THE UNIVERSITY OF MELBOURNE

COMP90043 Cryptography and Security

Research Project

Blockchain for Medical IoT Security

Group 26

Name	Email	SID
Luoying Dong	luoyingd@student.unimelb.edu.au	1038287
Bokai Yi	bokaiy@student.unimelb.edu.au	1143061
Lihua Wang	lihuwang@student.unimelb.edu.au	1164051

School of Computing and Information Systems

Reflective Statements

Luoying Dong

In this project, I'm mainly responsible for the model introduction, CIA evaluation and conclusion. In the topic selection stage, my teammates and I first determined the application of blockchain in IoT security. Later, we looked up relevant papers respectively, and I found several well-done papers about the application of improved blockchain models in medical IoT security. After discussion and comparison, we finally determined the current theme and completed the work allocation. In the presentation stage, I completed the slides explanation of the model introduction, CIA model evaluation and conclusion, and prepared some related questions, such as the embodiment of the blockchain in the medical IoT model, etc. In the final report, I consulted many related papers, and after comparing each model, I selected a more representative model. After fully understanding it, I applied it to our own case with combining some drawbacks of the original blockchain technology in the model introduction part. In the CIA evaluation part, I mainly used the definition of CIA in the textbook as the basis to evaluate the performance of the model in three aspects: confidentiality, integrity and availability, as well as the performance of authority and anonymity. Finally, I made a short summary of our whole research.

Bokai Yi

In this project, I am mainly responsible for the introduction of the entire project and the generalization of common security issues in the medical Internet of Things. The introduction of security issues is to guide the research direction of our selected topics. After determining the topic of the project, I read a lot of literature, so I have a deep understanding of Blockchain and Medical IoT Security. And I exchanged views with my teammates at each group meeting. Good group communication makes the project progress smoothly. During the production of the video, in order to get a better video performance, I provided relevant screen recording software and PowerPoint templates as a reference. In the report section, I am responsible for abstract, introduction, security issues and future work. Overall, this is a fulfilling and enjoyable learning experience.

Lihua Wang

In this project, I mainly undertook the introduction of the details of the technology used in the new model, as well as the algorithm simulation and code verification of the technology implementation. And compared the advantages and disadvantages of these technologies. The encryption technology used in the new model is mainly based on a paper about the medical IoT model in the blockchain. The highlight technologies in the entire model include the lightweight data encryption algorithm SPECK, the Diffie-Helmen key exchange technology, and the ring digital signature technology to ensure user anonymity. After briefly explaining the principles of these technologies, I made some implementation of such technologies applying in the model, and programmed it in a python environment for simple code verification, and reflected the entire algorithm process in pseudo-code in the report. Finally, in the evolution section, I made critical evolution in the respect of such technologies, especially discussed the pros and limitation of the technologies. During the entire project process, whether it is presentation or report, I have been in charge of the technical part. I think this makes me Have a deeper understanding of encryption technology, and also expand the learning of many new technologies. When comparing the advantages and disadvantages of these encryption technologies, I consulted a large number of papers. In these processes, I also exercised my dialectical thinking and research ability.

CONTENT

Abstract

This paper discusses the integration of blockchain technology into the security of medical IoT. It concerns the common security risks in the medical Internet of Things, the defects of the original blockchain, and the improved security technology based on the blockchain. Besides, to better understand the security performance of the new technology, this paper evaluates the models and IoT cryptographic technologies involved.

Keywords —Blockchain, IoT, Cryptographic, Security risks.

I. Introduction

The quality of patient care and real-time monitoring of the patient's condition has become a primary concern in the medical community in recent years. The remote patient monitoring (RPM) system, combined with the Internet of Things, can solve this problem well. Because doctors can monitor and remotely treat patients' conditions outside of the traditional clinical environment [1]. In this way, not only can the patients be treated in time, but also the doctor's work efficiency can be improved. The remote patient monitoring (RPM) system mainly includes monitoring equipment for recording patient health data, transmission equipment linked to the Internet, and a database for storage. The big data analysis of the health data in the database by hospitals or medical institutions will provide new reference materials for related diseases.

