CAAI Transactions on Intelligence Technology

Special Issue: Internet of Things and Intelligent Devices and Services

Efficient key management scheme for health blockchain

ISSN 2468-2322
Received on 8th December 2017
Revised on 12th January 2018
Accepted on 17th January 2018
doi: 10.1049/trit.2018.0014
www.ietdl.org

Huawei Zhao ✉, *Peidong Bai*, *Yun Peng*, *Ruzhi Xu*

College of Finance, Qilu University of Technology (Shandong Academy of Sciences), 58th Sangyuan Lu Road, Jinan, People's Republic of China
✉ *E-mail: zhuav@163.com*

Abstract: Healthcare is a big application scenario of blockchain, and blockchains used in healthcare are called health blockchain. In general, blockchain blocks are open and the transactions in them are public. If some privacy data are involved in these transactions, they will be leaked. Owing to healthcare system involving a great deal of privacy data, certain security mechanisms must be built to protect these privacy data in health blockchain. Furthermore, because the core of security mechanisms is the key management schemes, the appropriate key management schemes should be designed before blockchains can be used in healthcare system. Here, according to the features of health blockchain, the authors use a body sensor network to design a lightweight backup and efficient recovery scheme for keys of health blockchain. The authors' analyses show that the scheme has high security and performance, and it can be used to protect privacy messages on health blockchain effectively and to promote the application of health blockchain.

1 Introduction

Blockchain was first introduced in bitcoin and is the supporting technology of bitcoin [1]. It uses technologies such as consensus mechanism [2], digital signature, and hash chains to record bitcoins' transactions by building a distributed, shared database in a decentralised manner. These technologies provide security services such as non-repudiation, integrity, distributed storage, time-based traceability for transaction contents, which form a robustness system and make bitcoins circulate cross the Internet freely to realise the value migration in untrusted networks. Later, people gradually realise that blockchain can be used in various fields such as healthcare, fintech, computational law, audit, notarisation, and so on by designing various smart contracts based on blockchain. The use of blockchain can greatly improve the efficiency and the security of transactions' processing, and reduce the cost [3–5]. At present, it is widely believed that consensus in untrusted networks, robustness, and value migration in a decentralisation manner are the main features of blockchain. Based on these features, we can predict that blockchain will update the current information-Internet to value-Internet in the future, and thus dramatically change the mode of our society and our life. Fig. 1 shows the architecture of blockchain.

However, as a developing technology, blockchain still is facing some problems. For example, how to improve the speed of transaction recording? How to improve the efficiency of consensus? How to protect privacy data on blockchains? All of these problems have effects on the popularisation and application of blockchain. Among these problems, the third one is the most highlighted one, as many applications of blockchain concern about privacy data and people are becoming more and more concerned about privacy issues.

The core of the third problem is how to build a feasible key management scheme for blockchain. Blocks on blockchain are public and shared by all participants. When these blocks are involved with privacy data, it is necessary to encrypt these data to protect privacy information. However, the key management scheme related to the privacy protection is hard to design. One key for all blocks is unfeasible, the encrypted blocks will be vulnerable under the statistical attack. Yet, one key for one block is unfeasible, as it will require a high cost for storing and recovering a tremendous number of historical keys. At the same time, designing key management scheme for blockchain has to consider the application scenarios, for different scenarios have different features and it is hard to design a generic key management scheme for all scenarios.

At present, it is a consensus that blockchain has great potential application values in the field of healthcare. However, because blocks on health blockchain are involved in a great number of private health data, it is necessary to solve the problem of privacy protection before the popularisation of health blockchain.

With the development of electronic techniques, body sensor networks (BSNs) emerge to survey the health of the human. Biosensor nodes in BSNs can be deployed on/into the human body to collect physiological signals and send these signals to a remote hospital for further processing. To protect physiological signals from the human body, many researches have been done in designing the key management for BSNs. In the paper, we merge BSNs and health blockchain together, and make use of the idea of designing the key management scheme for BSNs to design a lightweight backup and efficient recovery scheme for keys of health blockchain.

