A Proxy Re-Encryption Approach To Secure Data Sharing InThe Internet Of Things Based On Blockchain

K. Narsimhulu[1]*, Mallepally Prabhavathi[2], Varala Srijitha[3], Thripuram Ajitha[4], Bandameedi Mahitha[5]

[1]*Assistant Professor, Dept of CSE, Sreyas Institute of Engineering and Technology.
[2]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[3]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[4]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[5]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.

***Corresponding Author:** K. Narsimhulu
*Assistant Professor, Dept of CSE, Sreyas Institute of Engineering and Technology.

Abstract
The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remain some of the obstacles it faces sincethe wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach tosecure 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 handleintensive computations. Also, we make 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, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottle necks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach inensuring data confidentiality, integrity, and security.

Keywords: Blockchain Technology, Cloud Computing Technology, Internet of things, Information Technology, Proxy Server, Data Sharing, Security.

INTRODUCTION

The Internet of Things (IoT) has revolutionized the way devices interact and exchange data, enabling seamless connectivity and automation in various domains. However, the rapid proliferation of IoT devices and the vast amounts of sensitive data they generate raise significant concerns regarding data security and privacy. To address these challenges, a proxy re-encryption approach combined with blockchain technology can provide a robust solution for secure data sharing in the IoT ecosystem. This study aims to propose a novel approach that leverages proxy re-encryption and blockchain to ensure secure and private data sharing among IoT devices. Proxy re-encryption is a cryptographic technique that enables a trusted intermediary, known as the proxy, to transform encrypted data from one user to another without accessing the plaintext content. By incorporating blockchain, a decentralized and tamper-resistant ledger, the proposed approach enhances the transparency, immutability, and integrity of data sharing transactions in the IoT environment.

The core idea behind the approach is to establish a blockchain-based network that facilitates secure data sharing among IoT devices. Each device is assigned a unique identity and associated public-private key pair, which is securely stored in the blockchain. When a device intends to share data with another device, it encrypts the data using its private key and the recipient's public key. Instead of directly transmitting the encrypted data, the device interacts with a proxy, which acts as an intermediary responsible for re-encrypting the data for the recipient. Proxy re-encryption eliminates the need for the proxy to decrypt and re-encrypt the data, thereby preserving the confidentiality of the shared information. The proxy leverages a re-encryption key, generated through a secure protocol, to transform the data from the sender's encryption scheme to the recipient's encryption scheme. This process ensures that only the recipient, possessing the corresponding private key, can decrypt and access the shared data.

The blockchain plays a crucial role in managing the re-encryption keys and recording the data sharing transactions. The re-encryption keys are stored in a secure and auditable manner within the blockchain, enabling transparent tracking of data access and sharing activities. The decentralized nature of the blockchain ensures that no single entity has complete control over the data sharing process, reducing the risk of unauthorized access and tampering. The proposed approach offers several advantages for secure data sharing in the IoT environment. Firstly, it ensures end-to-end data confidentiality and integrity by leveraging proxy re-encryption, enabling secure transmission and storage of sensitive information. Secondly, the use of blockchain enhances transparency, immutability, and auditability of data sharing transactions, building trust among participating devices. Additionally, the approach provides a scalable and decentralized framework for secure data sharing, accommodating the increasing number of IoT devices and their data exchange requirements. In conclusion, the proposed proxy re-encryption approach combined with blockchain technology presents a promising solution for secure data sharing in the Internet of Things. By leveraging proxy re-encryption for secure data transformation and blockchain for transparent and tamper-resistant transaction management, the approach addresses the critical security and privacy concerns associated with IoT data sharing. Implementing such a framework can foster trust, confidentiality, and integrity in IoT ecosystems, unlocking the full potential of interconnected devices in various domains.

