Secure Data Sharing using A Proxy Re-Encryption Approach in the IoT Based on Blockchain

Uppala Venkatachaitanya, studentmember, M.Tech (CSE) , Project Guide, Dr.Shaik Jaffar Hussain, Associate Professor and Head of Computer Science and Engineering Department, Sri Venkateswara Institute of Science and Technology,, Kadapa.

ABSTRACT

The evolution of the Internet of Things has viewed records sharing as one of its most beneficial functions in cloud computing. As appealing as this technological know-how has been, records protection stays one of the barriers it faces on account that the wrongful use of facts leads to quite a few damages. In this article, we advise a proxy re-encryption strategy to impervious statistics sharing in cloud environments. Data proprietors can outsource their encrypted records to the cloud the usage of identity-based encryption, whilst proxy re-encryption development will supply professional customers get admission to to the data. With the Internet of Things units being resource-constrained, an area system acts as a proxy server to manage intensive computations. Also, we make use of the points of information-centric networking to supply cached content material in the proxy effectively, as a consequence enhancing the first-rate of carrier and making appropriate use of the community bandwidth. Further, our device mannequin is primarily based on blockchain, a disruptive technological know-how that allows decentralization in statistics sharing. It mitigates the bottlenecks in centralized structures and achieves fine-grained get entry to manipulate to data. The safety evaluation and assessment of our scheme exhibit the promise of our strategy in making sure facts confidentiality, integrity, and security.

1. INTRODUCTION

The Internet of Things (IOT) has emerged as a science that has superb value to the world at present and its utilization has given upward jostle to an multiplied boom in community visitors volumes over the years. It is anticipated that a lot of gadgets will get related in the years ahead. Data is a central idea to the IoT paradigm as the statistics amassed serves various functions in functions such as healthcare, vehicular networks, clever cities, industries, and manufacturing, amongst others . The sensors measure a host of parameters that are very

beneficial for stakeholders involved. Consequently, as engaging as IoT appears to be, its development has brought new challenges to safety and privacy.

IoT wants to be secured towards assaults that restrict it from supplying the required services, in addition to these that pose threats to the.
A attainable answer is to encrypt the statistics earlier than outsourcing to the cloud servers. Attackers can solely see the records in its encrypted shape when normal protection measures fail. In facts sharing, any facts need to be encrypted from the supply and solely decrypted by way of licensed customers in order to hold its protection. Conventional encryption methods can be used, the place the decryption key is shared amongst all the statistics customers special with the aid of the facts owner.

The use of symmetric encryption implies that the identical key is shared between the records proprietor and users, or at least the contributors agree on a key. This answer is very inefficient. Furthermore, the statistics proprietors do no longer be aware of in improve who the meant statistics customers are, and, therefore, the encrypted information wants to be decrypted and as a result encrypted with a key recognised to each the statistics proprietor and the users. This decrypt-and-encrypt answer potential the information proprietor has to be on-line all the time, which is virtually no longer feasible.

The trouble will become increasingly more complicated when there are a couple of portions of records and various information proprietors Although simple, the ordinary encryption schemes contain complicated key administration protocols and, hence, are no longer apt for records sharing. Proxy re-encryption (PRE), a thinking first proposed by using Blaze et al. , approves a proxy to radically change a file computed below a delegator's public key into an encryption meant for a delegatee. Let the information proprietor be the delegator and the information person be the delegate. In such a scheme, the statistics proprietor can ship encrypted messages to the person quickly barring revealing his secret key.

The information proprietor or a depended on 0.33 birthday celebration generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the cipher textual content earlier than sending the new cipher textual content to the user. An intrinsic trait of a PRE scheme is that the proxy is no longer completely relied on (it has no thought of

the facts owner's secret key).

This is considered as a high candidate for delegating get entry to to encrypted records in a secured manner, which is a fundamental factor in any data-sharing scenario. In addition, PRE lets in for encrypted facts in the cloud to be shared to approved customers whilst preserving its confidentiality from illegitimate parties. Data disclosures can be minimized thru the use of encryption on the grounds that solely customers delegated through the records proprietor can successfully get right of entry to the outsourced data. Motivated by means of this scenario, this article proposes an enchancment in IOT information sharing through combining PRE with identification based totally encryption (IBE), information-centric networking (ICN), and block chain technology.

