Blockchain Based Data Storage Mechanism in Cyber Physical System

Jin Wang[1,2], Wencheng Chen[1], Yongjun Ren[3], Osama Alfarraj[4], Lei Wang[5]

[1] School of Information Science and Engineering, Fujian University of Technology, China
[2] School of Computer & Communication Engineering, Changsha University of Science & Technology, China
[3] School of Computer and Software, Nanjing University of Information Science & Technology, China
[4] Computer Science Department, King Saud University, Saudi Arabia
[5] School of Civil Engineering, Changsha University of Science & Technology, China
jinwang@csust.edu.cn, qwer159606cwc@163.com, renyj100@126.com, oalfarraj@ksu.edu.sa, leiwang@csust.edu.cn

Abstract

As cyber-physical systems (CPS) flourish, the data security issues it encounters have increasingly become a research focus in the field. And it has received widespread attention from academia and industry. Blockchain technology has the characteristics of decentralization, openness, transparency, reliability and non-tampering. It has natural advantages in solving the security of the CPS. Thus, this paper first analyzes the security risks associated with data storage in cyber-physical systems and proposes the use of blockchain technology to ensure the secure storage of data in CPS. In traditional blockchains, the data layer uses Merkle hash trees to store data; however, the Merkle hash tree cannot batch add/delete and provide non-membership proof. In order to solve this problem, this paper improves the accumulator and uses the combination of accumulator and Merkle hash tree to provide batch addition/removal and non-membership proof. This paper constructs a Merkle hash tree accumulator, and proves that the scheme is feasible through correctness and security.

Keywords: Cyber-physical systems, Merkle hash tree, Accumulator, Data storage

1 Introduction

The cyber-physical systems (CPS) is the next-generation intelligent system based on embedded systems, computer networks, control theories, wireless sensor networks [1]. The cyber-physical systems use the next generation network to realize the interaction between computing process and the physical process, and operates the physical entities in a remote, reliable, real-time, secure, and collaborative manner in the cyberspace, and realizes the calculation, communication, and control function at all levels [2]. The CPS can not only complete the functions that can be completed by the traditional embedded system, but also in the future operating room, next-generation grid (energy grid), smart dam system [3-5], future defense system, next-generation automobile and its manufacturing, robot manufacturing, next-generation aircraft, smart buildings, smart homes, anti-rejection drugs and care for patients will also be widely used in future emerging fields, attracting widespread attention.

The cyber-physical system supports the deep integration of informatization and industrialization. Through the integration advanced information technology such as perception, computing, communication, control and automatic control technology, a complex system of mapping, timely interaction and efficient cooperation between human, machine, object, environment and information elements in physical space and information space is constructed [6]. The on-demand response, fast iteration and dynamic optimization of resource allocation and operation in the system are realized. In the process of uploading data to the CPS source node, the attacker can monitor and obtain the source of the data, and use the data traffic to obtain the location of the source node [7]. Many smart devices in CPS bring a lot of data, so that centralized data centers (such as cloud storage) unable to undertake corresponding management tasks [8]. Cyber-physical system needs to use information systems and physical equipment to complete information exchange, which will bring security issues during the transmission of information [9]. Therefore, the security of cyber-physical systems has attracted much attention, and blockchain can provide the best solution.

To improve the data security of the cyber-physical systems, some scholars have integrated blockchain technology into CPS to improve security [10-12]. Blockchain technology has the characteristics of decentralization, openness, transparency and non-tampering, and provides trust, transparency and secure data guarantee for cyber-physical systems [13-14].

*Corresponding Author: Yongjun Ren; E-mail: renyj100@126.com
DOI: 10.3966/160792642020112106010

Moreover, smart contracts are introduced into CPS to improve the security and automatic execution capabilities of CPS [15]. In blockchain technology, the data layer of the blockchain uses the Merkle tree to store data. However, the Merkle tree has the following disadvantages: it can only provide member proof, not non-member proof and batch add/delete, and storage takes up large memory. In recent years, cryptographic accumulators have attracted more and more interest. Because the accumulator has the characteristics of strongness, universality, compactness, it can provide the advantages of non-member proof, delete members at will, reduce data storage memory, so this paper improves the Merkle tree, combining the accumulator and the Merkle tree, which can reduce the memory of node data storage and better protect privacy.

This paper studies the storage mechanism of blockchain data based on accumulators, and further proposes a secure storage method of cyber-physical data based on the blockchain. In addition, this paper proposes the concept of adding/removing accumulators in batches, constructs a specific scheme using Merkle trees, and proves its security.

