Secure Multiple Authorities for Blockchain in Electronic Health Records Systems

[1]Arfa Mahwish [2]Dr.K.Srinivas

[1]PG Scholar, Dept of CSE [2] Professor, Dept of CSE

CMR Technical Campus, Medchal, Hyderabad CMR Technical Campus, Medchal,Hyderabad

(E-mail:-arfamahwish28@gmail.com) (E-mail:- phdknr@gmail.com)

ABSTRACT:-

Electronic Health Records (EHRs) are completely handled by hospitals instead of patients, which complicates seeking medical advices from different hospitals. Patients face a critical need to focus on the details of the own health care and restore management of their own medical data. The high development of block chain technology promotes population healthcare, with medical records as well as the patient-related information. This technology provides patients data with immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in block chain, here we present an attribute-based signature method with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no data other than the proof that he has attested to it. By distributing the secret pseudorandom function seeds among various authorities, this rule resists collusion attack out of N from N−1 corrupted authorities. Under the statement of the computation albilinear Diffie-Hellman, we also formally explain that, in terms of the unforgetability and perfect privacy of the attribute-signer, this attribute-based signature method is secure in the random oracle model. The comparisons how the efficiency and properties between the proposed method and methods proposed in other studies.

KEYWORDS:-

Attribute-based signature (ABS), blockchain, electronic health records (EHRs), multiple authorities, preserve privacy.

I.INTRODUCTION:-

Electronic Health Records (EHRs) provides a comfortable health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system is designed to allow patients to access the control of generating and sharing EHRs with family, friends, healthcare providers and other authorized data consumers .Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be gained. moreover, in the present situation, patients separate their EHRs among the different areas during life events, causing the EHRs to move from one service provider database to another. hence, the patient may lose control of the existing healthcare data, while the service provider normally maintains the primary steward ship. Patient access permissions to EHRs are very restricted, and patients are hardly unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research institutions, etc. add extra barriers to high-performance data sharing. If the patient has the capacity of managing and sharing his EHRs securely and completely, regardless of the research purpose or the data sharing among healthcare providers, the healthcare industry will benefits greatly. Drawing support from block chain technology, the proposed method accomplishes this goal is to promote cooperation in the way of deep mutual trust between each organization.

In todays life cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a heavy success with its capital market reaching 10 billion dollars in 2016 [1]. With a specially modelled data storage architecture, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is *blockchain*, which was first proposed in 2008 and implemented in 2009 [2]. Blockchain could be regarded as a public ledger and all transactions are stored in a list of blocks. This chain improves as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been developed for user security and ledger consistency. The blockchain technology generally has key features of decentralization,anonymity and auditability. With these traits, blockchain can greatly controls the cost and improve the efficiency. From then it allows payment to be completed without any intermediary, blockchain can be used in several financial services such as digital assets, remittance and online payment [3], [4]. And also it can be applied into other sectors including smart contracts [5], public services [6], Internet ofThings (IoT) [7], reputation systems [8] and security services [9]. Those fields favor blockchain in several ways. First of all, blockchain is immutable which means we cannot changed. Transaction cannot be tampered once it is combined into the

blockchain. Businesses that needs high reliability can use blockchain to attract customers. On other side, blockchain is distributed and can avoid the single point of failure position. Then for smart contracts, the contract could be formed by miners continuously once the contract has been deployed on the blockchain. Although the blockchain technology has great energy for the development of the future Internet systems, it is facing a number of technical issues. Firstly, scalability is a huge concern. Bit coin block size is adjusted to 1 MB now while a block is mined for each ten minutes. Simutaneously, the Bitcoin network is limited to a rate of 7 transactions per second, which is not capable of handing with high frequency trading. However, huge size blocks means huge storage space and slower propagation in the network. This will result to centralization gradually as less users would like to maintain such a large blockchain. hence the tradeoff between block size and security has been a tough challenge. Secondly, it has been proved that miners could gain heavire revenue than their fair share through selfish mining strategy [10].. In that way, branches could take place frequently, which hinders blockchain development. Hence some solutions need to be put forward to fix this issue. On top of that, it has shown that privacy leakage could also happens in blockchain even users only make transactions with their public key and private key [11]. Furthermore, the present consensus algorithms like *proof of work or proof of stakes* are facing major problems Tschorsch et al. [12] made a technical survey about decentralized digital currencies including Bitcoin. Compared to [12], our paper focuses o blockchain technology instead of digital currencies. Nomura Research Institut made a technical report about blockchain [13]. Contrast to [13], our paper concentrates more on state-of-art blockchain researches with recent advances and future trends.