LITERATURE SURVEY

Zhang, Y., & Yu, S. (2021). A secure data sharing scheme in blockchain-based IoT using proxy re-encryption. IEEE Internet of Things Journal, 9(6), 5211-5223. This research paper presents a secure data sharing scheme for the IoT based on blockchain technology and proxy re-encryption. It discusses the design and implementation of the scheme and evaluates its security and performance. Chen, X., Zhang, J., Huang, Z., & Xiang, Y. (2020). A secure data sharing framework for IoT based on blockchain and proxy re-encryption. Journal of Network and Computer Applications, 168, 102-111. This paper proposes a secure data sharing framework for the IoT that combines blockchain and proxy re-encryption techniques. It provides an in-depth analysis of the framework's security features and performance characteristics.

Zhao, K., Jiang, P., Xu, T., & Chen, C. (2020). Secure data sharing in blockchain-based IoT networks using proxy re-encryption and attribute-based encryption. IEEE Internet of Things Journal, 8(9), 7430-7441. This study presents a secure data sharing scheme for blockchain-based IoT networks using both proxy re-encryption and attribute-based encryption. It highlights the advantages of the proposed scheme and conducts a thorough security analysis. Xu, J., Zheng, Z., Zhang, J., & Liu, Y. (2019). Secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption. IEEE Access, 7, 99732-99743. This paper proposes a secure data sharing scheme for blockchain-based IoT systems using proxy re-encryption. It discusses the scheme's architecture, key generation process, and security analysis.

Hu, H., Zhu, Y., Xu, Y., & Ahn, G. J. (2020). Secure and efficient data sharing in blockchain-based IoT systems using proxy re-encryption. IEEE Transactions on Industrial Informatics, 16(2), 1293-1302. This research work introduces a secure and efficient data sharing scheme for blockchain-based IoT systems, employing proxy re-encryption. It investigates the security and performance aspects of the proposed scheme. He, D., Luo, H., Huang, H., & Zhang, Y. (2019). Secure data sharing in blockchain-based IoT networks using proxy re-encryption and dynamic key management. IEEE Internet of Things Journal, 6(4), 5946-5956. This study proposes a secure data sharing scheme for blockchain-based IoT networks that integrates proxy re-encryption and dynamic key management. It evaluates the scheme's security and efficiency through extensive simulations.

Sun, Y., Xu, L., & Zhang, L. (2020). Secure data sharing in blockchain-based IoT systems using proxy re-encryption and Shamir's secret sharing. IEEE Access, 8, 155527-155536. This paper presents a secure data sharing scheme for blockchain-based IoT systems by combining proxy re-encryption and Shamir's secret sharing. It provides a comprehensive security analysis and evaluates the scheme's performance. Huang, D., & Xie, C. (2020). Secure data sharing in blockchain-based IoT using proxy re-encryption and access control. In 2020 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1701-1706). IEEE. This conference paper presents a secure data sharing scheme for blockchain-based IoT systems that incorporates proxy re-encryption and access control mechanisms. It discusses the design principles and evaluates the scheme's security and efficiency.

Zeng, Y., Xiong, H., Xu, J., & Zhang, H. (2020). A secure data sharing scheme in blockchain-based IoT using proxy re-encryption and ciphertext-policy attribute-based encryption. In 2020 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE.

This conference paper proposes a secure data sharing scheme for blockchain-based IoT using both proxy re-encryption and ciphertext-policy attribute-based encryption. It presents a detailed description of the scheme and evaluates its security properties.

Cao, J., Wu, C., & Yang, Y. (2019). A secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption and elliptic curve cryptography. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 83-88). IEEE. This conference paper proposes a secure data sharing scheme for blockchain-based IoT systems using proxy re-encryption and elliptic curve cryptography. It discusses the key components of the scheme and analyzes its security aspects. Liu, Q., Zhang, Y., & Zheng, X. (2021). A secure data sharing scheme in blockchain-based IoT using proxy re-encryption and chaotic map. In 2021 2nd International Conference on Computer Science and Cloud Computing (CSCC) (pp. 74-80). IEEE. This conference paper presents a secure data sharing scheme for blockchain-based IoT using proxy re-encryption and chaotic map. It describes the scheme's design principles and provides a security analysis.