The rest of the paper is organised as follows. Section 2 presents the existing research results related to key management schemes for blockchains. Section 3 proposes a lightweight backup and efficient recovery scheme for keys of health blockchain. The performance and security analyses are given in Section 4. In Section 5, conclusions are drawn.

2 Related work

As a supporting technology for bitcoin, the blockchain is known by the public with the popularisation of bitcoin. Later, people find that the blockchain has broad application space in the field of healthcare, fintech, law, energy, and so on by designing various smart contracts. As most application scenarios involve the storage of privacy data, before applying blockchain on these fields, the blockchain must solve the problem of privacy protection.

To address the problem, research in [6] proposes a scheme using blockchain to protect personal data, and the scheme ensures users own and control their data. However, the scheme focuses on the

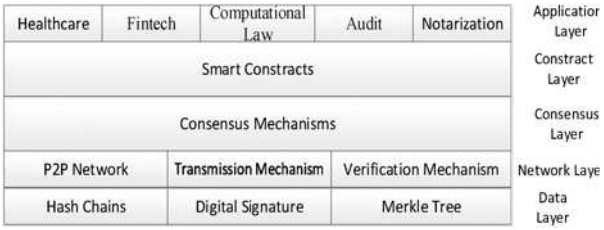

Fig. 1 *Architecture of blockchain*

construction of blockchain and how to authenticate the access to blockchain, but does not give a concrete solution to design the related key management scheme. A study in [7] proposes a method that uses bitcoins and the blockchain to solve subjective trust and quantification of trust in pretty good privacy (PGP) mechanism, and gives a solution to store and use the PGP certificates. However, the research does not concern the key management related to blockchain encryption. A study in [8] proposes a method using blockchain to authenticate the decentralised sensor data. The scheme makes use of timestamp, hash function, and the mechanism of work proof to check the validity of sensor data, and does not consider the confidentiality of sensor data, so the scheme does not concern the research of key management. Wang *et al*. [9] propose a data security sharing network architecture based on block chain to support exchange information for internal and intel-enterprise. However, the work also ignores the confidentiality of data and does not concern the key management on blockchain. Zhu *et al*. [10] point out using asymmetric encryption and multi-blind signature to realise privacy protection, while the two technologies are not available to protect a great deal of data because of their low efficiency.

It can be seen that at present, the blockchain is a developing technology, and the security research on it is only in an initial stage with few work being done on this field.

3 Lightweight backup and efficient recovery scheme for keys of the health blockchain

3.1 Application scenario of health blockchain

In this section, we first present the general application scenario of health blockchain.

Recently, the emergence of BSNs greatly promotes the development of smart healthcare industry. A BSN is composed of tens of biosensor nodes that are deployed on or into the human body [11]. These nodes are equipped with various biosensors that can collect the physiological signals such as blood pressure (systolic and diastolic), electrocardiogram, blood oxygen level (SpO2), photoplethysmogram (PPG) signals, and so on. In addition, they also are equipped with wireless network chips, and these chips not only help biosensor nodes form a BSN, but also help these nodes sending collected physiological signals to a special relay node (generally called PDA) that takes charge of merging and forwarding signals to a remote medical centre such as a hospital [12]. Thus, with the help of BSNs, a person can easily build his/her health file and a hospital can easily acquire the comprehensive health condition of a patient before treatment. It can be seen that BSNs can significantly improve the current medical environment and open the door for the smart healthcare time.

In the traditional application scenario of BSNs, a user's physiological signals generally only are sent to one target hospital. The hospital stores these data, and when the user needs to use these data for health purpose, or the doctor related to the user needs to use these data for medical purpose, the hospital will draw and analyse these data, and send the analysis results to the user or the doctor. However, the scenario has some problems: (i) monopoly problem: concentrating users' physiological signals in one target hospital will cause the monopoly of medical data. When the user goes to other hospitals for treatment, the hospital storing the user's physiological data generally is reluctant to share these data to other hospitals for the sake of interests. (ii) Vulnerability problem: storing physiological data in one hospital has vulnerability, and an accident will cause the loss of a user's physiological data. (iii) Privacy problem: the target hospital may deliver users' physiological data to insurance companies, medical companies, and so on for commercial purposes without user knowledge, which will violate users' privacy. (iv) Integrity problem: when a medical dispute occurs, a hospital may tamper with the medical data stored in the storage device owned by itself, so that the hospital will be in a favourable position in the dispute.

