ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue 2, 2024

A PROXY RE-ENCRYPTION APPROACH TO SECURE DATA SHARING IN THE IOT BASED ON BLOCK CHAIN

[1]SMT.S ARUNA, [2]PANJA CHAITANYA VENKATA PADMARAO

[1](Assistant Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Among the many beneficial uses of the Internet of Things in cloud computing, data sharing has emerged as a prominent trend in its development. Data security is still a challenge for this technology, despite its allure, as improper data usage causes many harms. To ensure the safety of data transfer in cloud settings, we provide a proxy re-encryption method in this piece. With identity-based encryption, data owners may send their encrypted files to the cloud, where they will remain secure. Proxy re-encryption construction ensures that only authorized users can access the files. Due to resource constraints on IoT devices, edge devices perform expensive calculations as a proxy server. Furthermore, we optimize the use of network capacity and enhance service quality by using information-centric networking capabilities to efficiently transport cached material in the proxy. Decentralization of data sharing is made possible by blockchain, a revolutionary technology that forms the basis of our system paradigm. It accomplishes granular data access control while reducing the strain on centralized systems. Our strategy shows promise in protecting the privacy, authenticity, and integrity of data, according to the security study and assessment of our plan.

1.INTRODUCTION

Over the years, network traffic levels have grown substantially due to the proliferation of the Internet of Things (IOT), a technology that has developed into a major player in today's world. In the future, it is anticipated that several gadgets will attain connectivity. With its many uses in fields as diverse as medicine, transportation, smart cities, industry, and manufacturing, data is vital to the Internet of Things (IoT) paradigm. Stakeholders benefit greatly from the sensor readings, which cover a wide range of vital factors. In light of this, new threats to privacy and security have emerged alongside the seemingly endless benefits of the Internet of Things (IoT). Internet of Things (IoT) security is essential to prevent intrusions that compromise data privacy, integrity, or confidentiality or that prevent it from delivering the necessary services. Implementing data encryption prior to outsourcing to cloud servers is a practical and effective approach. Whenever standard security protocols are bypassed, the material is only viewable in its encrypted form to attackers. Every piece of data that is shared has to be encrypted right from the start so that only authorized users can decode it. You may utilize standard encryption methods, where the data owner names all the people who will have access to the decryption key. Anyone using symmetric encryption must be in agreement on a key, or the data owner and users must share the same key. It is clear that this method is not particularly efficient. The data owners also don't know who will be using their data, so they have to decrypt it and then encrypt it again using a key that they and the users know. To use this decrypt-and-encrypt method, the data owner would need constant internet access, which is obviously impractical. With more data points and different people involved as owners and consumers, the issue becomes bigger and more complicated.

While basic, conventional encryption methods are ill-suited for data sharing due to the complexity of key management procedures. The concept of proxy re-encryption (PRE), first put out by Blaze et al., enables a proxy to convert a file encrypted using a delegator's public key into an encryption suitable for a delegatee. Arrange for the data user to be the delegate and the data owner to be the delegator. This method allows the data owner to briefly communicate with the user using encrypted communications without disclosing his secret key. It is the data owner or an authorized third party who produces the key for re-encryption. A third party, acting as a proxy, uses the key to re-encrypt the cipher text, making it more secure and secure before the user receives it. One characteristic of a PRE scheme is that the proxy is not completely trusted, since it does not know the private key of the data owner. Because of its apparent suitability for securely assigning access to encrypted data, an essential feature of any data-sharing situation, this is being considered strongly. Beyond that, PRE enables the secure transfer of encrypted data stored in the cloud to authorized users while protecting it from unauthorized parties. Using encryption, only authorized individuals may access the outsourced data, reducing the likelihood of data exposures.