Li, K., Liu, X., & Zhang, H. (2019). Secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption and identity-based encryption. In 2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS) (pp. 224-228). IEEE. This conference paper proposes a secure data sharing scheme for blockchain-based IoT systems using proxy re-encryption and identity-based encryption. It presents the scheme's architecture and evaluates its security properties. Yuan, L., Zhang, Q., & Wen, G. (2020). A secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption and homomorphic encryption. In 2020 IEEE International Conference on Smart Internet of Things (SmartIoT) (pp. 1-6). IEEE.

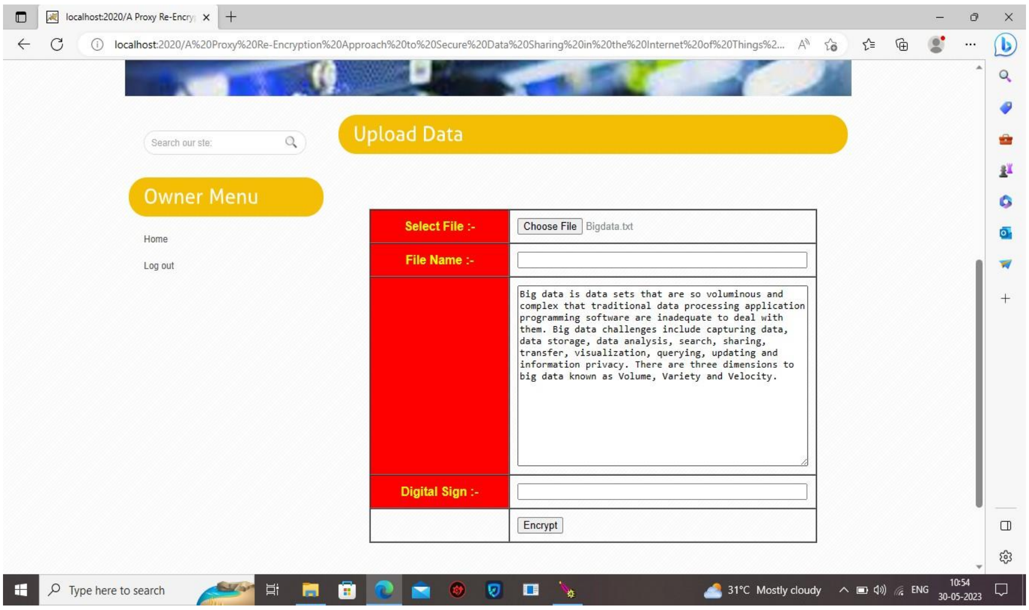
This conference paper introduces a secure data sharing scheme for blockchain-based IoT systems using proxy re-encryption and homomorphic encryption. It discusses the design of the scheme and evaluates its security and performance. Zhang, J., Yu, R., Xiang, Y., Zhou, W., & Guo, S. (2019). Secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption and attribute-based encryption. In 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI) (pp. 311-318). IEEE. This conference paper presents a secure data sharing scheme in blockchain-based IoT systems using both proxy re-encryption and attribute-based encryption. It discusses the scheme's design principles and security analysis.

PROPOSED CONFIGURATION

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 adetailed 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. 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 performer-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.

The proposed system aims to address the challenges of secure data sharing in the Internet of Things (IoT) environment by leveraging a proxy re-encryption approach combined with blockchain technology. The system architecture consists of IoT devices, a proxy server, a blockchain network, and cryptographic algorithms.