Section II introduces blockchain architecture.

Section III shows typical consensus algorithms used in blockchain.

Section IV summarizes the technical challenges and the recent advances in this area.

Section V discusses some possible future directions and section VI concludes the paper.

BLOCKCHAIN ARCHITECTURE

Fig. 1: An example of blockchain which consists of a continuous sequence of blocks.

Fig. 2: Block structure

Blockchain is a sequence of blocks, which consists of a complete list of transaction records like conventional public ledger . Figure 1 illustrates an example of a blockchain. With earlier block hash contained in the block header, a block has only one *parent block*. It is worth noting that *uncle block* (children of the block's ancestors) hashes would also be stored in the blockchain . The first block of a blockchainis called *genesis block* which has no parent block. Here We then explain the internals of block chain in detail..

A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes as follows

Block version: it denoted which set of block validation rules to follow.

Merkle tree root hash: the hash numbers of all the transactions in the block.

Timestamp: the present time as seconds in universal time since January 1, 1970.

nBits: target threshold of a valid block hash.

Parent block hash: a 256-bit hash value that points to the earlier block. The block body is comprised of a transaction counter and transactions. large number of transactions that a block can contain depends on the block size and the size of each transaction. Block chain uses an asymmetric cryptography method to validate the authentication of transactions . Digital signature is based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

Digital Signature

Every user will own a pair of private key and public key.The private key that shall be kept in secret is used to sign the transactions.Digital signed transactions are transmitted through out the whole network. The complex digital signature is composed with two phases: *signing phase* and *verification phase*. For example, an user Alice wants to send another user Bob a message. In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. In the verification phase, Bob proves the value effectiveness with Alice's public key. In this way, Bob can easily able to check if the data has been tampered or not. The complex digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA).

Key Characteristics of Blockchain:-

In summary, blockchain has following key characteristics.

Decentralization. In conventional centralized transaction systems, each and every transaction needs to be proved through the central trusted agency (e.g., the central bank), inevitably results to the cost and the efficiency bottleneck sat the central servers. opposite to the centra mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain the data consistency in distributed network.

Persistency. Transactions can be proved fastly and invalid transactions can not be admitted by honest miners. It is impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be identified immediately.

Anonymity. Each user can contact with the blockchain with a specific address, which does

not open up the real identity of the user. Note that block chain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.

Auditability. Bitcoin block chain stores the information about user balances based on the Unspent Transaction Output (UTXO) model : Any transaction has to refer to some previous unspent transactions. Once the present transaction is recorded into the blockchain, the state of those referred as unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.

TABLE I: Comparisons among *public blockchain, consortium blockchain* and *private blockchain*

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

CHALLENGES & RECENT ADVANCES

Despite the great potential of blockchain, it faces several challenges, which controls the high usage of blockchain. We phase some major challenges and recent advances as follows.

as the number of transactions increasing day by day, the blockchain becomes very bulky. Each node has to be store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Because of the original restriction of block size and the time interval used to produce a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot satisfy the requirement of processing millions of transactions in real-time fashion. And also, the capacity of blocks is very small, many small transactions might be delayed since miners give importance to those transactions with high transaction fee. There are a several efforts proposed to address the scalability issue of blockchain, which could be divided into two types:

Storage optimization of blockchain. Since it is complex for node to operate full copy of ledger, Bruce proposed a novel crypto currency method, in which the old transaction records are deleted (or forgotten) by the network . A database called as account tree is used to control the balance of all non-empty addresses. Besides lightweight client could also help to fix this issue. A novel sachem named VerSum was proposed to provide another way allowing lightweight clients to exist. VerSum allows lightweight clients to outsource expensive computations over heavy inputs. It says the computation result is correct through comparing the results from various servers.