The main contributions of our works include the following aspects.

(1) It is proposed to integrate blockchain technology into CPS, which provides trust, transparency and security data guarantee for cyber-physical systems. In addition, the introduction of smart contracts into CPS improves the security and automatic execution capabilities of CPS.

(2) It is proposed to replace Merkle Tree with a password accumulator to realize member addition, deletion and non-member verification.

(3) An improved accumulator, combining RSA accumulator and Merkle Tree, is proposed to realize batch addition and deletion of members and non-member proof.

The remainder of this paper is structured as follows. Section 2 presents some related work on cyber-physical systems, blockchain technology, hash trees and RSA accumulators. In Section 3, the data security issues of cyber-physical systems are described. Moreover, in Section 4, the secure storage of data based on blockchain-based cyber-physical systems is described. Finally, Section 5 provides conclusions.

2 Related Work

2.1 Cyber-Physical System

Cyber-physical system is the integration of computing, communication and physical processes. The architecture is as illustrated in Figure 1 below. The aim of CPS is to enable the physical system to have the capabilities of computing, communication, precise control, remote cooperation and autonomy, and to form various corresponding autonomous control systems and information service systems through the Internet to complete the organic coordination between the real society and the virtual space [16-17]. CPS has similar capabilities to the Internet of Things, but CPS emphasizes more on circular feedback, requiring the system to play a feedback control role on the physical world through communication and calculation after perceiving the physical world.

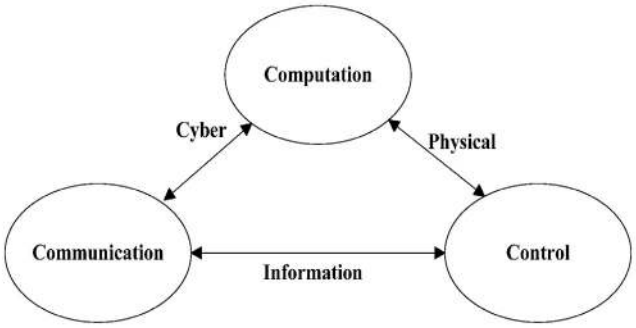


Figure 1. Cyber-physical system

2.2 Blockchain Technology

Blockchain is mostly known as the technology underlying the cryptocurrency Bitcoin [18-19]. The core idea of a blockchain is decentralization. This means that blockchain does not store any of its database in a central location, but will copy and distribute the blockchain on the participant network. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. This decentralized architecture has the advantages of tamper-proofing and no single point of failure vulnerabilities, which can ensure robust and secure operation on the blockchain [20]. In particular, everyone can access the blockchain without being controlled by any network entity. This is enabled through a mechanism called consensus, which is a set of rules that ensure that all participants agree on the state of the blockchain ledger.

Smart contracts are programmable applications that run on the blockchain network. Since the first smart contract platform known as Ethereum [21] was released in 2015, smart contracts have gradually become one of the most innovative topics in the blockchain field. A smart contract is essentially a collection of code and data, representing some business logic running on the blockchain [22]. The smart contract is located at a specific address on the blockchain. A basic example of a smart contract can be just to perform data update operations on the blockchain. For example, after verifying that there are sufficient funds in the account, update the account balance before debiting. As a more complex example, in the field of smart logistics, transportation costs can be dynamically adjusted according to the request time. The ledger will be agreed by both parties and will be coded as a smart contract. The corresponding funds

including the dynamic delivery fee will be automatically transferred according to the delivery time of the material.

2.3 Hash Tree

Hash trees are widely used to authenticate elements as set members. On the whole, the hash tree is a tag tree, the leaves are marked with different values $x \in X$, and the internal nodes are hashed on its sub-tags, and a fixed anti-collision hash function is used. In a hash tree prover, the positive proof consists of a minimum amount of data, which is necessary to verify the hash path from the leaf marked with x to the root.

2.4 RSA Accumulator

Suppose there is a set of k -bit elements $X = \{x_1, x_2, \ldots x_n\}$. Let N be a k'-bit *RSA* modulus with $k' > 3k$, namely $N = pq$, where p, q are strong primes numbers. Using the *RSA* accumulator, we can represent X compactly and securely with an accumulation value $acc(X)$, which is a k'-bit integer defined as $acc(X) = g^{r(x_1)r(x_2),\ldots r(x_n)} \bmod N$, Where $g \in QR_N$ and $r(x_i)$ is a $3k$ -bit prime representative, computed using a universal hash function h.