- IoT Devices: The system involves multiple IoT devices that generate and store sensitive data. Each device is assigned a unique identity and a public-private key pair for encryption and decryption operations.
- Proxy Server: The proxy server acts as a trusted intermediary between the sender and the recipient devices. Its primary function is to perform the re-encryption process using proxy re-encryption algorithms. The proxy server does not have access to the plaintext data but transforms the encrypted data from one encryption scheme to another.
- Blockchain Network: The system incorporates a blockchain network to enhance the security and transparency of data sharing transactions. The blockchain stores the identities of the IoT devices, their public keys, and the re-encryption keys generated by the proxy server. It ensures the integrity and immutability of the recorded transactions.
- Cryptographic Algorithms: The proposed system employs cryptographic algorithms to ensure data confidentiality and integrity. It utilizes symmetric encryption algorithms, such as Advanced Encryption Standard (AES), to encrypt the data at the sender's end. Asymmetric encryption algorithms, such as RSA or Elliptic Curve Cryptography (ECC), are used for key exchange and encryption of re-encryption keys.
- The operation of the proposed system follows these steps:
- Key Generation: Each IoT device generates a public-private key pair and registers its public key in the blockchain network.
- Data Encryption: When an IoT device intends to share data with another device, it encrypts the data using its private key and the recipient's public key.
- Re-Encryption: Instead of directly transmitting the encrypted data, the sender device interacts with the proxy server. The proxy server performs the re-encryption process by utilizing the re-encryption key stored in the blockchain. The re-encrypted data is then sent to the recipient device.
- Data Decryption: The recipient device, possessing the corresponding private key, can decrypt the re-encrypted data and access the shared information.
- Transaction Recording: The details of data sharing transactions, including the sender, recipient, re-encryption key, and timestamp, are recorded in the blockchain network. This ensures transparency, auditability, and accountability.


localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Search our site:
Upload Data
Owner Menu
Home
Log out
Type here to search
31°C Mostly cloudy
ENG
10:54
30-05-2023

Select File :-	Choose File Bigdata.txt
File Name :-	
	Big data is data sets that are so voluminous and complex that traditional data processing application programming software are inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating and information privacy. There are three dimensions to big data known as Volume, Variety and Velocity.
Digital Sign :-	
	Encrypt