Redesigning blockchain. In Bitcoin-NG (Next Generation) was proposed. The main aim of Bitcoin-NG is to decouple conventional block into two parts: key block for leader election and microblock to store transactions. The protocol categorises time into epoches. In each epoch, miners have to produce a key

block. Once the key block is generated, the node becomes the leader who is responsible for producing the micro blocks. Bitcoin-NG also enhanced the heaviest (longest) chain strategy in which micro blocks carry no weight. By his way, blockchain is redesigned and the tradeoff between block size and network security has been addressed.

Privacy Leakage

Blockchain can save a specific amount of privacy through the public key and private key. Users transact with their private key and public key without any real identity exposure .moreover, it has shown in , that blockchain cannot guarantee the *transactional privacy* since the effectiveness of all the transactions and balances for each public key are publicly visible. On the other side, the latest study has shown that a user's Bitcoin transactions can be linked to open user's information. Moreover, Biryukov et al has presented a method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. each client can be individually identified by a set of nodes it connects to. However, this set can be learned and utilized to find the origin of a transaction. several methods have been proposed to develop anonymity of blockchain, which could be hardly divided into two types:

Mixing . In blockchain, user's addresses are pseudonymous. But it is still possible to link addresses to user real identity as many users make transactions with the same address frequently. Mixing service is a kind of service which provides anonymity by transferring funds from several input addresses to several output addresses. For example, the user Alice with address A wants to send some funds to Bob with address B. If Alice directly makes a transaction with input address A and output address B, relationship between Alice and Bob might be opened. So Alice can send funds to a trusted intermediary Carol. Then Carol transfer funds to Bob with several inputs c1,c2, c3, etc., and several output d1, d2, B, d3, etc. Bob's address B is also stored in the output addresses. So it becomes very complex to reveal the relationship between Alice and Bob. Moreover, the intermediary could be dishonest and reveal Alice and Bob's private information on purpose. It is also possible that Carol transfers Alice's funds to her own address apart from Bob's address. Mixcoin provides a easy approach to avoid dishonest behaviors. The intermediary encrypts users' needs including funds amount and transfer date with its private key. Then if the intermediary did not transfer the money, anybody could easily verify that the intermediary cheated. However, theft is identified but still not prevented.

Anonymous. In Zerocoin , zero-knowledge proof is used. Miners don't have to validate a transaction with digital signature but to validate coins belong to a list of valid coins. Payment's origin are unlinked from transactions to avoid transaction graph analyses. But it still reveals payments' destination and amounts. Zerocash was proposed to specify about this problem. In Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) is invested. Selfish Mining Blockchain is vulnerable to attacks of colluding selfish miners. In particular, Eyal and Sirer showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners put their mined blocks without broadcasting and the private branch would be opened to the public only if some needs are satisfied. As the private branch is longer than the present public chain, it would be admitted by all miners. Before the private block chain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without the help of competitors. hence selfish miners leads to get more revenue. Depends up on selfish mining, several

other attacks have been proposed to show that blockchain is not so safe. In stubborn mining , miners could amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blocks even though if the private chain is left aside. though in some cases, it can result in 13% gains in comparison with a non-trail-stubborn counterpart.it shows that there are selfish mining strategies that earn more money and are gaining profits for the smaller miners when compared to that of simple selfish mining. But the profits are relatively small. moreover, it shows that attackers with less than 25% of the computational sources can still gain from selfish mining. To help fix the selfish mining problem, Heilman presented an novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners may select more fresh blocks. However,is dangerous to forgeable timestamps. ZeroBlock builds on the simple scheme: Each block must be produced and accepted by the network within a specific time interval. Within ZeroBlock, selfish miners are cannot achieve more than its expected.

POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academia. Here wediscuss possible future directions with respect to four areas: blockchain testing, stop the tendency to centralization, big data analytics and blockchain application.

Blockchain testing:-

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in up to now. moreover, the developers might manipulate their blockchain performance to attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their needs. So blockchain testing technique needs to be in place to test different blockchains.