Therefore, data privacy and secure data sharing in the Internet of Things have become incredibly important. Based on relevant medical IoT security literature, we found that blockchain technology can provide research ideas for solving such problems. The proof of work (PoW) encountered during the block creation process will be solved by hash calculation. Proof of work (PoW) is the essential decision to maintain block security [2]. Therefore, we used a distributed blockchain model that eliminates the concept of Proof of work (PoW).

II. Security issues in the medical Internet of Things (IoT)

A. privacy protection

The medical Internet of Things has many security risks in terms of user privacy and information transmission.

i. Attack by computer viruses, medical privacy is exposed without being noticed.

ii. The tracking of transmission equipment or medical equipment by the radio frequency identification system will threaten privacy and security.

iii. The positioning device, RFID device, or other medical equipment is monitored by the manufacturer.

iv. Local Information Server of Things (medical equipment carried by patients) and Remote Information Server of Things (equipment used by hospitals or medical institutions to receive health data) are vulnerable to malicious user behaviour analysis and traffic analysis.

B. Authentication and access control

i. IoT authentication includes identity authentication and message authentication. There are inevitably security issues at any stage of the certification process. The key can reasonably ensure that the user completes the identity authentication [3]. However, when any key in the communication user is stolen, the data security of the stolen user is threatened. Even the attacker will steal the data in the entire communication system.

ii. Message authentication can ensure the security and integrity of the information when the sender and receiver exchange information. Message authentication in the Internet of Things is accomplished through an authentication code. The sender determines that the receiver has received the data according to the returned message authentication code. An attacker can easily pretend to be the receiver by monitoring the static data stream of the verification code to steal the sender's transmission data.

iii. The purpose of access control is to reduce the intrusion of illegal users, but it cannot guarantee all users legal access to data resources. When the access authority is maliciously modified, or the access policy has loopholes, data security will be seriously threatened.

C. Data Security

The data in the Internet of Things (IoT) can be regarded as a dynamic data collection that continues to grow indefinitely over time [4]. Once the data stream is attacked, all data is at risk of being stolen. Mass data is received and sent through sensors, and then stored in the corresponding database. Unstructured data is generally uploaded through cloud storage. Regardless of the storage method, data needs to be repeatedly transmitted when it is used. The transmission of a large amount of data will increase the load of the server, and the security of the data will be reduced.

III. Blockchain solution for RPM and an improved model

A. Original blockchain solution and some disadvantages

1. Decentralization

In the blockchain network, there are no central management nodes and each node is equal. Each node records the information of the complete database [5]. This feature can significantly improve RPM's ability to resist external attacks because even if an attacker breaks a node, other nodes still retain the information of the whole database.

When a node receives data from the other node, it uses digital signatures to verify its identity. If the verification succeeds, the information it receives will be broadcast to the entire network. Thus, the blockchain can ensure the authentication of users.

However, the decentralized network has two obvious drawbacks, which are low scalability and delay. The IoT network is usually composed of a large number of nodes and is resource-limited. In original blockchain technology, to solve the PoW problem, a large amount of computational power is required in the hash function [6]. Therefore, as the number of users increases, blockchain will become less and less scalable. In our model, we use an overlay network of blockchain which is separated into multiple clusters to improve scalability and eliminate the PoW problem at the same time.

2. Trustless

In the blockchain network, data transmission at all nodes is open. But for medical data, patient privacy is important, and the original blockchain cannot guarantee the anonymity of data transmission. In our model, we use Ring Signature to ensure anonymity, that is, no one knows from whom the signature comes, except the signer himself.

3. Data Storage

In the blockchain, every node has all the records of a complete database, but the data of the Internet of Things is often so huge that it is unrealistic to store all the data in the blockchain. Therefore, we use the cloud to store big data and use the hash function to make access control.