According to the accumulative value $acc(X)$, each element in the set X hash a member witness, the value is: $W_{x_i} = g^{\Pi_{x_j \in X: x_j \neq x_i} r(x_j)} \bmod N$. Given the accumulated value $acc(X)$ and the witness W_{x_i}, you can verify the membership of x_i in X by computing $W_{x_i}^{r(x_i)} \bmod N$ and checking that it is equal to $acc(X)$. Any adversary A, who does not know $\phi(N)$, subject to computation restrictions, cannot find another set of elements $X' \neq X$ such that $acc(X') = acc(X)$ unless A breaks the strong *RSA* assumption.

3 Cyber-Physical Systems Data Security Issues

CPS counters security vulnerabilities and system privacy issues, and there are many challenges in data security, privacy, centralization, and networking [23]. The intelligent manufacturing of many smart devices in CPS brings a lot of data, which makes the centralized data center unable to undertake the corresponding management tasks [24].

There are many types of CPS, while the security of the specific physical system, but there are still some are interlinked. For example, it is necessary to implement a mutual trust mechanism between internal nodes and external networks; the failure of important nodes will affect some of the neighboring nodes, such as the gateway node being maliciously attacked may affect the entire local network [25-28]. Cyber-physical systems need to use information systems and physical equipment to complete information exchange, which will bring security problems during the transmission of information, mainly in terms of identity authentication, privacy protection, integrity of data and information, and access control [29]. The above problems will lead to security risks in cyber-physical systems.

The cyber-physical system uses the application control layer as the decision-making layer, mainly to make decisions on task scheduling and resource allocation, and analyze economic constraints [30-32]. The application control layer can provide a variety of cyber-physical system platforms to integrate middleware, business management, and data management technologies. However, it should be noted that user information will be involved through platform software, which can easily cause information leakage [33-35].

Because cyber-physical systems have special physical characteristics, both communication and computing must meet real-time requirements. When configuring resources in a limited scenario, the cyber-physical system should meet adaptive requirements to prevent excessive use of resources, thereby reducing effective utilization. The network system will directly affect the cyber-physical system, which is mainly manifested in the awareness of the physical world and control execution. The data transmission layer will also be compromised by many factors such as denial of service attacks, authentication attacks, and aggregation node attacks [36-41]. In risk prevention, attention needs to be paid to identity authentication, intrusion detection, random key distribution, and traffic detection.

4 Blockchain-Based Cyber-Physical System Data Cecurity Storage

4.1 CPS Data Storage Model Based on Blockchain

First of all, this paper deploys a blockchain-based cyber-physical system data storage mechanism in the smart factory, which is illustrated in Figure 2 below.

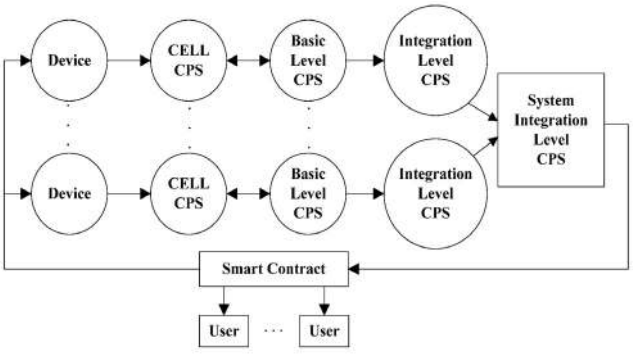


Figure 2. Cyber-physical system based on blockchain

The blockchain-based cyber-physical system data

security storage mechanism uses distributed storage. Firstly, the collected data is sensed by all devices in the smart factory. The data of each collected device can be transmitted to each other, and the data is uploaded to the basic level CPS. The CPS of each basic level will mutually store the information and transmission records of data transmission between each other. Then, the CPS at the basic level uploads the data to the CPS at the integration level. The CPS at the integration level deeply integrates and interconnects the uploaded data. At the same time, it audits and authenticates the newly accessed basic level CPS. Second, the system integration-level CPS realizes higher-level data storage for uploaded data. Finally, the data is fed back to the smart contract, and the smart contract processes the received data and generates a driving signal, which is fed back to the smart factory system. Setting up the smart contract can realize the user's access authority and the authority to obtain the type of data of the smart factory.