In response to this situation, the authors of this piece suggest enhancing IoT data exchange via the integration of PRE, IBE, ICN, and blockchain technologies. The idea of identity-based encryption (IBE), initially proposed by Shamir, allows a sender to encrypt a message and deliver it to a receiver by utilizing the recipient's email address as the public key. A number of cryptographic protocols have been built around it, such as public-key searchable encryption, secret handshakes, and selected cipher text attack (CCA) secure public-key encryption. It is a highly strong basic that is used to overcome many key distribution difficulties. The resource-constrained IoT devices cannot handle the intensive calculations required by attribute-based encryption (ABE) for data encryption, decryption, and key management, so IBE is considered superior. This essay gains more weight by adapting the concept of ICN to meet the needs of the evolving information sharing landscape.

To address the need for low-latency applications, the idea of ICN was created. In this model, data owners may distribute and label their data in a way that makes it replicable and saves it in network caches. This guarantees effective data transmission and usage of network capacity, which is essential for the IoT ecosystem despite the exponential increase in network traffic. When it comes to trust, Nakamoto proposed a distributed, decentralized system that can provide safe and trustworthy data sharing. The capacity of this technology to maintain the confidentiality of personal information has made it a hot topic; it is known as blockchain. Despite optimization challenges with storing massive amounts of data, new system applications have used blockchain access control in database administration. Using blockchain technology, data confidentiality and user revocation may also be accomplished. The security and privacy of data-sharing systems will be improved by combining PRE with IBE, ICN, and blockchain aspects.

A high level of service for data delivery is guaranteed by the ICN concept, thanks to in-network caching, which allows for efficient distribution of data, and by PRE and IBE, granular data access control is assured. Because of its design, the blockchain is able to provide a trustworthy system across network nodes while also minimizing storage and data-sharing overheads. As we discussed in the essay, the data owner propagates an ACL that is recorded on the blockchain. A limited set of authorized users have access to the data.

2.LITERATURE SURVEY

In the domain of secure data sharing in the Internet of Things (IoT) based on blockchain technology, several researchers have explored various approaches and techniques to enhance data security and privacy. Here is a literature survey based on the works of scholars in this field:

Proxy Re-Encryption (PRE) for IoT Data Sharing:

Aksu et al.: Proposed a PRE approach for secure data sharing in IoT environments. They focused on efficient re-encryption mechanisms to ensure data confidentiality and integrity.

Li et al.: Introduced a dynamic and efficient PRE scheme for IoT data sharing. Their approach aimed to minimize the computational overhead on resource-constrained IoT devices.

Blockchain Technology for Secure Data Sharing:

Nakamoto: Introduced blockchain as a decentralized and secure approach for data management and access control. Their work laid the foundation for using blockchain in IoT applications.

Zyskind et al.: Presented a blockchain-based model for distributed personal data management. They focused on ensuring privacy and access control without the need for a centralized authority.

Integration of Information-Centric Networking (ICN):

Jacobson et al.: Proposed the concept of ICN for efficient data delivery and utilization of network resources. Their work emphasized the importance of caching and content-based routing in IoT environments.

Ahlgren et al.: Explored the integration of ICN with IoT architectures. They highlighted the benefits of ICN in improving data delivery and reducing latency in IoT networks.

These studies demonstrate the ongoing efforts to enhance data security and privacy in IoT environments through the integration of PRE, blockchain technology, and ICN. These methodologies mean to address the difficulties of secure information sharing and access control in IoT applications.

3. EXISTING SYSTEM

To prevent service providers and revoked users from working together, Park proposed an amendment to the plan in. Their plan called for a third party to step in and take the role of the service provider, suggesting that a higher level of trust is required. While some techniques have used secret keys to encrypt data, others have used ciphertext-policy ABE (CP-ABE), which involves associating the access policy with the ciphertext. In addition, Liu et al. suggested an ABE and PRE-based time-constrained access control mechanism. Time-based access control rules were designed using ABE, and time attributes were updated using PRE. Despite these methods' benefits, the extensive calculations required for encryption and decryption make them unsuitable for use in the context of the Internet of Things (IoT).