4. Data Security

The blockchain uses asymmetric cryptography to encrypt data so that it cannot be tampered with during transmission [7]. In our model, to better improve key security, we first encrypt data using the ARX algorithm and then encrypt our key by using the public key of the receiver [5]. For safe public key transmission, the Diffie–Hellman key exchange technique is applied.

B. Improved model introduction

The model introduced in this section is cited from Dwivedi et al. (2019).

1. Overlay network

An overlay network is a distributed network based on p2p structure, which is directly connected with IoT devices and healthcare providers such as doctors and insurance companies. The overlay network consists of many nodes, which should have a legal certificate to get authorization before entering the network. The nodes can provide a digital signature for transactions or data after being authorized. To improve scalability and reduce delay, the nodes are divided into many clusters. In each cluster, a head node will take the responsibility of maintaining public the keys of its children. The cluster head shares the public keys with other cluster heads through Diffie–Hellman key exchange protocol. When a new node enters into the cluster, it can change the cluster state arbitrarily to avoid delay, such as altering the cluster head.

For example, let's consider a patient who wants to share his information with his health

insurance company. The patient node signs the transaction, sends his digital signature along with the company's public address to the overlay network. The cluster head verifies the signature with its public keys. If the verification succeeds, the head searches for the company's public key in the cluster. If available, broadcast the transaction in the cluster, otherwise broadcast the transaction and company's public address to other cluster heads. If verification fails, the head will broadcast the signature and public address to other clusters. The cluster heads also maintain the hash of data blocks that are stored in the cloud.

2. Cloud data storage

Instead of storing data in the blockchain, we use the cloud to store the huge data of the IoT network. Specifically, the cloud has multiple blocks intended for different user groups, and each block has a unique ID. The cloud is directly connected with the overlay network. When a block receives new data, the cloud calculates a new hash for all blocks, sends it along with the previous root hash to the overlay network. If the root hash value matches, the overlay network accepts the new hash, recalculates with the root value, and then generates a new hash for its hash chain. Therefore, the change of cloud can be easily detected by the overlay network.

3. IoT devices

Patients keep and collect their medical data by using wearable devices, such as a medical watch or other monitoring equipment. Patients can authorize or deny access from any other nodes, such as doctors or health care institutions. When the patient needs treatment, he can share his data with one or multiple doctors. Once the treatment ends, the patient can choose to close the share or continue authorizing access from certain targets.

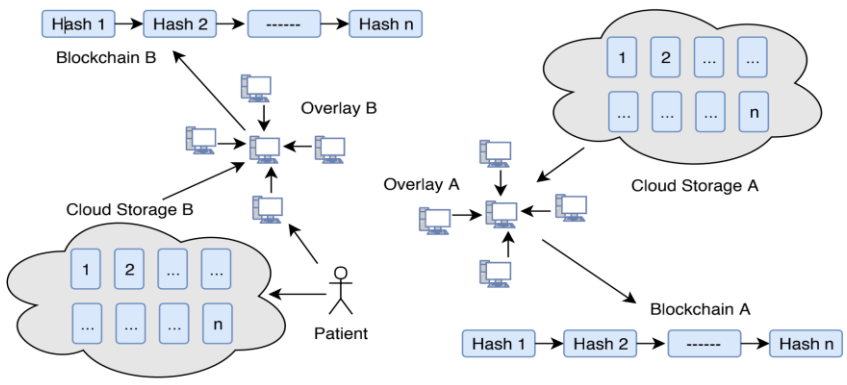

Figure1. Overlay network and cloud storage. [5]

IV. Cryptographic Techniques Details in the Model

A. ARX Encryption Algorithm

We implement data encryption based on the ARX algorithms, particularly, the latest example of ARX cipher -- SPECK [8] to support the encryption mechanism which is consists of simple Rotation, Addition and XOR operations. In our model, the main purpose is to protect the network from various attacks, rather than securing individual nodes. We suppose that once a defaulter node is found in the network, it can be blocked automatically. SPECK is a lightweight block cipher with the Feistel-like structure, in which each block is divided into two branches and both of them will be modified in each round. As shown in Figure 2, we illustrate how the rounding of SPECK work.