Shamir first introduced the thought of IBE, in which a sender encrypts a message to a recipient the usage of the identification (email) as the public key. It is a very effective primitive used to fight severa key distribution troubles and has consented to the improvement of countless cryptographic protocols, which include public-key searchable encryption, secret handshakes , and chosen cipher textual content assault (CCA) invulnerable public-key encryption .

IBE is desired over attribute-based encryption (ABE) due to the fact ABE includes heavy computations on records encryption, decryption, and key management, and these procedures are no longer handy for the resource-constrained IoT devices. The power of this article is extended by using borrowing the thought of ICN to cater for the The enchantment for low-latency functions brought the thinking of ICN , the place information proprietors can distribute and assign special names to their statistics which can be replicated and saved in community caches.

This ensures that there is an efficient information transport and utilization of community bandwidth, which is a prerequisite for the IOT ecosystem regardless of the sizeable increase in community volumes. On problems of trust, a decentralized, dispensed gadget that can smoothen impervious and depended on records sharing was once brought through Nakamoto . This is the block chain technology, and it has won a whole lot interest due to its capability to maintain records privacy.

Although there exist optimization troubles when storing widespread sizes of data, rising machine purposes have used the

block chain for get admission to manipulate in database management. Data confidentiality and consumer revocation can additionally be performed the usage of block chain. PRE, collectively with IBE and the elements of ICN and block chain, will decorate safety and privateness in data-sharing systems.
PRE and IBE will make certain fine-grained records get right of entry to control, whilst the notion of ICN guarantees a enough satisfactory of carrier in statistics shipping due to the fact the in-network caching offers environment friendly distribution of data. The block chain is optimized to forestall storage and data-sharing overheads and additionally to make sure a depended on device amongst entities on the network.

In our article, the information proprietor propagates an get entry to manage listing which is saved on the block chain. Only the licensed customers are in a position to get entry to the data. The contributions of this article are summarized.
1) We suggest a invulnerable get right of entry to manage framework to comprehend records confidentiality, and nice grained get entry to to information are achieved. This will additionally
2) We supply a particular description of our PRE scheme and the actualization of a entire protocol that ensures safety and privateers of data.
3) To enhance information shipping and successfully make use of the community bandwidth, side gadgets serve as proxy nodes and function re-encryption on the cached data.

The aspect gadgets are assumed to have ample computation abilities than the IOT units and as such furnish excessive overall performance networking.
The safety evaluation of our scheme is presented, and we additionally take a look at and evaluate its overall performance with present schemes.

2. LITERATURE SURVEY

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash,“Internet of Things: A survey on enabling technologies, protocols, andapplications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376,Oct./Dec. 2015.

This paper affords an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and software issues. The IoT is enabled with the aid of the modern-day trends in RFID, clever sensors, verbal exchange technologies, and Internet protocols. The fundamental premise is to have clever

sensors collaborate immediately besides human involvement to supply a new type of applications. The modern-day revolution in Internet, mobile, and machine-to-machine (M2M) applied sciences can be considered as the first section of the IoT.

In the coming years, the IoT is predicted to bridge numerous applied sciences to allow new functions via connecting bodily objects collectively in assist of clever selection making. This paper starts offevolved by way of offering a horizontal overview of the IoT. Then, we supply an overview of some technical important points that pertain to the IoT enabling technologies, protocols, and applications. Compared to different survey papers in the field, our goal is to grant a greater thorough precis of the most applicable protocols and software troubles to allow researchers and utility builders to get up to pace shortly on how the specific protocols in shape collectively to supply favored functionalities except having to go thru RFCs and the requirements specifications.

We additionally supply an overview of some of the key IoT challenges introduced in the current literature and grant a precis of associated lookup work. Moreover, we discover the relation between the IoT and different rising applied sciences which includes large facts analytics and cloud and fog computing. We additionally existing the want for higher horizontal integration amongst IoT services. Finally, we existing specific provider use-cases to illustrate how the one-of-a-kind protocols introduced in the paper suit collectively to supply preferred IoT services.
2. D. Balfanzet al., "Secret handshakes from pairing-based key agreements,"in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

Consider a CIA agent who needs to authenticate herself to a server however does no longer choose to disclose her CIA credentials until the server is a authentic CIA outlet. Consider additionally that the CIA server does now not prefer to divulge its CIA credentials to everyone however CIA retailers - no longer even to different CIA servers. We first exhibit how pairing-based cryptography can be used to enforce such secret handshakes. We then advocate a formal definition for tightly closed secret handshakes, and show that our pairing-based schemes are invulnerable beneath the Bilinear Diffie-Hellman assumption. Our protocols help role-based team membership authentication, traceability, indistinguishability to eavesdroppers,

unbounded collusion resistance, and ahead repudiability. Our secret-handshake scheme can be carried out as a TLS cipher suite. We record on the overall performance of our preliminary Java implementation.

