2017 IEEE 13th International Symposium on Autonomous Decentralized Systems

Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys

Huawei Zhao*
Department of Internet Finance
Qilu University of Technology
Jinan, China
zhuav@163.com

Yong Zhang
LaiShang Bank Co.,LTD
Laiwu,China
lwbankzy@sina.com

Yun Peng
Department of Internet Finance
Qilu University of Technology
Jinan, China
296595865@qq.com

Ruzhi Xu
Department of Internet Finance
Qilu University of Technology
Jinan, China
rzxu@fudan.edu.cn

***Abstract*—Blockchain is a technology of recording ledgers in a distributed manner. It uses a consensus mechanism, digital signature and hash chains to realize the reliable storage of ledgers, and provide services such as traceability, integrity and no-repudiation for transactions in ledgers in a decentralized way. These services make blockchain have great application potentiality in the fields of healthcare, Fintech, computational law and so on. Before wide spreading its applications, blockchain must solve problems such as efficiency and privacy. Among these problems the privacy is an important one. Because blocks on blockchain are open, when transactions in blocks involve privacy data, these data can be leaked. Thus, certain security mechanisms must be built to protect privacy data. The core of these mechanisms is the appropriate key management schemes. However, blockchain is a developing technology, and few studies have been done on key management schemes for it. Because healthcare is a big application scenario of blockchain, in this paper, according to the features of health blockchain, we use body sensor network to design a lightweight backup and efficient recovery scheme for keys of health blockchain. 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.**

Keywords-blockchain, body sensor networks, biosensor nodes, fuzzy vault, PPG signals.

I. INTRODUCTION

Blockchain is first introduced in 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 decentralized manner. These technologies provide security services, such as non-repudiation, integrity, traceability for transaction contents and make bitcoins circulate cross the Internet freely to realize the value migration in untrusted networks. Later, people gradually realize that blockchain can be used in various fields such as healthcare, Fintech, computational law, audit, notarization and so on by designing various smart contracts based on blockchain, and can be greatly improve the efficiency and the security of transactions' processing and reduce the cost [3,4,5]. At present, it is widely believed that consensus in untrusted networks, robustness, value migration in a decentralization 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 future, and thus dramatically change the mode of our society life. Figure 1 shows the architecture of blockchain.

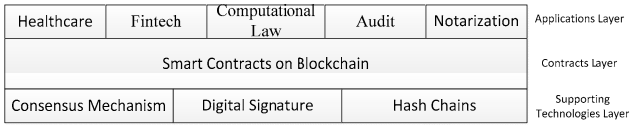

Figure 1. The architecture of blockchain

However, as a developing technology, blockchain still has been 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 popularization and application of blockchain. And among the problems the third one is the most highlighted one, for many applications of blockchain concern about privacy data and at present 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. Because blocks on

978-1-5090-4042-1/17 $31.00 © 2017 IEEE
DOI 10.1109/ISADS.2017.22

blockchain are public and shared by all of participants, when these blocks involve 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, for the encrypted blocks will be under the attack of statistical attack, while one key for one block is unfeasible yet, as it will spend a high cost storing and recovering 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 general 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 involve a great number of private health data, and it is necessary to solve the problem of privacy protection before the popularization of health blockchain.

With the development of electronic techniques, body senor networks (BSNs) emerge to surveille 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 remote hospital for further processing. In order 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 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 organized 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 and section5. In section 6 conclusions are drawn.

II. RELATED WORK

As a supporting technology of Bitcoin, the blockchain is known by the public with the popularization 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. Because 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 that using blockchain to protect personal data, and the scheme ensures users own and control their data. However, the scheme focuses on the construction of blockchain and how to authenticate the access to blockchain, and 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 PGP mechanism, and it 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 decentralized 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.

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, and few work has been done on this field.

III. A LIGHTWEIGHT BACKUP AND EFFICIENCT RECOVERY SCHEME FOR KEYS OF THE HEALTH BLOCKCHAIN

A. Application scenrio of health blockchain

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

Recently, the emergence of body senor networks (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 [9]. These nodes are equipped with various biosensors that can collect the physiological signals such as blood pressure (systolic and diastolic), electrocardiogram (ECG), 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 center such as a hospital [10]. Thus with the help of BSNs, a person can easily build his/her health file and a hospital can easily achieve a comprehensive health condition of a patient before treatment. So it can be seen that BSNs can significantly improve the current medical environment and open the door of the smart healthcare time.

In the traditional application scenario of BSNs, a user's physiological signals generally only are sent to one pointed 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 analyze these data, and send the analyses results to the user or the doctor. However, the scenario has some problems: (1) Monopoly problem: Concentrating users' physiological signals in one pointed 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. (2) Vulnerability problem: Storing physiological data in one hospital has vulnerability, and an accident will cause the loss of user's physiological data. (3) Privacy problem: The pointed hospital maybe delivers users' physiological data to insurance companies, medical companies and so on for commercial purposes without users knowing, which will violate users' privacy.