SPECK Round Function

SPECK uses 3 basic operations on n-bit word for each round:

a) bitwise XOR, $\oplus$,
b) addition modulo 2^n, $+$
c) left and right circular shifts by r_2 and r_1 bits, respectively

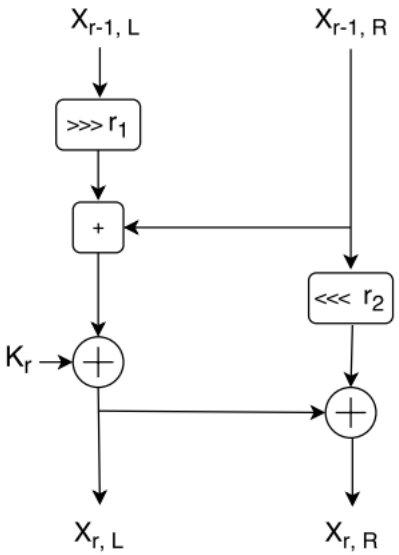

Figure 2. The SPECK round function. [5]

The left half n-bit word is represented by $X_{r-1,L}$ and the right half n-bit word is represented

by $X_{r-1,R}$ to the r-th round and n-bit round key applied in the r-th round is denoted by k_r. $X_{r,L}$and $X_{r,R}$represent the words output from the r wheel, which are calculated as follows:

$$X_{r,L} = ((X_{r-1,L} >>> r_1) + X_{r-1,R}) \oplus k_r \quad (1)$$
$$X_{r,R} = ((X_{r-1,R} <<< r_2) \oplus X_{r,L}) \quad (2)$$

B. Diffie–Hellman Key Exchange

All the technologies we mentioned before require public keys transferring over the network which may cause the model to be vulnerable. In order to enhance data security, we apply the Diffie–Hellman key exchange technique to secretly share the public key. For example, Alice (sender) and Bob (receiver) could exchange a shared secret as the way below:

1. Firstly, both parties (Alice and Bob) generate their own private/public keys (k_A; K_A) and (k_B; K_B), then publish or exchange their public keys and keep their private keys.
2. It is clear to figure out,

$$S = k_A \cdot K_B = k_A \cdot k_B \cdot G = k_B \cdot k_A \cdot G = k_B \cdot K_A \quad (3)$$

Alice could compute $S = k_A \cdot K_B$ privately, and Bob could calculate $S = k_B \cdot K_A$, which allows them to share this value as a secret.

C. Digital Ring Signature

We use Ring signature technology to provide anonymous data signature service for users (Figure 3). The signer uses the public key of other possible signers to generate a ring with a gap and then uses the private key to connect the gap into a complete ring. Once a user wants to mix his transaction with the ring, he/she will send a request containing self-public key $sk_{s_{pub}}$ to the blockchain network and waiting for a certain number of public keys sends back, where the public keys $sk1_{s_{pub}}, sk2_{s_{pub}}, sk3_{s_{pub}}, sk4_{s_{pub}}$are collected from other users $(u_1, u_2, \ldots, u_N)$ who also applied for mixing service, including $sk_{s_{pub}}$. Any verifier can use the public key of a ring member to verify whether a ring signature is generated by a potential signer. During the process, there is no trusted centre and no group establishment which makes the signer completely anonymous for the verifier.

