies.

Despite these schemes' benefits, their high computational costs for encryption and decryption make them unsuitable for use in the IoT.

Han et al. introduced an IBE PRE scheme appropriate for data exchange in [21]. The re-encryption keys were linked to a particular ciphertext in addition to the identities of the users.

This suggested that each combination of data users and shared files required the data owner to generate a unique reencryption key. Lin et al. presented a related notion.

[22] where a hierarchical PRE was employed as opposed to an identity-based PRE. When taking into account many and complicated data elements, these two approaches frequently exhibit inefficiency. Zhou et al. in [23] suggested an identity-based broadcast encryption (IBBE) coupled with PRE for data sharing. Their plan was a hybrid one that enabled conversion between the two protocols without disclosing any private data. Wang et al. [24] furthermore created

a PRE (IBPRE) identity-based system for accessing medical records. Large-scale access control was made possible by the plan.

All of the ciphertexts may be re-encrypted and made accessible to the intended users if a proxy gets the re-encryption key from the data owner, or none may be. A condition-based IBE PRE scheme was presented by Shao et al. [25] in response to this. According to their suggestion, the proxy might convert a portion of ciphertexts belonging to one identity into ciphertexts belonging to another identity. It was impossible to grant a set of users the ability to decrypt data, though. In addition to the aforementioned uses, PRE has been employed to address IoT security issues [26].

**EXISTING SYSTEM:**

The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks …etc and manufacturing, among others. 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.

**PROPOSED SYSTEM:**

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., allows a proxy to transform a file computed under a delegator’s public key into an encryption intended for a delegate. 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.

Motivated by this scenario, this article proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology. Shamir first presented the notion of IBE, in which a sender encrypts a message to a recipient using the identity (email ) as the public key. It is a very powerful primitive used to combat numerous key distribution problems and has consented to the development of several cryptographic protocols, including public-key searchable encryption , secret handshakes , and chosen cipher text attack (CCA) secure public-key encryption . IBE is preferred over attribute-based encryption (ABE) because ABE involves heavy computations on data encryption, decryption, and key management, and these processes are not convenient for the resource-constrained IoT devices

**RESULT:**



**CONCLUSION:**

Data sharing has become one of the IoT's most well-known uses as a result of its development. In a cloud computing context, we provide a secure identity-based PRE data-sharing mechanism to ensure data confidentiality, integrity, 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 intensive calculations due to resource limitations. T

The plan also makes advantage of ICN's capabilities to effectively serve cached information, enhancing service quality and optimising network traffic. Then, we describe a system paradigm built on a blockchain that enables flexible permission for encrypted data. It is possible to implement fine-grained

access control, which can effectively aid data owners in preserving privacy. The analysis and outcomes of the suggested model demonstrate how effective our plan is when compared to other plans.

**REFERENCES**

[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.

[11] A. 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.

[12] I. Psaras, W. K. Chai, and G. Pavlou, “Probabilistic in-network caching for

information-centric networks,” in *Proc. 2nd ed. ICN Workshop Inform.-*

*Centric Netw.*, Aug. 2012, pp. 55–60.

[13] Y. Sun *et al.*, “Trace-driven analysis of ICN caching algorithms on video

on-demand workloads,” in *Proc. 10th ACM Int. Conf. Emerging Netw. Exp.*

*Technol.*, Dec. 2014, pp. 363–376.

[14] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, vol. 4.

Bitcoin.org, 2008. Available: https://bitcoin. org/bitcoin. pdf

[15] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and

fifine-grained data access control in cloud computing,” in *Proc. IEEE*

*INFOCOM*, Mar. 2010, pp. 1–9.

[16] N. Park, “Secure data access control scheme using type-based re

encryption in cloud environment,” in *Semantic Methods Knowledge Man*

*agement and Communications*. Berlin, Germany: Springer, 2011, pp. 319–

327.

17] G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-based

encryption and scalable user revocation for sharing data in cloud servers,*”*

*Comput. Secur.*, vol. 30, no. 5, pp. 320–331, Jul. 2011.

[18] J. Hur, “Improving security and effificiency in attribute-based data shar

ing,” *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 10, pp. 2271–2282,

Apr. 2011.

[19] P. K. Tysowski and M. A. Hasan, “Hybrid attribute-and re-encryption

based key management for secure and scalable mobile applications

in clouds,” *IEEE Trans. Cloud Comput.*, vol. 1, no. 2, pp. 172–186,

Nov. 2013.

[20] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme

for secure data sharing in a cloud environment,” *Inform. Sci.*, vol. 258,

pp. 355–370, Feb. 2014.

[21] J. Han, W. Susilo, and Y. Mu, “Identity-based data storage in cloud

computing,” *Future Gener. Comput. Syst.*, vol. 29, no. 3, pp. 673–681,

Mar. 2013.

[22] H.-Y. Lin, J. Kubiatowicz, and W.-G. Tzeng, “A secure fifine-grained access

control mechanism for networked storage systems,” in *Proc. IEEE 6th Int.*

*Conf. Softw. Secur. Rel.*, Jun. 2012, pp. 225–234.