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

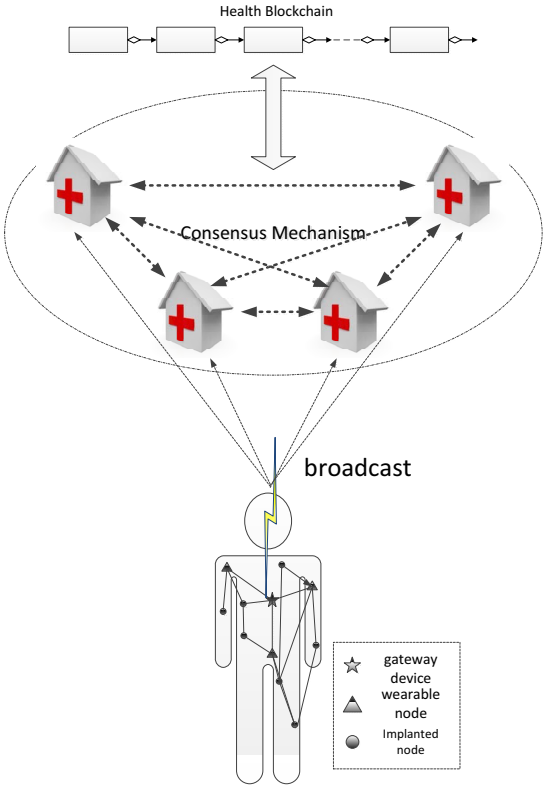

Figure 2. A smart healthcare system with blockchain and a BSN

In figure 2, a smart healthcare system consists of a BSN and a blockchain. The BSN is deployed on a user's body and is composed of a number of 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 pointed hospitals. These pointed hospitals form a healthcare alliance and each of them provides a blockchain node (a computer server). All of blockchain nodes make uses of consensus mechanism, digital signature and hash chain technology to maintain a health blockchain. When these blockchain nodes receive a broadcast message from the gateway device, they use consensus mechanism to check its validity, and once the message is checked valid, blockchain nodes will put the physiological message on the health blockchain.

In the scenario, each blockchain node stores a duplicate of the health blockchain, and when the user goes to any hospital in the health alliance, the visited hospital can draw the user's physiological data from its blockchain node. It solves the monopoly problem of users' physiological data. In addition, it solves the vulnerability problem of physiological data storage by multi-nodes' backup.

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 pointed 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 pointed signals. Next the node sends the encrypted signals to the health blockchain with the help of the gateway device. Because the blockchain nodes and the corresponding hospitals don't know the encrypting key, they cannot leak users' private physiological data to other organizations. 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 can be seen that in the scheme the health blockchain only store the cipher text of physiological data and the power of decrypting these data are controlled by the users. In other words, the user controls who can access his/her physiological data. It will solve the privacy problem.

In the realization, we use fuzzy vault technology to carry out the generation, backup and recovery of keys of health blockchain. And to explain the scheme clearly, we first give the detail of fuzzy vault in part *B*.

B. 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 [11] proposed a key management scheme called *PKA* that uses photoplethysmogram (PPG) signals to negotiate a common key between two biosensor nodes. The scheme including 5 steps:

(1) Production of PPG vector. Under a loose synchronization mechanism, biosensor node *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:

$$F_s =< f_s^1, f_s^2, ..., f_s^a > \text{ and } F_r =< f_r^1, f_r^2, ..., f_r^a > .$$

(2) Creating polynomial. Biosensor node *A* creates a polynomial $p(x)$ with a public order *a*. And 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 $K=e_a||e_{a-1}||, ..., ||e_1||e_0$.

(3) 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 $C=\{c_i, d_i\}$, $1 \leqslant i \leqslant W$, 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 $R=D \cup C$.

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

(5) 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 F_r. 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 [12] found that PKA left some practical problems unsolved. For instance: (1) PKA requires that biosensor node A and B share at least v+1 feature points to reproduce a v^{th} order polynomial, but it is not a goal easy to reach. (2) 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 [12] proposed an improved scheme for PKA: When biosensor node 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. And 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 don't need as many matched points as the research [11] 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 part C we use the improved PKA scheme to design the keys' generation, backup and recovery scheme for health blockchain.

C. The keys' generation and lightweight backup scheme for healt blockchain

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

(1) In the initialization 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.

(2) 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 $K=k_a||\ k_{a-1}||,...,||k_1\ ||k_0$, and then uses RS code to encode k_i ($0<=i<=a$) 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.

(3) A communicates with adjacent biosensor nodes measuring PPG signals to find a group of the same PPG signals to get a stable signals set. And then A encodes these signals into a vector F_s using FFT. Next, A puts 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.

(4) A chooses a pseudo-random function $F(\cdot)$ and calculates $K^*= F(k_0,K)$ as the encrypting key for the health blockchain. Here, k_0 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_0 to hide the vault R: $M=E(r \oplus k_0,R)$, here $E()$ is a symmetric encryption algorithm, $\oplus$ is the XOR operation.