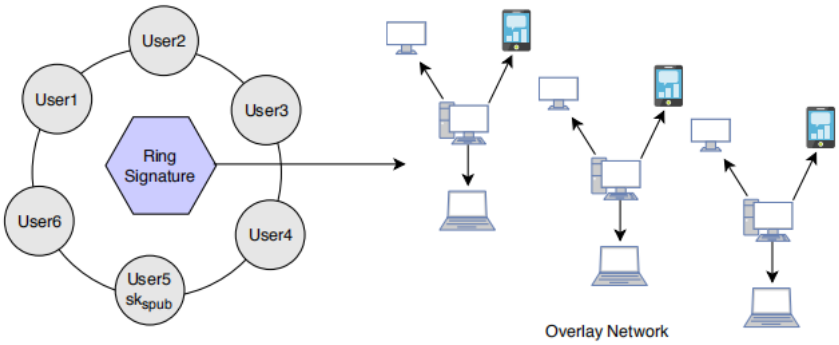

Figure 3. Ring Signature. [5]

V. Algorithms of Cryptographic Techniques in model

We first define the variable name k_{sym} for the symmetric key in symmetric encryption algorithms, as for asymmetric encryption, we define that the sender have generated one key pair: private key (sk_{priv}), public key (sk_{pub}), while the receiver have created another key pair: private key (rk_{priv}) and public key (rk_{pub}).

A. Algorithm 1 Data Encryption and Decryption

We use the symmetric key k_{sym} to encrypt plaintext P and generate a ciphertext C. Then, applying public-key cryptography to double encrypt the key k_{sym} with the receiver's public key rk_{pub}, and send the encrypted key C_k together with the ciphertext C.

Algorithm 1 Data Encryption.

```
1: function ENCRYPTION (P)
2:     if data is stored on the blockchain then
3:         Create a symmetric key k_sym
4:         C ← Encrypt_sym (P, k_sym)
5:         C_k ← Encrypt_asym (k_sym, rk_pub)
6:     else
7:         Nothing to do
8:     end if
9: end function
```

In Algorithm 2, the data decryption process is to decrypt the ciphertext C using the symmetric key k_{sym}. We first need to decrypt C_k to obtain the k_{sym}, since the C_k was produced by using the public key rk_{pub} of the receiver to double encrypt the original k_{sym}, so that, it can only be decrypted by using corresponding private key rk_{priv}. Then, we can apply the k_{sym} on ciphertext c and calculate the plaintext P.

Algorithm 2 Data Decryption.

1: **In:** Ciphertext C, C_k
2: **Out:** Decrypted plaintext P
3: **function** DECRYPTION $(C, C_k, rk_{priv}, k_{sym})$
4: $k_{sym} \leftarrow Decrypt_{asym}(C_k, rk_{priv})$
5: $P \leftarrow Decrypt_{asym}(C, k_{sym})$
6: **end function**

B. Algorithm 2 Ring Signature and Public Key Sharing

To add the digital signature, the sender firstly creates the hash value $hash_p$ by applying a hash algorithm to plaintext data P, and then encrypts $hash_p$ with private key $sk_{s_{priv}}$, thus obtaining the digital signature. The sender sends the plaintext P together with the digital signature to receivers so that they can use the public key $sk_{s_{pub}}$ to verify the signature. We also applied the ring signature to implement the anonymity of users in Algorithm 2. The block diagram of the model describes this process (see Figure 4).