When we use blockchain in the healthcare system, and merge blockchain and BSNs together, the above problems will be solved thoroughly. Fig. 2 shows a smart healthcare system with blockchains and a BSN.

In Fig. 2, a smart healthcare system consists of a BSN and two health blockchains, *A*-chain and *B*-chain. The BSN is deployed on a user's body and is composed of a few wearable nodes. One of them is the gateway device and some are implanted nodes. Wearable nodes and implanted nodes are used to measure the user's various physiological signals and send these signals to the gateway node. The gateway device takes charge of converging these physiological signals and broadcast the related physiological data to some target hospitals. These target hospitals form a healthcare alliance and each of them provides a blockchain node (a computer server). All blockchain nodes make uses of consensus mechanism, digital signature, and hash chain technology to maintain the two health blockchains. When these blockchain nodes receive a broadcast physiological message from the gateway device, they use consensus mechanism to check its validity. Also, once the message is checked valid, blockchain nodes will put it on the *A*-chain by signing it. Otherwise, if the message is checked invalid or some nodes vote against the message, blockchain nodes will reject the message according to their consensus mechanism, and put the messages and the cause on the *B*-chain.

In the scenario, each blockchain node stores a duplicate of each blockchain. When the user goes to any hospital in the health alliance, the visited hospital can draw the user's physiological data

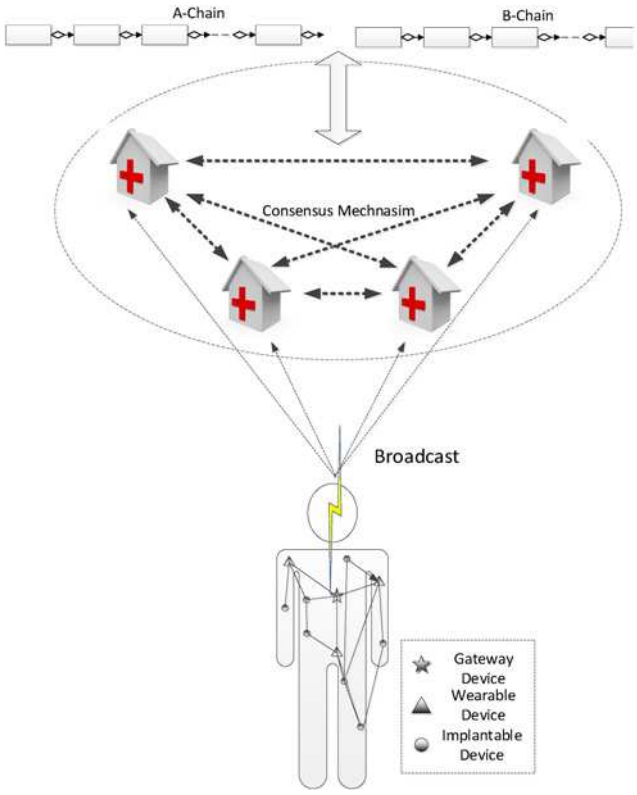

Fig. 2 *Smart healthcare system with blockchain and a BSN*

from A-chain on its blockchain node. It solves the monopoly problem of users' physiological data. In addition, it solves the vulnerability and integrity problems of physiological data storage by multi-nodes' backup and nodes signatures.

To solve the problem of privacy, we adopt the idea of key management for BSNs to improve the broadcast process in the smart healthcare system as follows: before a biosensor node sends the target physiological signals to the gateway device, the node first produces a key using other physiological signals it measures, and uses the key to encrypt the target signals. Next, the node sends the encrypted signals to the health blockchain with the help of the gateway device. As the blockchain nodes and the corresponding hospitals do not know the encrypting key, they cannot leak users' private physiological data to other organisations. When a user wants to recover his/her physiological data from the health blockchain, the user can ask his/her biosensor node to recover the encrypting key and then use the key to restore his/her physiological data.