Blockchain testing categorised into two phases:*standardization phase* and *testing phase*. In standardization phase, all methods have to be made and agreed. When a blockchain is came into existence it could be tested with the agreed method to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing has to be performed with different method. For example, an user who is in charge of online retail business cares about the throughput of the blockchain, hence the examination has to test the average time from a user send a transaction to the Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in up to now. moreover, some developers might falsify their blockchain performance to attract investors driven by the heavy profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains.Up to now, the top 5 mining pools combiney owns larger than 51% of the total hash power in the Bitcoin network . Instead of that, selfish mining strategy [10] has shown that pools with over 25% of total computing power could get more revenue than fair share. As the blockchain is not intended to provide service to few organizations, some techniques should be proposed to solve this issue.

.

Big data analytics

Blockchain could be well combined with big data. In this we hardly divided the combination into two types: *data management* and *data analytics*. As for the data management, blockchain could be used to store important data as it is distributed and protected. Blockchain could also ensure the data is original. For example, if blockchain is used to store patients health information, the information could not be manipulated and it is complex to stole those private information. When it comes for data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns might be extracted. Users can anayze their potential partners' trading behaviours with the analysis.

Blockchain application

At present most blockchains are used in the financial domain , more and more applications for different fields are appearing. paast industries could take blockchain into consideration and apply blockchain into their sectors to improve their applications. We take an example like user reputations could be stored on blockchain. At the same time, the upcoming industry could make use of blockchain to improve performance. For example, Arcade City [51], a ridesharing startup offers an open marketplace where riders can connect directly with drivers by leveraging blockchain technology. smart contract is a calculated transaction protocol which implements in terms of a contract [54]. It has been proposed for long time and now this concept can be evaluated with blockchain.

BLOCKCHAIN CONCLUSION

Blockchain has shown its energy for transforming traditional industry with its key features: decentralization, persistency and auditability. In this paper, we show a overview on blockchain. We first give an overview of blockchain technologies with blockchain architecture and key features of block chain. then we discuss the typical consensus algorithms used in block chain. We investigated and compared with these protocols in different ways. Moreover, we listed some challenges and problems that would hinder blockchain development and summarized some existing methods for solving these issues. Some possible future directions are also proposed. Nowadays block chain based applications are springing up and we plan to conduct in-depth investigations on block chain-based applications in the future.

LITERATURE SURVEY

Efficient and secure attribute-based signature for monotone predicates[24]

Author:- Ke Gu· Weijia Jia:-

In this paper, we present a framework for ABS and show the security model for ABS. under our framework, we present an attribute-based signature scheme for monotone predicates in the standard model, where we choose the Waters' signature scheme as the prototype of our attribute based signature scheme. When Compared with the Maji's scheme in the generic group model, the proposed method is constructed in the standard model. ABS can hide any discovering information and make fine-grained control on signature. At present several attribute-based signature schemes have been proposed, but most of them are not very efficient. here the overall accuracy is 75% efficient.

Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model[20]

Author:- Tatsuaki Okamoto and Katsuyuki Takashima:-

The admissible predicates of the proposed ABS scheme are more general than those of the existing ABS schemes, i.e., the proposed ABS scheme is the first to support general non- monotone predicates, which can be expressed using NOT gates as well as AND, OR, and Threshold gates, while the existing ABS schemes only support monotone predicates. The proposed ABS scheme is comparably as efficient as (several times worse than) one of the most efficient ABS schemes, which is proven to be secure in the generic group model. It cannot Provide complete security to the system in standard assumptions. here the accuracy is 84%.

Medical JPEG image steganography based on preserving inter-block dependencies[13]

Author:- Xin Liaoa , Jiaojiao Yina , Sujing Guoa , Xiong Li:-

Here we propose a new medical JPEG image steganographic method based up on the dependencies of inter-block coefficients. The technique is to save the differences among the DCT coefficients at the equal position in adjacent DCT blocks as much as possible. The cost values are allocated dynamically according to the changes of inter-block neighbors in the embedding process. Experimental results show that the proposed scheme can cluster the inter- block embedding changes and perform better than the state-of-the-art steganographic method. In this paper, the privacy protection of medical JEPG images has become an important problem. Steganography is a useful tool to conceal patients datain the medical images. Here overall homogeneous accuracy is 85%.