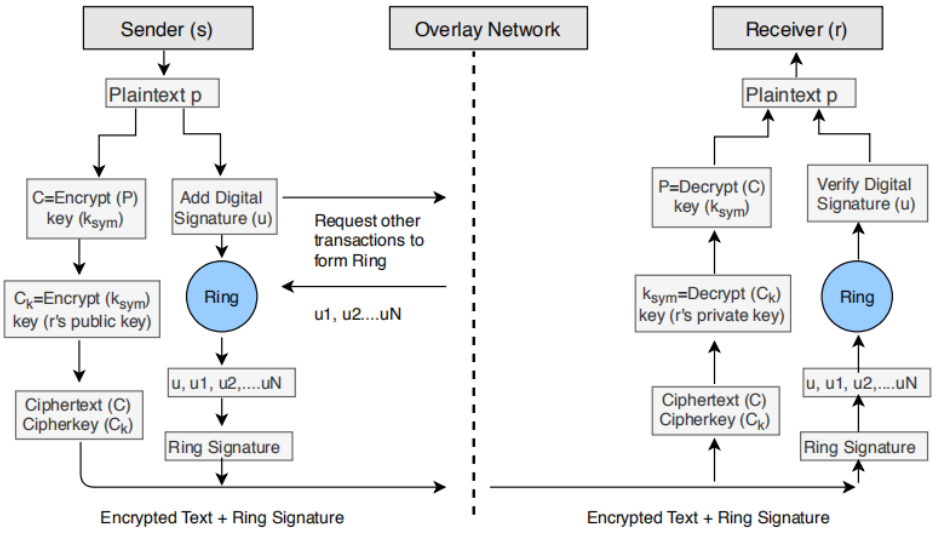

Figure 4. Block Diagram of Model. [5]

Algorithm 3 Ring Signature and Public Key Sharing.

1: **function** SIGNATURE (P)
2: **if** user chooses to be anonymous in the blockchain **then**
3: Create an asymmetric key pair: public key $sk_{s_{pub}}$ and private key $sk_{s_{priv}}$
4: $hash_p \leftarrow$ Create hash value of the data P
5: Generate the Digital Signature by $hash_p$ and signer's private key $sk_{s_{priv}}$
6: Applying Diffie-Hellman key exchange to share the public key $sk_{s_{pub}}$ with the receiver
7: Mix the signature with another network group into a ring
8: **end if**
9: **end function**

VI. Model Evaluation

A. Based on CIA Standard

CIA is the core requirement of all computer security models, which is confidentiality, integrity, and availability of information system resources [9].

Confidentiality involves a set of rules or acknowledgements. These rules are usually executed by confidential agreements which are used for restricting access or limiting some types of information, to provide security or privacy protection [9]. In other words, the security model must ensure that confidential information can't be obtained by unauthorized users. In our model, this requirement is satisfied with the public key and ARX algorithm. Our data is first processed with the ARX algorithm, and after symmetrically encrypted, the private key will be encrypted with the public key. The double-key encryption system ensures that the data is confidentially preserved, and the Diffie-Hellman key exchange protocol can ensure the safety of the public key.

Integrity means the accuracy and completeness of the information [9]. In our model, this requirement is satisfied with the data blocks hashing chain. The updated data will be accepted by the overlay network only if their root hash matches.

Availability means that authorized users can access the data freely [9]. This requirement is achieved by the use of a multi-cluster overlay network. Each transaction or request will first be processed by cluster headers, and then broadcast to the cluster group if verified. This mechanism can ensure the timely availability of information and avoid delay.

There are also two important requirements in RPM, which are authority and anonymity. They can be achieved by digital signature and ring signature respectively.

B. Techniques Discussion

1. ARX Encryption Algorithm (SPECK)

Pros: According to ECRYPT's Stream Cipher Benchmark (East), Speck is one of the fastest ciphers available, which can run well on various IoT devices and maintain an acceptable security

level regardless of the length of messages. According to the designers, although Speck is a "lightweight" cipher, it is designed to completely and safely resist attacks of Standard Selective Clear Text (CPA) and Selective Cipher Text (CCA) for each block and key size. Resisting related key attacks is also considered as a target.

Limitation: However, in a known key-differentiated attack model, there are no resistors to resist the attack, nor do the designers evaluate Speck as a hash function. In addition, although the Speck password family contains variants with the same block and key sizes as AES (Speck 128/128, Speck 128/192, and Speck 128/256 [10]), it also includes variants with block sizes as low as 32 bits and the same key size as AES. As low as 64-bit. These block and key sizes are unsafe for general use because they allow birthday and brute force attacks, regardless of the secure form of password. Therefore, though SPECK itself was severely criticized before it was rejected by ISO standardization due to a well-known password backdoor problem, it is still used here because it can safely resist key recovery attacks.

