International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 3, Jul.-Aug. 2022, pp: 125-128 www.ijhssm.org

# A Proxy Re-Encryption Approach for Secured Data Sharing In Internet of Things Based On Blockchain

A. Ancilin Divya[1]
[1]*Student, CSI Institute of Technology Thovalai, Kanyakumari District, Tamil Nadu- 629 302.*
*Dr. K. P. Ajitha Gladis, M.E, MISTE, Ph.D, CSI Institute of Technology, Thovalai, Kanyakumari District, Tamil Nadu- 629 302.*

Date of Submission: 13-07-2022 Date of Acceptance: 27-07-2022

**Abstract-** Due to the evolution of Internet of Things, data sharing is seen as one of the most useful applications in cloud computing. In data sharing, data security has become one of the obstacles, since the wrongful use of data leads to several damages. In this paper, a proxy re-encryption approach to secure data sharing in cloud environments is proposed. Identity-based encryption is used by data owners to outsource their encrypted data to the cloud, where proxy re-encryption construction will grant legitimate users access to the data. With the IoT devices being resource-constrained, for handling intensive computations, an edge device acts as a proxy server. Also, this system makes use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, the proposed system is based on blockchain, a disruptive technology that enables decentralization in data sharing. It achieves fine-grained access control to data by mitigating the bottlenecks in centralized systems. The security analysis and evaluation shows that the proposed proxy re-encryption approach ensures data confidentiality, integrity, and security.

**Keywords:** Access control, Blockchain, Data Security, Identity Based Proxy Re-Encryption, Information-Centric Network (ICN), Internet of Things (IoT), Transmission, Cryptography, Steganography, Pseudorandom**.**

## I. INTRODUCTION

The internet of things is a system of interrelated computing devices, mechanical and digital machines or objects, which are provided with unique intensifiers (UIDs) and which facilitate the ability to transfer the data through a network without the requirement of humans. The IoT provides businesses with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations. Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to provide enhanced customer service, improve decision-making and increase the value of business. An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data sent to the cloud to be analyzed. The devices communicate with other related devices and act on the information they get from one from another. The devices almost work without human intervention, although people can interact with the devices for instance, to set them up, give them instructions or access the data.

### Steganography

The two Greek words for steganography are ‘steganos’ which mean hide or secret and ‘graphy’ which means ‘writing’. That means hidden writing and embedding data into an object which cannot be noticed or recognized by anyone. Data can be embedded into an audio file, image file and or video file. Cryptography gives one layer of security and confidentiality. Steganography gives an additional layer of security to the data.

### Types of Steganography

*Image steganography*: Images are used as the message carriers. Images are one of the important secret message carriers as the data is stored inside the pixels of the image which cannot be sensed by human vision.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 3, Jul.-Aug. 2022, pp: 125-128 www.ijhssm.org

*Textual steganography*: Text steganography is hiding the data in a paragraph. The secret message is altered among the paragraph and by using the key we can retrieve the information from the paragraph.
*Audio steganography*: In audio steganography, a secret message is embedded into the audio signals which makes changes in the binary sequence of the original audio file.

**Image Steganography**
A digital image is the most secure way to carry the sensitive information through the internet using steganography.

## II. RELATED WORK

The data is used more widely in present days and authenticity is becoming a much more common problem while sharing or transmitting through mediums. In order to securely transmit the data through the internet there were several methodologies developed using image steganography and cryptography. The model proposed uses visual cryptography and neural networks. Neural network is used to find the best location in the image blocks generated by the visual cryptography and to embed the data using LSB.

The application of inverse cryptography is accomplished during decryption. The blocks are encrypted using double random phase encoding which converts into stationary noise. Using Fourier transformation, the image multiplied by a random phase mask is converted to frequency domain from time domain and a random phase mask is applied. It presented an enhanced safe data transfer scheme in the smart Internet of Things (IoT) environment.

The proposed technique employs an integrated approach of steganography and cryptography during data transfer between the IoT device & home server and home server & cloud server. The sensed data from an IoT device is encrypted and embedded in a cover image along with a message digest of sensed data and sent to the home server for authentication purposes. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with a newly computed digest to ensure the data integrity and authentication. The same procedure is carried out between home server and cloud server.

## III. PROPOSED SYSTEM

The technique to hide the data inside an image is called image steganography. Humans cannot make a difference in the image when the data is embedded in it. It takes quite knowledge and tool practice to identify the image. The proposed work uses cryptography and steganography to provide high security to the data over a network.