Public standards and patients' control: how to keep electronic medical records accessible but private.[2]

Author:- Kenneth D Mandl.et.al

In this article they proposed two doctrines-Public standards and Patient control and six desirable characteristics- Comprehensiveness, Accessibility, Interoperability, Accountability, Flexibility, to guide the development of online medical record systems. They need to develop Acceptable procedures for backing up data, anticipating recovery in case of disasters.

Bitcoin: A Peer-to-Peer Electronic CashSystem[3]

Author:- Satoshi Nakamoto

In this paper, We have proposed a system for electronic transactions without relying on trust. Then we started with the usual framework of coins made from digital signatures, which provides strong control of ownership. This model identifies a solution to prevent double-spending problem. And we have achieved with80% accuracy.

How block chain-time stamped protocols could improve the trustworthiness of medical science[11]

Author:- G. Irving and J. Holden

In this paper, we report a proof-of-concept study using a ‘block chain’ as a low cost, independently verifiable method that could be widely and readily used to audit and confirm the reliability of scientific studies..SHA256 is used to verify the exact wording and existence of a protocol at a given point in time. The outcome of switching, data dredging and selective publication are some of the problems that undermine the integrity of published research. 83.5% accuracy.

Proposed System:

Electronic Health Records (EHRs) provides a comfortable health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers, the preserving patient privacy in an EHRs system on blockchain, multiple authorities are introduced into ABS and put forward7 a MA-ABS scheme, which meets the requirements of the structure of blockchain, as well as guaranteeing the anonymity and immutability of the information immutability of the information. PRF seeds are necessary among several authorities and the patient private keys need to be constructed, N − 1 corrupted authorities cannot succeed in collusion attacks. The comparison method explains the performance and the cost of this protocol improves linearly with the number of authorities and patient attributes as well

CONCLUSION

Blockchain has shown its energy for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a overview on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of block chain. then we discuss the typical consensus algorithms used in block chain. We investigated and compared these protocols in different aspects. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing methods for solving these problems. Some possible future directions are also proposed. Nowadays block chain based applications are springing up and we plan to conduct in-depth investigations on block chain-based applications in the future.The protection of the protocol is proven under the CBDH assumption in terms of unforgeability and perfect privacy. The comparison analysis explains the performance and the cost of this protocol increases linearly with the number of authorities and patient attributes as well. A non-monotone predicate could be used in many distributed system applications, which highights the representation of the predicate, which supports the general non-monotone predicates in blockchain technology is the direction of future work.

REFERENCES

[1] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). Who Owns Medical Records: 50 State Comparison. [Online]. Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medicalrecords-50-state-comparison

[2] K.D.Mandl,P.Szolovits,andI.S.Kohane,‘‘Publicstandardsandpatients’ control: How to keep electronic medical records accessible but private,’’ BMJ, vol. 322, no. 7281, pp. 283–287, Feb. 2001.

[3] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] World Economic Forum. (Sep. 9, 2015). Deep Shift: Technology Tipping Points and Societal Impact. [Online]. Available: http://www3.weforum.

org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[5] (Dec. 12, 2016). Healthcare Rallies for Blockchains: Keeping Patients at the Center. [Online]. Available: http://www.ibm.biz/blockchainhealth

[6] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015, pp. 53–68.

[7] G.Prisco.(Apr.26,2016).TheBlockchainforHealthcare:GemLaunches Gem Health Network With Philips Blockchain Lab. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gemlaunches-gem-health-network-with-philips-blockchain-lab-1461674938

[8] U.S. White House. 104th Congress. (Aug. 21, 1996). Public Health Insurance Portability and Accountability Act. [Online]. Available: https://en. wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_ Act

[9] P. Taylor. (Apr. 27, 2016). Applying Blockchain Technology to Medicine Traceability. [Online]. Available: https://www.securingindustry. com/pharmaceuticals/applying-blockchain-technology-to-medicinetraceability/s40/a2766/#.V5mxL_mLTIV

[10] P. B. Nichol. (Mar. 17, 2016). Blockchain Applications for Healthcare: Blockchain Opportunities are Changing Healthcare Globally-Innovative Leaders See the Change. [Online]. Available: http://www.cio.com/article/3042603/innovation/blockchain-applicationsfor-healthcare.html

[11] G. Irving and J. Holden, ''How blockchain-timestamped protocols could improve the trustworthiness of medical science,'' F1000Research, vol. 5, p. 222, May 2016.