3. A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme forcontent-based networking," in Proc. IEEE INFOCOM 2004, vol. 2, 2004,pp. 918–928.

This work proposes a routing scheme for content-based networking. A content-based community is a verbal exchange community that aspects a new superior conversation mannequin the place messages are now not given specific vacation spot addresses, and the place the destinations of a message are decided via matching the content material of the message in opposition to decision predicates declared by means of nodes. Routing in a content-based community quantities to propagating predicates and the vital topological records in order to preserve loop-free and perchance minimal forwarding paths for messages.

The routing scheme we recommend makes use of a mixture of a ordinary broadcast protocol and a content-based routing protocol. We existing the mixed scheme and its requirements over the broadcast protocol. We then element the content-based routing protocol, highlighting a set of optimization heuristics. We additionally existing the consequences of our evaluation, displaying that this routing scheme is high quality and scalable.

4. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, andfine-grained facts get admission to manipulate in cloud computing," in Proc. IEEEINFOCOM, Mar. 2010, pp. 1–9.

Cloud computing is an rising computing paradigm in which assets of the computing infrastructure are furnished as offerings over the Internet. As promising as it is, this paradigm additionally brings forth many new challenges for information protection and get admission to manage when customers outsource touchy facts for sharing on cloud servers, which are now not inside the identical relied on area as records owners. To maintain touchy consumer information private towards untrusted servers, current options generally follow cryptographic techniques by means of disclosing information decryption keys solely to approved users. However, in doing so, these options inevitably introduce a heavy computation overhead on the facts owner for key distribution and records

administration when fine-grained statistics get admission to manage is desired, and hence do no longer scale well.

The hassle of concurrently accomplishing fine-grainedness, scalability, and information confidentiality of get right of entry to manage without a doubt nevertheless stays unresolved. This paper addresses this difficult open difficulty by, on one hand, defining and imposing get right of entry to insurance policies primarily based on statistics attributes, and, on the different hand, permitting the statistics proprietor to delegate most of the computation duties concerned in fine-grained facts get admission to manage to untrusted cloud servers besides disclosing the underlying facts contents.

We acquire this purpose by way of exploiting and uniquely combining strategies of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme additionally has salient homes of consumer get admission to privilege confidentiality and consumer secret key accountability. Extensive evaluation suggests that our proposed scheme is pretty environment friendly and provably impenetrable underneath present safety models.

5. J. Hur, "Improving protection and effectivity in attribute-based statistics sharing,"IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282,Apr. 2011.

With the latest adoption and diffusion of the records sharing paradigm in dispensed structures such as on-line social networks or cloud computing, there have been growing needs and worries for dispensed facts security. One of the most difficult troubles in facts sharing structures is the enforcement of get right of entry to insurance policies and the assist of insurance policies updates. Ciphertext coverage attribute-based encryption (CP-ABE) is turning into a promising cryptographic answer to this issue. It permits facts proprietors to define their very own get right of entry to insurance policies over person attributes and put in force the insurance policies on the information to be distributed. However, the gain comes with a main disadvantage which is recognised as a key escrow problem. The key technology middle may want to decrypt any messages addressed to particular customers by means of producing their non-public keys. This is no longer appropriate for statistics sharing situations the place the

facts proprietor would like to make their non-public facts solely reachable to particular users. In addition, making use of CP-ABE in the information sharing gadget introduces any other task with regard to the consumer revocation considering that the get admission to insurance policies are described only over the attribute universe. Therefore, in this study, we advocate a novel CP-ABE scheme for a statistics sharing device via exploiting the attribute of the gadget architecture.