**Methodology**

In this work a secure access control framework is proposed to realize data confidentiality, and fine-grained access to data is achieved and this will also guarantee data owners' complete control over their data. The pre scheme actualizes a complete protocol that guarantees security and privacy of data. The data delivery effectively utilizes the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have more computation capabilities than the IoT devices and as such provide high performance networking. A consortium blockchain is adopted due to its suitability to access control and privacy preservation. Authorized users can have access to the data.

Data owners can effectively manage their data and audit logs. Consortium blockchains provide a high level of security. IoT security concerns that are addressed by the blockchain network include verifying the identity of the connected users or devices, their account information, and also preventing cached data from being misused. Because edge devices have enough computing resources and storage, they act as proxy servers to provide re-encryption services and other computations for the resource-constrained IoT devices. They easily cache data at these edge nodes.

Retrieving data via high-speed networks, the user can make requests for data access, thus providing a smooth user experience. A private key is used as seed to randomly generate the sequence of number of pixels which can be used to store the secret message. Using the same private key, the message is encrypted and then used to embed into the pixels. Since noise will be generated after embedding the bits, instead we use pictures where each pixel has a noise before using it. It is helpful because, since all the pixels has noise, the hacker will have a hard time to find the pixels with embedded information.

The system architecture diagram of proxy re-encryption approach for secure data sharing in the internet of things based on blockchain is shown in the Fig 3.1. The figure shown below is the overall process of the proxy re-encryption approach for secure data sharing.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 2, Issue 3, Jul.-Aug. 2022, pp: 125-128 www.ijhssm.org

**System Architecture**

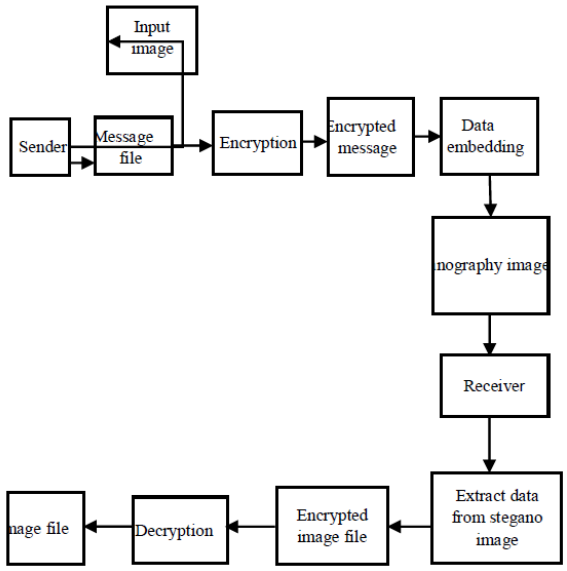


**Fig 3.1 System Architecture**

**Algorithm**

- Given the private key, Generate Pseudo random number of pixels required to store the secret message.
- Rand (seed=private key).
- Read a byte from the private key stream PK.
- Read a byte from the secret message stream SM.
- Encrypt a secret message with a private key using XOR operation.
- SM XOR PK = MessageByte.
- Loop over the number of pixels one by one.
- Get the color components of the current pixel used to embed MessageByte.
- P(i,j) = RGB.
- Replace the first component in the pixel with MessageByte.
- R = MessageByte.
- Loop over a number of pixels one by one.
- Loop over the components in the pixel to store

## IV. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, a secure identity-based PRE data-sharing scheme is proposed 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, a blockchain-based system model is presented that allows flexible authorization on encrypted data. Fine-grained access control is achieved, and it can help data stewards achieve privacy preservation in an adequate way.

## REFERENCE

[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]. 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.

[4]. 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 computing and cloud computing," IEEE Trans. Ind. Inform., vol. 14, no. 10, pp. 4519–4528, Jan. 2018.

[5]. J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Apr. 2011.

[6]. H.-Y. Lin, J.Kubiatowicz, andW.-G. Tzeng, "A secure fine-grained access control mechanism for networked storage systems," in Proc. IEEE 6th Int. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.

[7]. M. Ma, D. He, N. Kumar, K.-K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," IEEE Trans. Ind. Inform., vol. 14, no. 2, pp. 759–767, May 2017.

[8]. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc.Workshop Theory Appl. Cryptographic Techn.*, Springer, Aug. 1984, pp. 47–53.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Apr. 2018.