It could be seen that in the scheme, the health blockchain only stores the cipher text of physiological data and the power of decrypting these data is controlled by the user. In other words, the user controls who can access his/her physiological data. It will solve the privacy problem.

In the realisation, we use fuzzy vault technology to carry out the generation, backup, and recovery of keys of health blockchain. Also, to explain the scheme clearly, we first give the detail of fuzzy vault in Section 3.2.

3.2 Fuzzy vault

Fuzzy vault is a cryptographic primitive, and it can use a set A to build a structure denoted by vault to hide a secret S. S could be unhidden if another set B is similar enough to the set A. Based on fuzzy vault, research in [13] proposed a key management scheme called Photoplethysmogram based key agreement (PKA) that uses PPG signals to negotiate a common key between two biosensor nodes. The scheme including five steps:

(i) Production of PPG vector. Under a loose synchronisation mechanism, biosensor nodes A and B on the same human body collect PPG signals, and then both of them use fast Fourier transform (FFT) to encode these signals into vectors:

$$\boldsymbol{F}_s = \langle f_s^1, f_s^2, \ldots, f_s^a \rangle \text{ and } \boldsymbol{F}_r = \langle f_r^1, f_r^2, \ldots, f_r^a \rangle.$$

(ii) Creating polynomial. Biosensor node A creates a polynomial $p(x)$ with a public order a. Also, the coefficients are produced from a random number and are used to be encoded into a common key. For instance, if the coefficients are e_a, e_{a-1},…, e_1, e_0, the common key will be $K = e_a \| e_{a-1} \|, \ldots, \| e_1 \| e_0$.

(iii) Vault production. A first computes a set $D = \{f_s^i, p(f_s^i)\}$, $1 \le i \le a$, and then uses random numbers to build a chaff points set $C = \{c_i, d_i\}$, $1 \le i \le W$, where W is a pre-defined value; c_i and d_i are random, $d_i \neq p(c_i)$. Next, A mixes the values in D and C to produce a vault $R = D \cup C$.

(iv) Vault transmission. A sends $R \| T(K, R)$ to B, where $T()$ is a keyed MAC function to protect the integrity of R.

(v) Opening vault. When B receives the vault R, it draws a points set U from R, where the x ordinates of points in U are elements in Fr. Next, B tries to reproduce the polynomial p based on points in U by Lagrangian Interpolation. If B could produce a polynomial p', it will use the coefficients of p' to produce a key K' as mentioned in the first step. Finally, B use K' to check validity of the MAC $T(K, R)$ it receives. If the MAC is valid, it means that A and B share the common key K successfully, otherwise A and B will restart the key negotiation process.

A later study [14] found that PKA left some practical problems unsolved. For instance: (i) PKA requires that biosensor nodes A and B share at least $v+1$ feature points to reproduce a vth-order polynomial, but it is not a goal easy to reach. (ii) Some important parameters are inversely correlated. Namely, when the length of the common key is determined, the order v of the produced polynomial $p(x)$ and the average length of each coefficient of the polynomial e are inverse correlated. While from the perspective of security, both v and e are all required to be large enough to resist brute-forcing attack.

To solve these problems, a study in [14] proposed an improved scheme for PKA: when biosensor nodes A and B need to negotiate a common key, A first generates a key material and encodes it into RS (Reed–Solomon) codewords using RS code. Also, then these codewords are encoded as the coefficients of the chosen polynomial $p(x)$ with the order v. Next, A collects physiological signals and uses FFT to encode these signals into a feature vector. Finally, A inputs the feature vector into the polynomial $p(x)$, and uses the produced points on $p(x)$ and a chaff points set to build a vault. To B, when it receives a vault from A, it uses a reconstruction method called lower-order twice reconstruction (LOTR) to reproduce $p(x)$. In other words, in the beginning, B maybe cannot find enough matched physiological signals with A to construct a v-order polynomial. In this condition, B can use a small number of matched physiological signals to build a lower-order polynomial. Next, B estimates the left points in $p(x)$ according to the lower-order polynomial. Finally, B recovers $p(x)$ using the matched points and the estimated points. After LOTR process, if B obtains the coefficients of $p(x)$, it can calculate the key material using RS code.