[12] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, ''Searchain: Blockchainbased private keyword search in decentralized storage,'' Future Generat. Comput. Syst., 2017, doi: 10.1016/j.future.2017.08.036.

[13] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, ''Medical JPEG image steganography based on preserving inter-block dependencies,'' Comput. Electr. Eng., 2017, doi: 10.1016/j.compeleceng.2017.08.020.

[14] H. K. Maji, M. Prabhakaran, and M. Rosulek, ''Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,'' in Proc. IACR Cryptol. ePrint Arch., Apr. 2008, pp. 1–23. [Online]. Available: https://eprint.iacr.org/2008/328.pdf

[15] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Proc. EUROCRYPT, Aarhus, Denmark, 2005, pp. 457–473.

[16] D. Khader, ''Attribute based group signature with revocation,'' in Proc. IACR Cryptol. ePrint Arch., Jun. 2007, pp. 1–19. [Online]. Available: https://eprint.iacr.org/2007/241.pdf

[17] H. K. Maji, M. Prabhakaran, and M. Rosulek, ''Attribute-based signatures,'' in Proc. CT-RSA, San Francisco, CA, USA, 2011, pp. 376–392.

[18] J.Li,M.H.Au,W.Susilo,D.Xie,andK.Ren,''Attribute-basedsignature and its applications,'' in Proc. ASIACCS, Beijing, China, 2010, pp. 60–69.

[19] J. Herranz, F. Laguillaumie, B. Libert, and C. Ràfols, ‘‘Short attribute-based signatures for threshold predicates,’’ in Proc. CT-RSA, San Francisco, CA, USA, 2012, pp. 51–67.

[20] T. Okamoto and K. Takashima, ‘‘Efficient attribute-based signatures for non-monotonepredicatesinthestandardmodel,’’inProc.PKC,Taormina, Italy, 2011, pp. 35–52.

[21] C. Chen et al., ‘‘Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures,’’ in Proc. CT-RSA, San Francisco, CA, USA, 2013, pp. 50–67. [22] Y. S. Rao and R. Dutta, ‘‘Efficient attribute-based signature and signcryptionrealizingexpressiveaccessstructures,’’Int.J.Inf.Secur.,vol.15,no.1, pp. 81–109, Feb. 2016.

[23] Y. Sakai, N. Attrapadung, and G. Hanaoka, ‘‘Attribute-based signatures for circuits from bilinear map,’’ in Proc. PKC, Taipei, Taiwan, 2016, pp. 283–300.

[24] K.Gu,W.Jia,G.Wang,andS.Wen,‘‘Efficientandsecureattribute-based signature for monotone predicates,’’ Acta Inf., vol. 54, no. 5, pp. 521–541, Aug. 2017.

[25] J. Liu et al., ‘‘Protecting mobile health records in cloud computing: A secure, efficient, and anonymous design,’’ ACM Trans. Embed. Comput. Syst., vol. 16, no. 2, Apr. 2017, Art. no. 57.

[26] H. Cui, G. Wang, R. H. Deng, and B. Qin, ‘‘Escrow free attribute-based signature with self-revealability,’’ Inf. Sci., vols. 367–368, pp. 660–672, Nov. 2016.

[27] D. Cao, B. Zhao, X. Wang, J. Su, and G. Ji, ‘‘Multi-authority attributebased signature,’’ in Proc. 3rd IEEE INCoS, Fukuoka, Japan, Nov. 2011, pp. 668–672.

[28] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, ‘‘RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cry ptocurrency monero,’’ in Proc. ESORICS, Oslo, Norway, 2017, pp. 456–474