The proposed scheme facets the following achievements: 1) the key escrow hassle ought to be solved by using escrow-free key issuing protocol, which is developed the use of the tightly closed two-party computation between the key technology middle and the data-storing center, and 2) fine-grained consumer revocation per every attribute may want to be accomplished by means of proxy encryption which takes benefit of the selective attribute crew key distribution on pinnacle of the ABE. The overall performance and protection analyses point out that the proposed scheme is environment friendly to securely control the statistics dispensed in the records sharing system.

3. EXISTING SYSTEM

As Park supplied a change to the scheme in , the place collusion between the provider company and revoked customers is avoided. Their scheme was once to essentially substitute the provider company with a depended on 1/3 party, which implies that there need to be reliance on more advantageous have faith assumption. Other schemes have made comparable procedures however utilized ciphertext-policy ABE (CP-ABE) rather, in which the get right of entry to coverage is related with the ciphertext as a substitute of the secret keys. Liu et al.

additionally proposed a time-constrained get entry to manage scheme based totally on PRE and ABE. ABE was once used to sketch time-based get right of entry to manage insurance policies whilst PREwas used to replace the time attributes. Although these schemes have their advantages, they are no longer appropriate in the context of IoT due to the heavy computations on encryption and decryption. An IBE PRE scheme appropriate for facts sharing was once introduced through Han et al. in . The re-encryption keys had been now not solely sure to the users' identities however additionally to a particular ciphertext.

This implied that the facts proprietor had to create a one of a kind reencryption key for every pair of facts person and shared file. A comparable notion was once proposed by way of Lin et al. the place they used a hierarchical PRE alternatively of an identity-based PRE. These two schemes have a tendency to be inefficient when more than one and complicated facts portions are considered. An identity-based broadcast encryption (IBBE) blended with PRE used to be proposed through Zhou et al. in for statistics sharing.

Their scheme used to be a hybrid one that allowed the conversion to be carried out between the two protocols withoutleaking any touchy information.Wanget al. additionally designed an identity-based PRE (IBPRE) scheme for having access to fitness records. The scheme finished coarse-grained get admission to control.
If a proxy receives the re-encryption key from the statistics owner, both all the ciphertexts can be re-encrypted and available to the meant customers or none at all. On that note, Shao et al. proposed an IBEPREscheme that is based totally on conditions. In their proposal, the proxy may want to radically change a subset of ciphertexts underneath an identification to different ciphertexts beneath any other identity. However, decryption rights to a crew of customers should no longer be authorized. In addition to the above, PRE has been used to mitigate safety troubles in IoT .Zyskindet al. used blockchain to furnish disbursed non-public records administration and make sure privateness as well. The blockchain was once utilized as an computerized get admission to manage manager, and, hence, no 0.33 birthday celebration used to be required. Only the statistics tackle used to be saved on the blockchain and a allotted hash desk was once used as the implementation of the statistics storage. This decreased the chance of statistics leakage.
Fan et al. designed a comparable mannequin to the place the encrypted statistics is uploaded to the cloud and get right of entry to insurance policies on the facts are saved on the blockchain as transactions. Although these two schemes gain tamper-proof structures and effortless auditing, there is a leakage of get right of entry to insurance policies on account that the blockchains used are public ones and are accordingly seen to everyone. Singh and Kimpresented a blockchain-based mannequin for sharing records in vehicular networks and additionally allow impenetrable verbal exchange amongst vehicles. However, the

use of a public blockchain does no longer work nicely in peer-to-peer (P2P) records sharing amongst cars due to the excessive price concerned in setting up a public blockchain in resource-constrained vehicles.

Disadvantages

1) The machine used to be no longer applied Attribute Based Encryption Mentod which leads much less protection on outsourced data.

2) The machine is much less protection due to lack of Identity-Based Encryption.

4. PROPOSED SYSTEM

The machine proposes a impenetrable get right of entry to manage framework to comprehend facts confidentiality, and fine-grained get right of entry to to facts are achieved.

This will additionally warranty records owners' whole manipulate over their data. The machine offers a specific description of our PRE scheme and the actualization of a entire protocol that ensures protection and privateness of data. To enhance information shipping and correctly make use of the community bandwidth, part gadgets serve as proxy nodes and operate re-encryption on the cached data. The area gadgets are assumed to have ample computation abilities than the IoT units and as such supply excessive performance networking. The safety evaluation of our scheme is presented, and we additionally check and examine its overall performance with current schemes.