In the improved scheme, A and B do not need as many matched points as the research [13] to reconstruct $p(x)$, which solves the first problem of PKA scheme. Besides, because RS code is used in q-ary field, when we use RS code as the coefficients of $p(x)$, the bit length of each coefficient of $p(x)$ is a fixed length q, which breaks the inverse correlation between the length of coefficient and the order of $p(x)$, and solves the second problem to some extent.

Since the improved PKA scheme is superior to the original one in terms of security, in Section 3.3, we use the improved PKA scheme to design the keys' generation, backup, and recovery scheme for health blockchain.

3.3 Keys' generation and lightweight backup scheme for health blockchain

In the scheme, key generation process is designed as follows:

(i) In the initialisation period of a BSN, some biosensor nodes measuring PPG signals are appointed to generate encrypting keys for health blockchain. Here, we suppose that biosensor node A works as the role.

(ii) When the gateway device needs to encrypt a physiological data, it asks A to produce a key for health blockchain. Once A receives the order from the gateway device, it first generates a pre-key $K = k_a \| k_{a-1} \|, \ldots, \| k_1 \| k_0$, and then uses RS code to encode k_i $(0 \le i \le a)$ into codewords e_i with the length of q. Finally, A uses e_i as coefficients to construct a polynomial $p(x)$ with the order a.

(iii) A communicates with adjacent biosensor nodes measuring PPG signals to find a group of the same PPG signals to get a stable signals set. Also, then A encodes these signals into a vector $\boldsymbol{F}_s$ using FFT. Next, A puts $\boldsymbol{F}_s$ into $p(x)$ to calculate some points on $p(x)$. These points form a set D, and in order to protect D, A generates a chaos set C, and then mixes D and C to form the set $R = D \cup C$ as the vault.

(iv) A chooses a pseudo-random function $F(\cdot)$ and calculates $K^* = F(k^*, K)$ as the encrypting key for the health blockchain. Here, k^* is the pre-distributed key in all of biosensor nodes. At the same time, A generates a random number r, and uses r and k^* to hide the vault R: $M = E(r \oplus k^*, R)$, where $E()$ is a symmetric encryption algorithm, $\oplus$ the XOR operation.

(v) A sends $K^* \| M \| r \| H(K^*) \| \mathrm{ID}_A$ to the gateway device G in a secure manner using the security association between A and G. Here, $H()$ is a hash function, symbol '$\|$' denotes concatenation operation; ID_A is the identity of A.

(vi) G uses K^* to encrypt the physiological data Mp, and broadcasts the encrypted Mp and $M \| r \| H(K^*) \| \mathrm{ID}_A // B_A$among blockchain nodes

CAAI Trans. Intell. Technol., 2018, Vol. 3, Iss. 2, pp. 114–118

Fig. 3 *Encrypted block on the health blockchain*

to let them put these messages on the health blockchain. Here B_A denotes the index of the block and includes the information such as which biosensor node generating K^*, the time of generating the block, what kind of physiological data being in the block, and so on. Finally, for the sake of security, G will delete K^*.

In addition, there should be authentication mechanisms among biosensor nodes, gateway devices, and blockchain nodes to realise entities authentication and message authentication in steps v and vi. Similar researches were proposed in [15–17], while authentication mechanisms in them are not available to the scenario in the paper. So, in subpart E, we give our design.

Fig. 3 shows the encrypted block on the health blockchain.

3.4 Efficient recovering keys of health blockchain

When the user needs to decrypt his/her physiological data and authorises a target hospital or a target doctor to use them for treatment, he/she can execute the following process.

(i) The user uses his/her gateway to point out which encrypted block on the health blockchain will be decrypted. Also, then G searches the corresponding encrypted block on the health blockchain by the index B_A. When it finds the block, it will send the related $M||r||H(K^*)$ to the biosensor node A.