By presenting an IBE PRE scheme that is well-suited for data sharing, Han et al. The re-encryption keys were associated with both the users' identities and a particular ciphertext. Because of this, the data owner was compelled to generate a unique re-encryption key for every combination of data user and shared file. Instead of an identity-based PRE, Lin et al. suggested a hierarchical PRE that was conceptually comparable. When dealing with complicated and many bits of data, these two techniques often fail to provide satisfactory results. Zhou et al. presented a method for exchanging data that combines PRE with identity-based broadcast encryption (IBBE). They came up with a hybrid technique that could convert between the two protocols securely, without exposing any private data. Additionally, Wang et al. developed a system for accessing health records called identity-based PRE (IBPRE). Achieving coarse-grained access control was the goal of the approach.

After receiving the re-encryption key from the data owner, a proxy has the option to re-encrypt all ciphertexts and make them available to the intended users, or not re-encrypt any at all. To that end, Shao et al. put forth a conditionally-based IBE PRE scheme. According to their plan, the proxy might change the encryption of certain ciphertexts using one identity to another. However, it was not possible to approve a set of users to have decryption privileges. Not only that, but PRE has also been used to lessen the impact of IoT security issues.

Distributed personal data management with privacy assurance was implemented by Zyskind et al. using blockchain technology. There was no need for a middleman since the blockchain was used as an automated ACL manager. The implementation of data storage on the blockchain was a distributed hash table, and the only data kept there was the address. The possibility of sensitive information leaking out was minimalized as a result.

In a comparable scenario, Fan et al. envisioned uploading encrypted data to the cloud and storing data access rules on the blockchain as transactions. While both techniques provide tamper-proof systems and simple auditing, the usage of public blockchains causes access rules to leak as they are available to everyone. To facilitate safe communication between cars and to facilitate data exchange in vehicular networks, Singh and Kim introduced a concept based on blockchain technology. Due to the high expense of creating a public blockchain in cars with limited resources, it is not practical to utilize public blockchains for peer-to-peer (P2P) data exchange among vehicles.

Disadvantages:

Not a single system was put into place. Outsourced data is less secure because of attribute-based encryption and the absence of identity-based encryption in the system.

PROPOSED SYSTEM

The system achieves fine-grained access to data and presents a safe access control mechanism to realize data secrecy. In addition to ensuring data privacy and security, this will also provide full control to data owners. • The system explains our PRE strategy in detail and implements a comprehensive protocol.

The edge devices re-encrypt the cached data and act as proxy nodes to enhance data delivery and make better use of the network capacity. It is believed that the edge devices provide high-performance networking due to their superior computational capabilities compared to the IoT devices.We show the results of our scheme's security examination, put it through its paces, and compare it to other schemes.

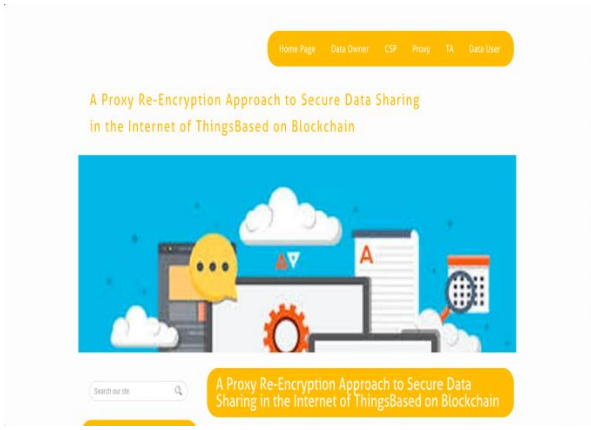
Advantages:

The suggested approach has the advantage of being resistant to man-in-the-middle (MITM) assaults. The purpose of a man-in-the-middle attack is to get counterfeit public keys and provide them to the certificate authority (CA).