(5) A sends $K^*||M||r||H(K^*)||ID_A$ to the gateway device in a secure manner using the security association between A and the gateway device. Here, $H()$ is a hash function, symbol "||" denotes concatenation operation. The security association may be built by a key management scheme for BSN. Currently many studies have been conducted on the kind of schemes [13,14, 15].

(6) The gateway device uses K^* to encrypt the physiological data and the encrypted data form a block to be put on the health blockchain. The messages $M||r||H(K^*)||ID_A||B_A$ also will be put on the health blockchain and used as a clue to recover K^*. 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, the gateway will delete K^*.

Figure 3 shows the encrypted block on the health blockchain.

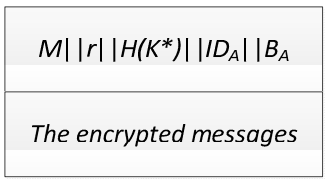

Figure 3. The encrypted block on the health blockchain

D. Efficient recovering keys of health blockchain

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

(1) The user uses his/her gateway to point out which encrypted block on the health blockchain will be decrypted. And then the gateway device 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.

(2) Once A receives $M||r||H(K^*)$, it uses r and pre-distributed k_0 to decrypt M to get the set R. And 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 F_r and then draws a points set U from R, where the x ordinates of points in U are the elements in F_r.

(3) 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.

(4) 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 $K^{*\prime}$. And 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 the gateway device by the security association between A and the gateway device. And then gateway device will decrypt the physiological data by K^*, and authorize other entities visiting them by other security mechanisms. Finally, the gateway device deletes K^* for the sake of security.

IV. Security analysis

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 analyze 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 one is attacking the BSN.

A. 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 Figure 3, the only information about K^* the adversary can get from the encrypted block is $H(K^*)$. Due 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.

Because 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.

B. 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.

V. Performance analysis

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 use change the

encrypting 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 heal 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.

VI. CONCLUSIONS

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 popularization 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 merged the BSN and the health blockchain, and used 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: (1) 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. (2) 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.

ACKNOWLEDGMENT

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).

REFERENCES

[1] Satoshi Nakamoto, “Bitcoin:A Peer-to-Peer Electronic Cash System”, www.bitcoin.org, pp.1-9, 2008.

[2] D. kraff, “Difficulty control for blockchain-based consensus systems”, PEER-TO-PEER NETWORKING AND APPLICATIONS, Vol.9,No.2, pp.397-413, 2016.

[3] K.Fanning, D.P. Centers,” Blockchain and Its Coming Impact on Financial Services”, JOURNAL OF CORPORATE ACCOUNTING AND FINANCE,Vol.27, No.5,pp.53-57,2016.

[4] J. Kishigami, S. Fujimura, H. Watanabe,A. Nakadaira, A. Akutsu, “The Blockchain-based Digital Content Distribution System”, IEEE 5th International Conference on Big Data and Cloud Computing, Dalian, China, pp.187-190,2016.

[5] S. Fujimura, H. Watanabe, A. Nakadaira, T.Yamada, A. Akutsu, J. Kishigami, ” BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain”, 5th IEEE International Conference on Consumer Electronics ,Berlin,pp.345-346, 2016.

[6] G. Zyskind, O. Nathan, A.S. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data”, IEEE Security and Privacy Workshops, 180-184, San Jose,CA, 2015.

[7] D.Wilson,G. Ateniese,“From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain (LONG), http://www.pubzone.org/dblp/journals/corr/WilsonA15,2015.08.

[8] H.Zhao, X.F. Li, L.K. Zhan, Z.C.Wu, “Data integrity protection method for microorganism sampling robots based on blockchain technolgy”, J.Huazhong Univ. of Sci.&Tech.(Natural Science Edition), Vol.43, pp. 216-219, 2015.

[9] H.W.Zhao, R.Z Xu, M.L. Shu, J.K.Hu,” Physiological-signal-based key negotiation protocols for body sensor networks: A survey”, Simulation Modelling Practice and Theory,Vol.65, pp.32-44,2016.

[10] M. Quwaider, Y. Jararweh, “Cloudlet-based Efficient Data Collection in Wireless Body Area Networks”, Simulation Modelling Practice and Theory. vol. 50, pp.57-71, Jan. 2015.

[11] K.K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, “Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks” , Proc. IEEE Military Communications Conference, San Diego, pp.1-7, 2008.

[12] F. Miao, S.D.Bao, Y.LI, “A modified fuzzy vault scheme for biometrics-based body sensor networks security”, IEEE Global Telecommunications Conference, Miami, pp.1-5, 2010.

[13] Huawei Zhao, Jing Qin, Jiankun Hu, “Energy Efficient Key Management Scheme for Body Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol.24, no.11, pp.2202-2210, 2013.

[14] A.A. Sarah, I.F. Kausar, F.A. Khan, “A cluster-based key agreement scheme using keyed hashing for Body Area Networks”, Multimed Tools Appl, pp.201-214, 2013.

[15] Yinong Chen, W.T. Tsai, Service-Oriented Computing and Web Software Integration, 5th edition, Kendall Hunt Publishing, 2015.