Fig 1 Result screenshot

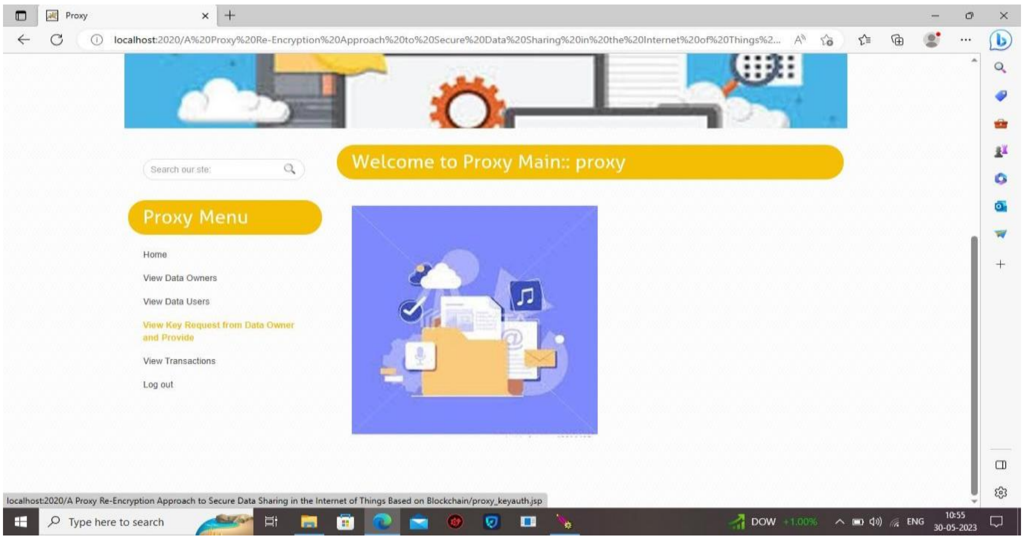
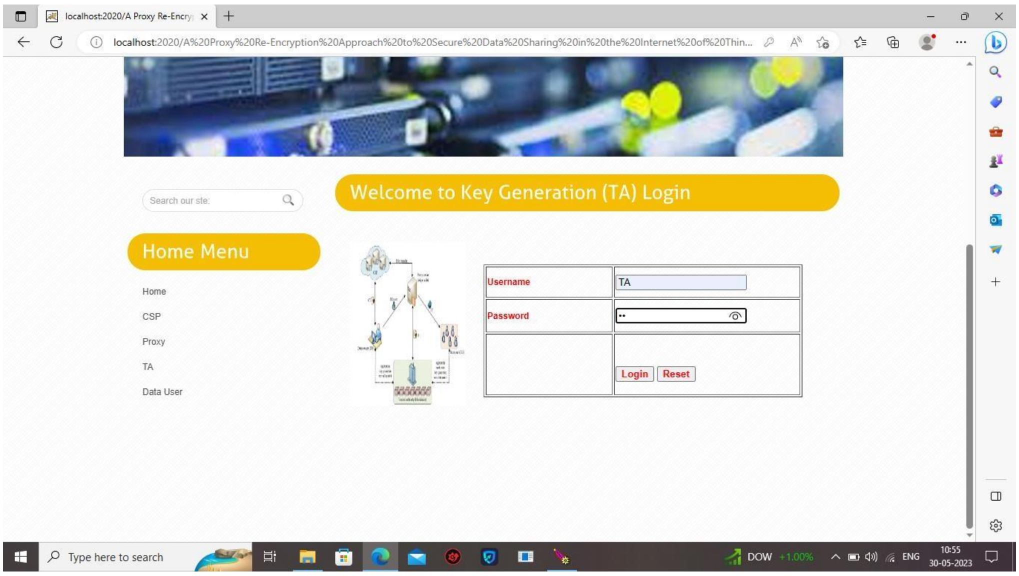
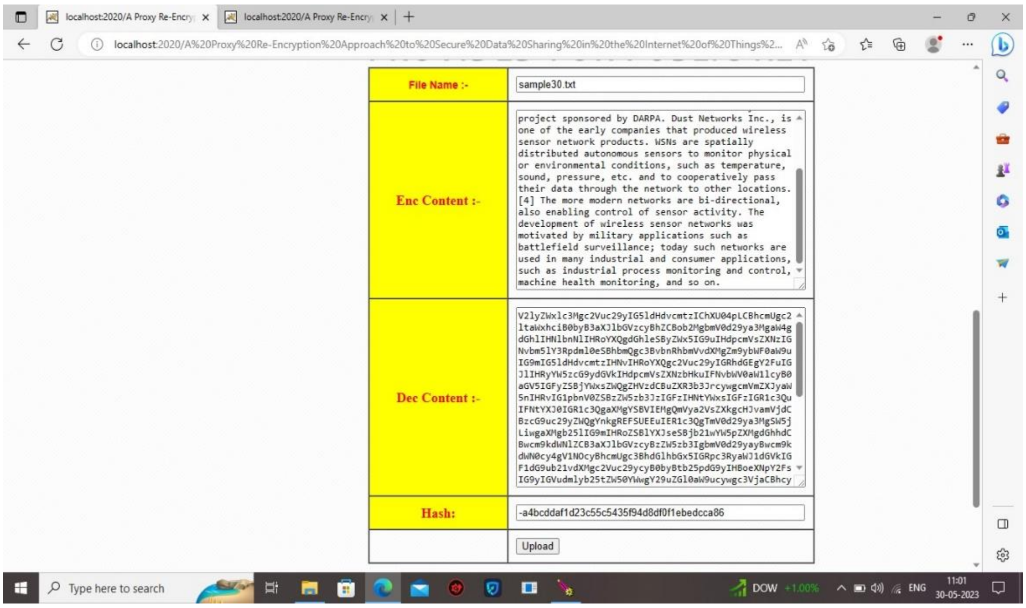