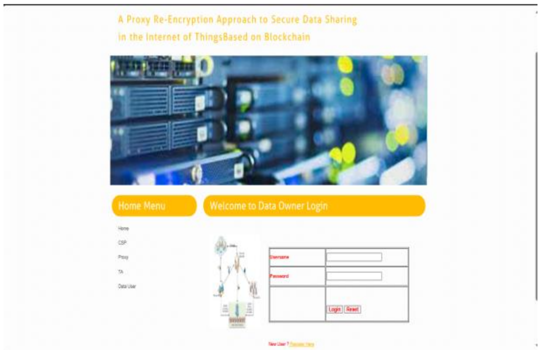
If the suggested approach is successful in detecting data tampering, it will prevent hackers from injecting their own versions of data into compromised systems.

.4. OUTPUT SCREENS

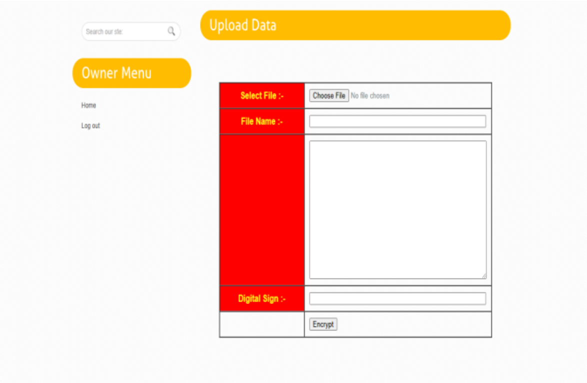
Home Page:


Home Page
Data Owner
CSP
Proxy
TA
Data User
A Proxy Re-Encryption Approach to Secure Data Sharing
in the Internet of ThingsBased on Blockchain
Search our site
A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of ThingsBased on Blockchain

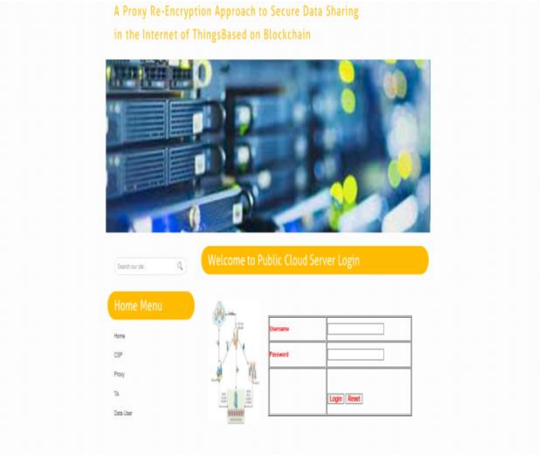
Data owner Login:


A Proxy Re-Encryption Approach to Secure Data Sharing
in the Internet of ThingsBased on Blockchain
Home Menu
Welcome to Data Owner Login
Home
CSP
Proxy
TA
Data User
Username
Password
Login
Reset
New User ? Register Here

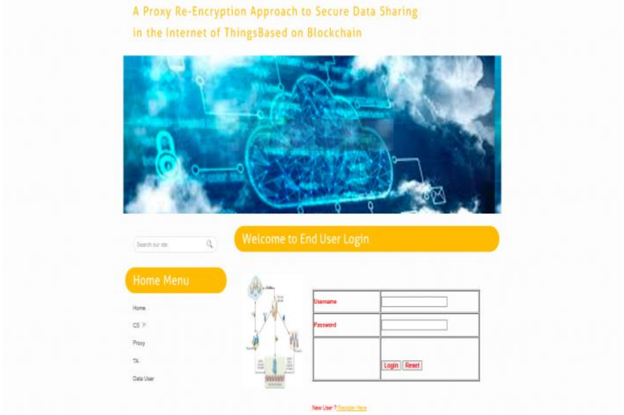
Upload Data:



Public Cloud Server login:


A Proxy Re-Encryption Approach to Secure Data Sharing
in the Internet of ThingsBased on Blockchain
Search our site
Welcome to Public Cloud Server Login
Home Menu
Home
CSP
Proxy
TA
Data User
Username
Password
Login
Reset

End User Login:



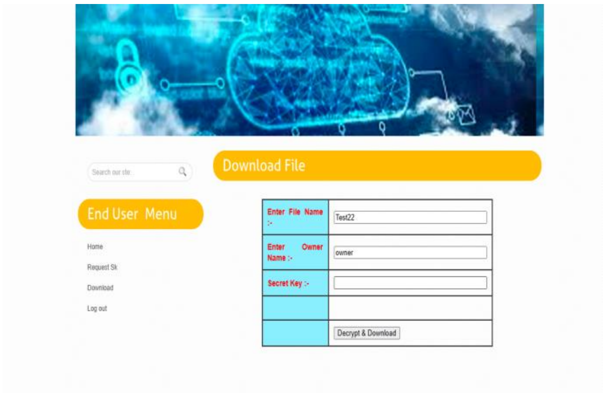
A Proxy Re-Encryption Approach to Secure Data Sharing
in the Internet of ThingsBased on Blockchain

Welcome to End User Login

Username	
Password	
	Login Reset

New User ? Register Here

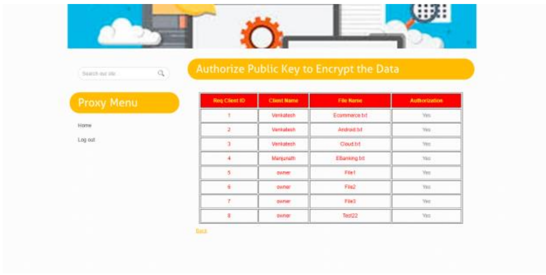
Download Data:



Download File

Enter File Name :-	Test22
Enter Owner Name :-	owner
Secret Key :-	
	Decrypt & Download

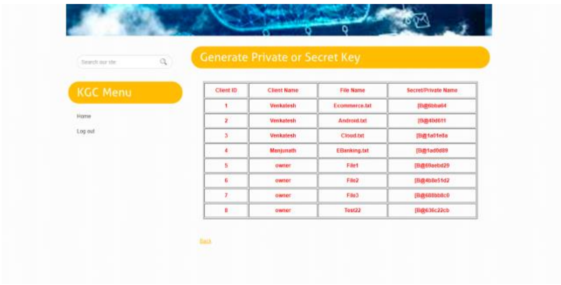
Proxy Menu:



Authorize Public Key to Encrypt the Data

Req Client ID	Client Name	File Name	Authorization
1	Venkatesh	Ecommerce.txt	Yes
2	Venkatesh	Android.txt	Yes
3	Venkatesh	Cloud.txt	Yes
4	Manjunath	EBanking.txt	Yes
5	owner	File1	Yes
6	owner	File2	Yes
7	owner	File3	Yes
8	owner	Test22	Yes

KGC Menu:



Generate Private or Secret Key

Client ID	Client Name	File Name	Secret/Private Name
1	Venkatesh	Ecommerce.txt	[B@6bba64
2	Venkatesh	Android.txt	[B@40d611
3	Venkatesh	Cloud.txt	[B@1a01e8a
4	Manjunath	EBanking.txt	[B@1ad0d89
5	owner	File1	[B@69aebd29
6	owner	File2	[B@4b8e51d2
7	owner	File3	[B@688bb8c0
8	owner	Test22	[B@636c22cb

5. CONCLUSION

One of the most notable uses of the Internet of Things (IoT) since its inception has been data sharing. We present a safe identity-based PRE data-sharing strategy for the cloud that ensures privacy, secrecy, and integrity of data. Data owners can store protected data in the cloud and distribute it efficiently with legitimate users using the IBPRE technology, which realizes secure data sharing. The intensive computations are handled by an edge device as a proxy due to resource constraints. In order to efficiently provide cached material, the scheme additionally uses ICN features. This improves service quality and makes great use of the network bandwidth. Next, we show a model of the system that is built on the blockchain and permits flexible authorization on encrypted data. Data owners can accomplish acceptable privacy preservation with the help of fine-grained access control. In comparison to other schemes, ours is far more efficient, as shown by the analysis and outcomes of the suggested model.

6.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 videoon-demandworkloads,” in *Proc. 10th ACMInt. 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 fine-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 reencryption 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-encryptionbased 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, 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.

[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.