2. Diffie–Hellman Key Exchange

Pros: Since the output of the hash function is "random" and Discrete Logarithm Problem, the external observer would hardly decode the shared secret. Besides, the shared key is only generated when needed, which reduced the probability of being attacked when storing the key for a long time.

Limitation: However, Diffie–Hellman algorithm is computationally intensive, so it is vulnerable to blocking attacks, especially when a large number of keys requested by the adversary. The victims spend huge computing resources to solve the useless power coefficient instead of doing real work, which results in very expensive resources and CPU performance. Besides, it also cannot prevent a reply attack.

3. Digital Ring Signature

Pros: We can achieve two security properties, that is, Signers Anonymity and Signature Correctness by applying the digital ring signature, which makes it more prominent in terms of privacy and data security. For the former, the attacker cannot determine which member of the

ring generated the signature. Even if an attacker illegally obtains the private keys of all possible signers, the probability that he/she can determine the true signer is no more than $1/n,$ where n is the number of members (possible signers) of the ring. For the latter, this means the signature must be verified by everyone else, users can only accept valid signature and an invalid signature will be always rejected.

Limitation: However, there are still many problems with ring signature. For example, there are the limitations of the length of ring signature and ring public keys, since they all depend on the ring size, that is, the capacity to describe the information of ring members and all of their public keys. Besides, the signer can generate fake signers in the group due to the unconditional anonymity property of the ring signature. In addition, the algorithm cannot resist the public key attack of the selection group because it can choose any member to form a ring.

VII. Future Work

This paper conducts a preliminary study on the security blockchain model of the medical Internet of Things. The models used are all single components and involve relatively few types of algorithms and encryption technologies. Through numerous literature reviews, we found that there are still many cryptographic techniques and algorithms that can be implemented in the medical Internet of Things. Therefore, our future research direction is mainly to implement more algorithms and encryption technologies. In addition, we need to compare these methods to ensure better use of Blockchain to protect Medical IoT Security.

VIII. Conclusion

Blockchain technology is a good choice to address the privacy and security problems of the RPM system. However, some drawbacks of the original blockchain have significantly affected the efficient use of the model. Therefore, we introduce an improved model that is based on blockchain technology but uses cloud data storage, overlay networks, and some cryptography algorithms to build a more secure and efficient model for the RPM system.

Reference

[1] Polisena, J, Tran, K, Cimon, K. Home monitoring for congestive heart failure: a systematic review and meta-analysis. J Telemed Telecare 2010; 16: 68–76.

[2] Andrychowicz M., Dziembowski, S., Malinowski D., and Mazurek, L. 2014. Secure multiparty computations on bitcoin. In IEEE Security and Privacy.

[3] Kevin Ashton. That 'Internet of Things' Thing. RFiD Journal, 22:97--114, 2009.

[4] J. Habibi, A. Panicker, A. Gupta, and E. Bertino. Disarm: Mitigating buffer overflow attacks on embedded devices. In Network and System Security - 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings, pages 112–129, 2015.

[5] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.

[6] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 260-264). IEEE.

[7] Zhao, K., & Xing, Y. H. (2017). Overview of Internet of Things Security research driven by block chain technology. Information network security, 17(5), 1-6.

[8] Chen, H., & Wang, F. Y. (2005). Guest editors' introduction: Artificial intelligence for homeland security. IEEE intelligent systems, 20(5), 12-16.

[9] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.

[10] Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP Journal on Wireless Communications and Networking, 2020(1), 1-15.

[11] Wang, Dr. (2020). IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology. Journal of ISMAC. 2. 154-159. 10.36548/jismac.2020.3.003.

[12] G. Srivastava, J. Crichigno and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 2019, pp. 1-5, doi: 10.1109/CCECE.2019.8861593.