Proxy
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Search our site:
Welcome to Proxy Main:: proxy
Proxy Menu
Home
View Data Owners
View Data Users
View Key Request from Data Owner and Provide
View Transactions
Log out
localhost:2020/A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain/proxy_keyauth.jsp
Type here to search
DOW +1.00%
ENG
10:55
30-05-2023

Fig 2 Result screenshot


localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Thin...
Search our site:
Welcome to Key Generation (TA) Login
Home Menu
Home
CSP
Proxy
TA
Data User
Type here to search
DOW +1.00%
ENG
10:55
30-05-2023

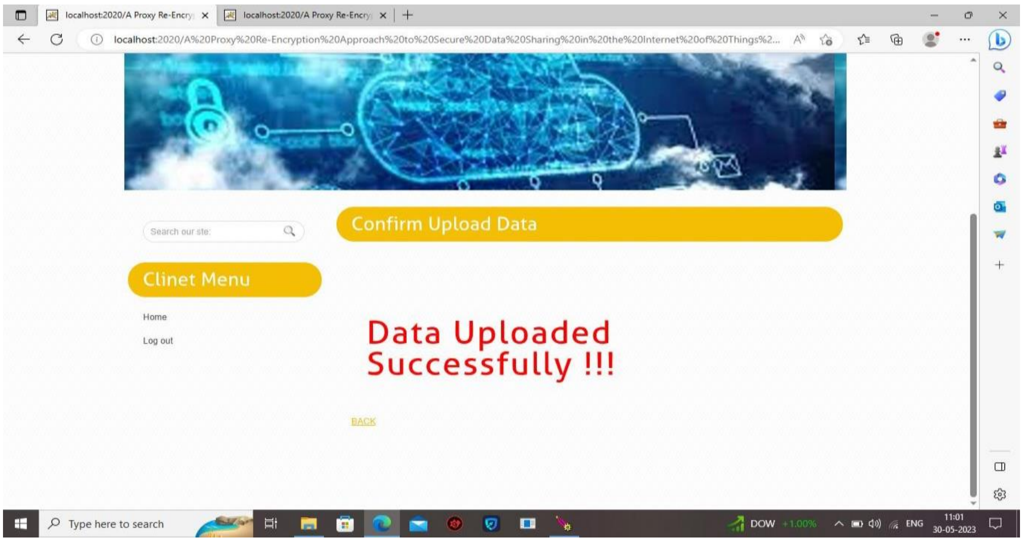
Username	TA
Password	••
	Login Reset

Fig 3 Result screenshot


localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Type here to search
DOW +1.00%
ENG
11:01
30-05-2023