Advantages

1) The proposed device is impenetrable in opposition to man-in-the-middle (MITM) attacks. MITM assaults get to the certificates authority (CA) to furnish the consumer with cast public keys.

2) The proposed gadget finds Data Tampering and blocks when hackers compromise a system, they inject their personal variations of the facts into the system.

.

5. MODULES

5.1 Data Owner: In this module, the information proprietor uploads their statistics in the public cloud server. For the safety reason the facts proprietor encrypts the facts file and assigns the digital signal and then keep in the cloud. The statistics proprietor can take a look at the statistics integrity of the file over Corresponding cloud server.

The Data proprietor can have succesful of; manipulating the encrypted facts file and records proprietor can replace the file contents as properly as delete his personal

file.

5.2 Key Generation Centre: In this module, the KGC Generates the Secret Key requested through the facts user, the KGC assessments the file if current generates the gorgeous Secret Key. The KG-CSP approves viewing the Secret Key generated archives and additionally the transactions associated to the file.

5.3 Proxy Server: The server will manipulate and authorize Users and preserve all information transactions between records proprietor and cloud server, cease user.

5.4 Data User Module: In this module, Data consumer logs in through the usage of his consumer identify and password. After he will request for secret key of required file from CSP, and get the secrete key from KGC. After getting secrete key he is making an attempt to down load file by means of getting into file title and secrete key from cloud server.

5.5 Data Encryption and Decryption: All the prison customers in the gadget can freely question any involved encrypted and decrypted data. Upon receiving the statistics from the server, the consumer runs the decryption algorithm Decrypt to decrypt the cipher textual content with the aid of the use of its secret keys from extraordinary Users. Only the attributes the consumer possesses fulfill the get admission to shape described in the cipher textual content CT, the consumer can get the content.

5.6 Attacker Module : In Data person module, whilst downloading time if far off person enters incorrect trapdoor or secrete key then he is handled as Digital signal attacker or Secret Key attacker.

5.7 Data Integrity Check: Data will be confirmed in the cloud to take a look at it is built-in with the aid of attacker or not. If it is built-in then it is convalescing from the information owner.

6. CONCLUSION

The emergence of the IOT has made information sharing one of its most distinguished applications. To warranty information confidentiality, integrity, and privacy, we advocate a impervious identity-based PRE data-sharing scheme in a cloud computing environment. Secure facts sharing is realized with IBPRE technique, which permits the records proprietors to keep their encrypted information in the cloud and share them with professional customers efficiently. Due to aid constraints, an aspect gadget serves as the proxy to cope with the intensive computations. The scheme additionally accommodates the elements of ICN to proficiently supply

cached content, thereby enhancing the fine of carrier and making terrific use of the community bandwidth. Then, we existing a block chain-based gadget mannequin that permits for bendy authorization on encrypted data. Fine grained get right of entry to manipulate is achieved, and it can assist facts proprietors attain privateness renovation in an ample way. The evaluation and effects of the proposed mannequin exhibit how environment friendly our scheme is, in contrast to current schemes.

BIBLIOGRAPHY

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash,"Internet of Things: A survey on enabling technologies, protocols, andapplications," 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 atomicproxy cryptography," in Proc. Int. Conf. Theory Appl. CryptographicTechn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," inProc.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.CryptographicTechn., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building anencrypted and searchable audit log," in NDSS, vol. 4. Citeseer, Feb. 2004,pp. 5–6.

[6] D. Balfanzet 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 fromidentity-based encryption," in Proc. Int. Conf. Theory Appl. CryptographicTechn., Springer, 2004, pp. 207–222.

[8] T. Koponenet 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, "Developinginformation 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 namingfor 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 forcontent-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, andfine-grained data access control in cloud computing,” in Proc. IEEEINFOCOM, Mar. 2010, pp. 1–9.

[16] N. Park, “Secure data access control scheme using type-based reencryptionin cloud environment,” in Semantic Methods Knowledge Managementand Communications. Berlin,Germany: Springer, 2011, pp. 319–327.

[17] G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-basedencryption 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-encryptionbasedkey management for secure and scalable mobile applicationsin 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 schemefor 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 cloudcomputing,” 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 accesscontrol 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: Makingmobile 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 securee-health cloud system using identity based cryptographic techniques,”Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.