(ii) Once A receives $M||r||H(K^*)$, it uses r and pre-distributed k_0 to decrypt M to get the set R. Also then, A communicates with the adjacent biosensor nodes measuring PPG signals to obtain a stable set of PPG signals. Next, A uses FFT to encode the set of PPG signals into the vector $\boldsymbol{F}_r$ and then draws the points set U from R, where the x ordinates of points in U are the elements in $\boldsymbol{F}_r$.

(iii) If the set U has enough points, node A can directly use Lagrange's interpolation to build a polynomial with the order a. While in most cases, due to physiological noises, the elements in U are not enough to build a polynomial with the order a, and in this condition, A can adopt the LOTR method, that is to say, A first constructs a lower-order polynomial pl(x), and next, A estimates the left points in $p(x)$ according to the polynomial pl(x). Finally, A recovers $p(x)$ using the matched points and the estimated points.

(iv) To verify the validity of the recovered polynomial, A first decodes its coefficients by RS code and uses the decoded results to form a key $K^{*\prime}$. Also then, A checks whether $H(K^{*\prime}) = H(K^*)$. If they are the same value, it means that $p(x)$ is recovered successfully, and otherwise A repeats the recovery process.

After A recovers the key K^*, it sends K^* to G by the security association between A and G. Also then, G will decrypt the physiological data by K^*, and authorise other entities visiting them by other security mechanisms. Finally, G deletes K^* for the sake of security.

3.5 Authentication mechanisms

In the scenario, blockchain nodes cannot identify the authenticity of physiological data delivered by gateway devices. If these data come from illegal gateway devices or illegal biosensor nodes, it will disturb the normal operation of the whole system. Based on the consideration, the whole system requires gateway devices authenticating biosensor nodes, and blockchain nodes authenticating gateway devices. According to the requirement, we propose the following authentication mechanisms.

We implant the authentication mechanism in steps v and vi of subpart C if node A is an adversary and operates as the description in steps i–iv. It will exposure its identity under the authentication mechanism in step v, which means it consumes its energy unnecessarily in steps i–iv.

In step v, the gateway device G needs to ensure the received messages coming from a legal biosensor node. Thus, biosensor node A will change the messages in step v into the following form:

$$M_A = E(r \oplus k^*, K^*)||M||r||H(K^*)||\mathrm{ID}_A$$

After G decrypts K^* using the pre-distributed key $k^*$and r, and verifies K^* using $H(K^*)$, it can ensure that M_A comes from a legal biosensor node because only legal biosensor nodes have the pre-distributed key k^*.

In step vi, G should use digital signature algorithm to sign messages using its private key before broadcasting these messages. Thus, blockchain nodes will know which gateway device broadcasts. Suppose, Mp denotes the physiological signals and $\mathrm{Mg} = M||r||H(K^*)||\mathrm{ID}_A//B_A$, and then the broadcasted messages have the following form:

$$E(K^*, \mathrm{Mp})||\mathrm{Mg}||\mathrm{Sig}(\mathrm{Kpg}, H(E(K^*, \mathrm{Mp})||\mathrm{Mg}))$$

Here, Sig(.) denotes the signature algorithm and Kpg the private key of gateway device.

After each blockchain node receives the message, it can verify the message by using the public key of G. According to the consensus mechanism, if blockchain nodes believe G is a legal device and the signature is valid, they will put $E(K^*,\mathrm{Mp})||\mathrm{Mg}$ on the A-chain.

If G is illegal device or the message's signature send by G is invalid, blockchain nodes will put $\mathrm{Sig}(\mathrm{Kpg},H(E(K^*,\mathrm{Mp})||\mathrm{Mg}))||\mathrm{Mw}||\mathrm{MSig}(\mathrm{Sig}(\mathrm{Kpg},H(E(K^*,\mathrm{Mp})||\mathrm{Mg}))||\mathrm{Mw})$ on the B-chain to record the accident. Here, Msig(.) denotes a broadcasting multi-digital signature scheme executed by blockchain nodes [18]; Mw records the broadcasting time of physiological messages and the reason of rejection. For the sake of saving storage, B-chain need not to store $(E(K^*,\mathrm{Mp})||\mathrm{Mg})$. When G asks question about the rejection, it can inquire B-chain by clues: $\mathrm{Sig}(\mathrm{Kpg},H(E(K^*,\mathrm{Mp})||\mathrm{Mg}))$ and the messages' broadcasting time.