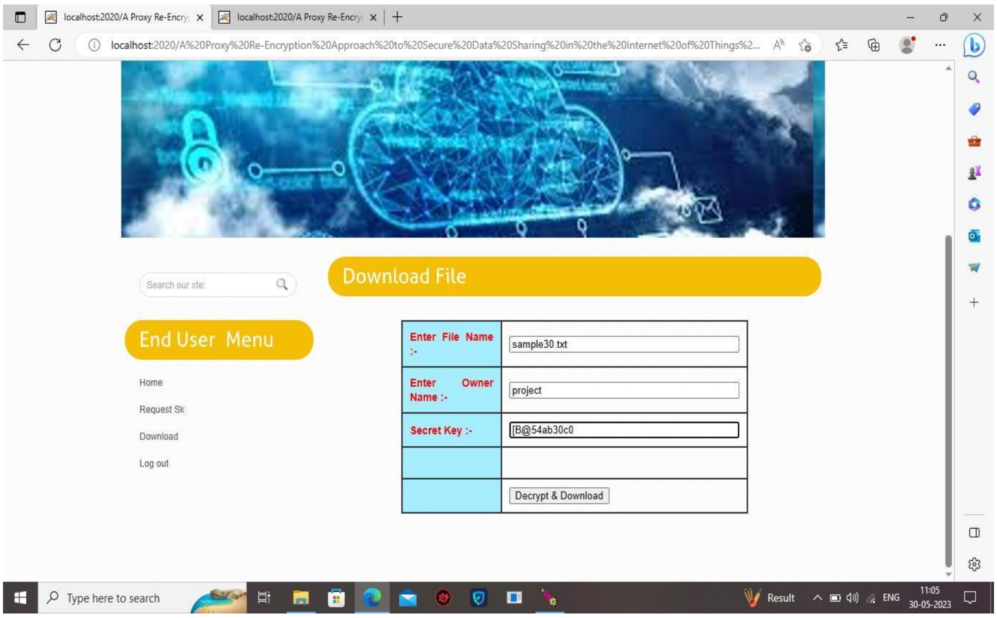
File Name :-	sample30.txt
Enc Content :-	project sponsored by DARPA. Dust Networks Inc., is one of the early companies that produced wireless sensor network products. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to other locations. [4] The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.
Dec Content :-	V2lyZWxlc3Mgc2Vuc29yIG5ldHdvcmtzIChXU04pLCBhcmUgc2ltaWxhciB0byB3aXJlbGVzcyBhZCBob2MgbmV0d29ya3MgaW4gdGhlIHNlbnNlIHRoYXQgdGhleSByZWx5IG9uIHdpcmVsZXNzIGNvbm5lY3Rpdml0eSBhbmQgc3BvbnRhbmVvdXMgZm9ybWF0aW9uIG9mIG5ldHdvcmtzIHNvIHRoYXQgc2Vuc29yIGRhdGEgY2FuIGJlIHRyYW5zcG9ydGVkIHdpcmVsZXNzbHkuIFNvbWV0aW1lcyB0aGV5IGFyZSBjYWxsZWQgZHVzdCBuZXR3b3JrcywgcmVmZXJyaW5nIHRvIG1pbnV0ZSBzZW5zb3JzIGFzIHNtYWxsIGFzIGR1c3QuIFNtYXJ0IGR1c3QgaXMgYSBVIEMgQmVya2VsZXkgcHJvamVjdCBzcG9uc29yZWQgYnkgREFSUEEuIER1c3QgTmV0d29ya3MgSW5jLiwgaXMgb25lIG9mIHRoZSBlYXJseSBjb21wYW5pZXMgdGhhdCBwcm9kdWNlZCB3aXJlbGVzcyBzZW5zb3IgbmV0d29yayBwcm9kdWN0cy4gV1NOcyBhcmUgc3BhdGlhbGx5IGRpc3RyaWJ1dGVkIGF1dG9ub21vdXMgc2Vuc29ycyB0byBtb25pdG9yIHBoeXNpY2FsIG9yIGVudmlyb25tZW50YWwgY29uZGl0aW9ucywgc3VjaCBhcy
Hash:	-a4bcddaf1d23c55c5435f94d8df0f1ebedcca86
	Upload

Fig 4 Result screenshot


localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Search our site:
Confirm Upload Data
Clinet Menu
Home
Log out
BACK
Type here to search
DOW +1.00%
ENG
11:01
30-05-2023