[23] Y. Zhou *et al.*, “Identity-based proxy re-encryption version 2: Making

mobile access easy in cloud,” *Future Gener. Comput. Syst.*, vol. 62,

pp. 128–139, Sep. 2016.

[24] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, “Cost-effective secure

e-health cloud system using identity based cryptographic techniques,”

*Future Gener. Comput. Syst.*, vol. 67, pp. 242–254, Feb. 2017.

[25] J. Shao, G. Wei, Y. Ling, and M. Xie, “Identity-based conditional

proxy re-encryption,” in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011,

pp. 1–5.

[26] K. O. B. Obour Agyekum *et al.*, “A secured proxy-based data sharing

module in IoT environments using blockchain,” *Sensors*, vol. 19, no. 5,

Jan. 2019, Art. no. 1235.

[27] G. Zyskind *et al.*, “Decentralizing privacy: Using blockchain to protect

personal data,” in *Proc. IEEE Secur. Privacy Workshops*, May 2015,

pp. 180–184.

[28] D. D. F. Maesa, P. Mori, and L. Ricci, “Blockchain based access control,”

in *Proc. IFIP Int. Conf. Distributed Appl. Interoperable Syst.*, Springer,

Jun. 2017, pp. 206–220.

[29] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, “Blockchain-based effificient

privacy preserving and data sharing scheme of content-centric network in

5G,” *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[30] M. Singh and S. Kim, “Branch based blockchain technology in intelligent

vehicle,” *Comput. Netw.*, vol. 145, pp. 219–231, Nov. 2018.

[31] R. S. Da Silva and S. D. Zorzo, “An access control mechanism to ensure

privacy in named data networking using attribute-based encryption with

immediate revocation of privileges,” in *Proc. 12th Annu. IEEE Consum.*

*Commun. Netw. Conf.*, Jan. 2015, pp. 128–133.

[32] B. Li, D. Huang, Z. Wang, and Y. Zhu, “Attribute-based access control for

ICN naming scheme,” *IEEE Trans. Dependable Secure Comput.*, vol. 15,

no. 2, pp. 194–206, Apr. 2016.

[33] S. Misra *et al.*, “Accconf: An access control framework for leveraging

in-network cached data in the ICN-enabled wireless edge,” *IEEE Trans.*

*Dependable Secure Comput.*, vol. 16, no. 1, pp. 5–17, Feb. 2017.

[34] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, “DACPI: A decen

tralized access control protocol for information centric networking,” in

*Proc. IEEE Int. Conf. Commun.*, May 2016, pp. 1–6.

[35] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, “Effificient and

robust certifificateless signature for data crowdsensing in cloud-assisted

industrial IoT,” *IEEE Trans. Ind. Inform.*, vol. 15, no. 9, pp. 5099–5108,

Jan. 2019.

[36] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, “Secure

data storage and searching for industrial IoT by integrating fog comput

ing and cloud computing,” *IEEE Trans. Ind. Inform*., vol. 14, no. 10,

pp. 4519–4528, Jan. 2018.

[37] M. Ma, D. He, N. Kumar, K.-K. R. Choo, and J. Chen, “Certifificateless

searchable public key encryption scheme for industrial Internet of Things,”

*IEEE Trans. Ind. Inform.*, vol. 14, no. 2, pp. 759–767, May 2017.

[38] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, “A lightweight privacy-preserving

protocol for VANETs based on secure outsourcing computing,” *IEEE*

*Access*, vol. 7, pp. 62785–62793, 2019.

[39] Y. Zhang, D. Zheng, and R. H. Deng, “Security and privacy in smart

health: Effificient policy-hiding attribute-based access control,” *IEEE In*

*ternet Things J.*, vol. 5, no. 3, pp. 2130–2145, Apr. 2018.

[40] L. Zhang, Q. Wu, Y. Mu, and J. Zhang, “Privacy-preserving and secure

sharing of PHR in the cloud,” *J. Med. Syst.*, vol. 40, no. 12, pp. 1–13,

Dec. 2016.This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

12

IEEE SYSTEMS JOURNAL

[41] S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data

sharing with fifine-grained access control in decentralized storage systems,*”*

*IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[42] S. Niu, L. Chen, J. Wang, and F. Yu, “Electronic health record sharing

scheme with searchable attribute-based encryption on blockchain,” *IEEE*

*Access*, vol. 8, pp. 7195–7204, 2019.

[43] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy

re-encryption schemes with applications to secure distributed storage,”

*ACM Trans. Inform. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, Feb. 2006.

[44] R. Pecori, “S-kademlia: A trust and reputation method to mitigate a sybil

attack in Kademlia,” *Comput. Netw.*, vol. 94, pp. 205–218, Jan. 2016.

[45] A. De Caro and V. Iovino, “ JPBC: Java pairing based cryptography,” in

*Proc. IEEE Symp. Comput. Commun.*, Jun. 2011, pp. 850–855.

[46] E. Barker, L. Chen, S. Keller, A. Roginsky, A. Vassilev, and R. Davis,

“Recommendation for pair-wise key-establishment schemes using discrete

logarithm cryptography,” National Institute of Standards and Technology,

Gaithersburg, MD, USA, Tech. Rep. 800-56Ar3, Aug. 2017.