The reason that biosensor nodes do not use digital signature mechanism is that signature algorithm is a high-energy operation, and energy in biosensor nodes is little.

4 Security and performance analysis

4.1 Authentication mechanisms

In the smart healthcare system, K^* and the private physiological data are the objects being protected and they also are the objects the adversary wants to attack. In the following, we analyse the security of the healthcare system by attack method of the adversary.

Generally, the adversary has two possible attack ways to obtain K^* and the private physiological data. One is attacking the health blockchain, and the other is attacking the BSN.

4.1.1 Attacking the health blockchain: If the adversary wants to launch an attack to a special physiological data or an encrypting key from the health blockchain, he will first draw the encrypted block according to ID_A and B_A from the health blockchain.

However as shown in Fig. 3, the only information about K^* the adversary can get from the encrypted block is H (K^*). Owing to the one-way feature of hash function, the adversary cannot recover K^* from H (K^*).

Maybe the adversary wants to get some information about K^* from M. However, M is an encrypted result of a symmetric encryption algorithm, and when we use AES or 3DES as the algorithm instance, the adversary hardly has chance to decrypt M. Though the adversary is fortunate enough to get the vault R from M by some method, he still does not know which true points take part in the generation of K^*, for R is a mixed set of true points set D and a chaos set C.

As the private physiological data are protected by K^*, in the condition that the adversary does not K^*, he cannot obtain the private physiological data yet.

4.1.2 Attacking the BSN: Since K^* is produced by the BSN, the other way that the adversary can obtain K^* or the private physiological data is attacking the BSN.

However, the biosensor nodes in BSN are deployed on or into the human body and under the surveillance of the user all the time, the adversary has little chance to touch these biosensor nodes and draw physiological signals from them.

In the worst case, maybe a user's BSN has more wearable biosensor nodes that can measure PPG signals, and the adversary can touch some of these nodes in some condition. In this case, we can increase the order of the polynomial used to produce the pre-key. Since we use the improved PKA scheme to produce pre-key, when we increase the order, the length of the polynomial's coefficients will not be reduced, which will increase the security of the smart healthcare system.

4.2 Performance mechanisms

The main advantage of the proposed scheme is the storage of keys. In general methods, in order to resist the statistical attack, the health blockchain has to change the encryption keys frequently, and it will cause the generation of a great amount of historic keys. These historic keys must be well stored and indexed; thus, when a user wants to decrypt a block, the healthcare system could find the corresponding keys quickly. In the case, the storage cost will be great.

In our scheme, the health blockchain does not need to store an encrypting key but a clue to a key. The recovery of the key is executed by the BSN. It will greatly reduce the storage cost.

In addition, the clue of encrypting keys is with the encrypted block, so the healthcare system does not need to search the related keys. It will improve the efficiency of decrypting block.

5 Conclusion

The health blockchain is a good solution to address the problem of monopoly of physiological data and improve the robustness of storing these data, and has a broad application prospect in the area of healthcare system. However, before the popularisation of the health blockchain, we must address the problem of protecting private physiological data. The core problem is designing an effective key management scheme.

In the paper, we merge the BSN and the health blockchain, and use the biosensor nodes in the BSN to propose a lightweight backup and efficient recovery scheme for keys of health blockchain. The scheme has the following advantages: (i) biosensor nodes in the BSN are in charge of generation, backup, and recovery of the keys of health blockchain, and it will increase the security of these keys. (ii) In the scheme, each block on the blockchain can be encrypted by a distinguished key with lower storage cost and high performance, and it will greatly improve the security of privacy physiological data on the health blockchain.