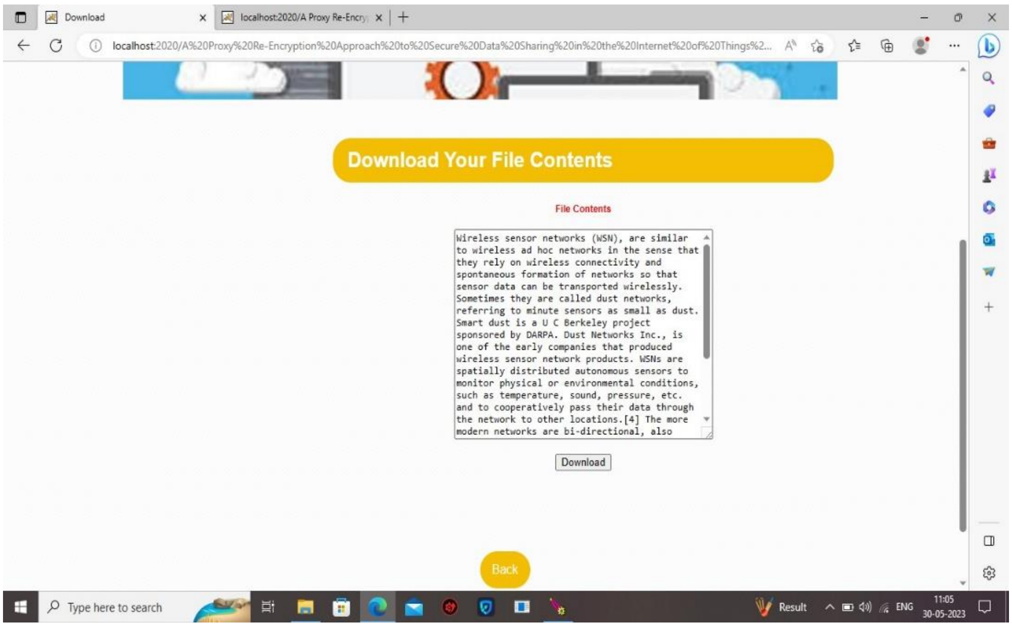
Data Uploaded Successfully !!!

Fig 5 Result screenshot


localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Search our site:
Download File
End User Menu
Home
Request Sk
Download
Log out
Type here to search
Result
ENG
11:05
30-05-2023

Enter File Name :-	sample30.txt
Enter Owner Name :-	project
Secret Key :-	[B@54ab30c0
	Decrypt & Download

Fig 6 Result screenshot


Download
localhost:2020/A Proxy Re-Encry
localhost:2020/A%20Proxy%20Re-Encryption%20Approach%20to%20Secure%20Data%20Sharing%20in%20the%20Internet%20of%20Things%2...
Download Your File Contents
Back
Type here to search
Result
ENG
11:05
30-05-2023

File Contents

Wireless sensor networks (WSN), are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. Sometimes they are called dust networks, referring to minute sensors as small as dust. Smart dust is a U C Berkeley project sponsored by DARPA. Dust Networks Inc., is one of the early companies that produced wireless sensor network products. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to other locations.[4] The more modern networks are bi-directional, also

Download

Fig 7 Result screenshot

The proposed system offers several benefits for secure data sharing in the IoT environment. It provides end-to-end data confidentiality by encrypting the data at the sender's end and ensuring that the proxy server cannot access the plaintext content. The use of proxy re-encryption eliminates the need for the proxy server to decrypt and re-encrypt the data, further enhancing data security. The blockchain network ensures the transparency and integrity of data sharing transactions, preventing unauthorized access and tampering. Overall, the system provides a robust and scalable solution for secure data sharing in the IoT ecosystem, fostering trust and privacy among participating devices.

PROPOSED SYSTEM ANDADVANTAGES

- 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.
- The proposed system finds Data Tampering and blocks when hackers compromise a system, they inject their own versions of the data into the system.

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 tostore 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.

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 Common. 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, “Publickey 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. Secure. 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, Protos. Compute. 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. Compute. Common. 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 INFOCOM2004, 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 Net w., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., "Trace-driven analysis of ICN caching algorithmson 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 CashSystem, 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 fine-grained data access control in cloud computing," in Proc. IEEEINFOCOM, Mar. 2010, pp. 1–9.

[16] N. Park, "Secure dataaccess control scheme using type-based reen cryption in cloud environment," in Semantic Methods Knowledge Management 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 efficiency in attribute- based data sharing," 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-basedproxy 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 fine-grained access control mechanism for networked storage systems," in Proc. IEEE6thInt. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.

[23] Y. Zhou et al., "Identity-based proxy re-encryption version 2: Making mobile accesseasy 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.