6 Acknowledgments

This work was supported in part by following funds: Shandong Provincial Natural Science Foundation (ZR2015FM020, ZR2014FQ007); National Natural Science Foundation (61502258); National Spark Program (2015GA740096).

7 References

[1] 'Bitcoin: a peer-to-peer electronic cash system'. Available at http://www.bitcoin.org, accessed 9 November 2008
[2] Kraff, D.: 'Difficulty control for blockchain-based consensus systems', *Peer Peer Netw. Appl.*, 2016, **9**, (2), pp. 397–413
[3] Fanning, K., Centers, D.P.: 'Blockchain and its coming impact on financial services', *J. Corp. Account. Finance*, 2016, **27**, (5), pp. 53–57
[4] Kishigami, J., Fujimura, S., Watanabe, H., *et al.*: 'The blockchain-based digital content distribution system'. IEEE 5th Int. Conf. Big Data and Cloud Computing, Dalian, China, 2016, pp. 187–190
[5] Fujimura, S., Watanabe, H., Nakadaira, A., *et al.*: 'BRIGHT: a concept for a decentralized rights management system based on blockchain'. 5th IEEE Int. Conf. Consumer Electronics, Berlin, 2016, pp. 345–346
[6] Zyskind, G., Nathan, O., Pentland, A.S.: 'Decentralizing privacy: using blockchain to protect personal data'. IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180–184
[7] 'From pretty good to great: enhancing PGP using bitcoin and the blockchain (LONG)'. Available at http://www.pubzone.org/dblp/journals/corr/WilsonA15, accessed August 2015
[8] Zhao, H., Li, X.F., Zhan, L.K., *et al.*: 'Data integrity protection method for microorganism sampling robots based on blockchain technolgy', *J. Huazhong Univ. Sci. Tech. (Nat. Sci. Ed.)*, 2015, **43**, pp. 216–219
[9] Wang, J., Gao, L., Dong, A., *et al.*: 'Block chain based data security sharing network architecture research', *J. Comput. Res. Dev.*, 2017, **54**, (4), pp. 742–749
[10] Zhu, Y., Gan, G., Deng, D., *et al.*: 'Security architecture and key technologies of blockchain', *J. Inf. Secur. Res.*, 2016, **2**, (12), pp. 1090–1097
[11] Zhao, H.W., Xu, R.Z., Shu, M.L., *et al.*: 'Physiological-signal-based key negotiation protocols for body sensor networks: a survey', *Simul. Modelling Pract. Theory*, 2016, **65**, pp. 32–44
[12] Quwaider, M., Jararweh, Y.: 'Cloudlet-based efficient data collection in wireless body area networks', *Simul. Modelling Pract. Theory*, 2015, **50**, pp. 57–71
[13] Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: 'Plethysmogram-based secure inter-sensor communication in body area networks'. Proc. IEEE Military Communications Conf., San Diego, 2008, pp. 1–7
[14] Miao, F., Bao, S.D., Li, Y.: 'A modified fuzzy vault scheme for biometrics-based body sensor networks security'. IEEE Global Telecommunications Conf., Miami, 2010, pp. 1–5
[15] Zhao, H.W., Qin, J., Hu, J.K.: 'Energy efficient key management scheme for body sensor networks', *IEEE Trans. Parallel Distrib. Syst.*, 2013, **24**, (11), pp. 2202–2210
[16] Sarah, A.A., Kausar, I.F., Khan, F.A.: 'A cluster-based key agreement scheme using keyed hashing for body area networks', *Multimedia Tools Appl.*, 2013, **66**, (2), pp. 201–214
[17] Chen, Y.N., Tsai, W.T.: 'Service-oriented computing and web software integration' (Kendall Hunt Publishing, Iowa, United States, 2015)
[18] Wu, S.M., Wei, L.L.: 'A broadcasting multi-digital signature scheme based on RSA', *Comput. Secur.*, 2013, **7**, pp. 25–28

CAAI Trans. Intell. Technol., 2018, Vol. 3, Iss. 2, pp. 114–118