4.2 Blockchain Data Storage Mechanism Based on Accumulator

Since the data in the traditional blockchain is stored using Merkle hash trees, meaning that provide non-member proof, batch addition and deletion cannot be provided. By contrast, the accumulator has the function of providing non-member certification. Accordingly, this paper proposes to use the accumulator instead of the original Merkel tree in the block to build an accumulator-based blockchain data storage mechanism. The architecture is as illustrated in Figure 3 below.

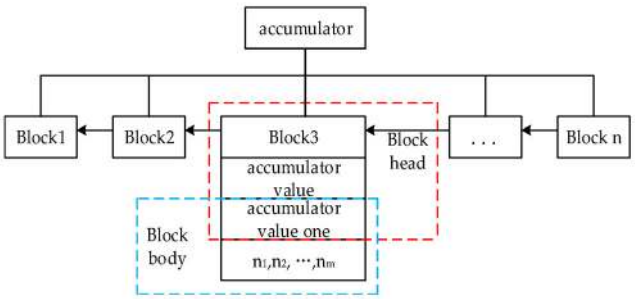


Figure 3. Improved blockchain based on accumulator

In the improved blockchain in this paper, all full nodes are connected to an accumulator, and full nodes are used for data storage and data verification. The Merkle tree of each block is replaced with an accumulator. All light nodes are not verified, only the current state and data transmission are stored, and the Merkle tree is replaced with an accumulator. Each block contains a block header and a block body. In addition to replacing the Merkle tree in the block body with an accumulator, this article also allows each full node in the blockchain network to share an accumulator, and light nodes do not. The Merkle root hash value in the block header becomes the accumulated value, and an accumulated value of 1 is added. This accumulated value is the accumulated value of the accumulator replacing the Merkle tree, and the Merkle tree in the block body becomes the accumulator. The data points $n_1, n_2, \ldots n_m$ represent the data collected by the nodes over a certain period. At this time, the hash value is not computed in the block body, but the accumulated value is computed, and the obtained accumulated value exists in the block header.

The blockchain is jointly maintained by the network nodes. The improved blockchain proposed in this paper comprises an accumulator for each block, and then each full node shares an accumulator, and the light node also has an accumulator, but the light node does not share an accumulator. Both accumulated values are stored in the block header, and each block connects each block by obtaining the hash value of the block header. When you want to query historical data, you can query it through the accumulator of the full node, and you can also verify whether the data belongs to the originally collected data. If you want to query the specific historical data in a certain period of time, you can query the corresponding data through the block accumulator, whether it is the overall data query or the block data query.

4.3 Improve Accumulator Definition

Because the accumulator usually has a single update element, it is difficult to meet the requirements of large-scale data addition. Therefore, this paper improves the accumulator. An improved accumulator is proposed, which can update elements in batches. The newly added data can be added to the accumulator in batches. For the elements to be deleted, useless data can be deleted from the accumulator in batches. G_i is the element group, A_i is the accumulated value of the element group G_i, an algorithm with the following functions: {*Setup*, *AccVal*, *Wit*, *Verify*, *Add*, *Del*, *UpdWit*, *Check*}.

①*Setup*: When the security parameter k is input, the public parameter ξ is output, and other functions take ξ as the input, and are set to run with a time polynomial of k. The accumulator manager will save the accumulated value and the G_i element group.

② *AccVal*: The given element group set $G = \{G_1, G_2, \ldots G_n\}$ is accumulated into the corresponding accumulated value $\{A_1, A_2, \ldots A_n\}$. The accumulated value set $X = \{A_1, A_2, \ldots A_n\}$ is accumulated as the accumulated value acc.

③*Wit*: Witness is a random algorithm. Input the element x_i, if $x_i \in X$, indicating that x_i has been accumulated, then output the witness of the membership W.

④*Verify*: Verification is a random algorithm. The witness W is used to check whether the element x

belongs to the element group G_i represented by the accumulated value A_i. The witness W of x effectively returns Yes, otherwise returns No.

⑤ *Add*: Adding is a random algorithm. The accumulated value is updated by adding an element group to the element group set G. Output a new accumulated value A^+ and acc', an updated witness W_{add}.

⑥ *Del*: Deletion is a random algorithm. Delete elements in batches from the element group set to update the accumulated value, and output the new accumulated value A^- and acc', an updated witness W_{del}.

⑦*UpdWit*: Witness update is a random algorithm. Take the added value/deleted value, the updated cumulative value and the witness update W_{add}/W_{del} as input, and return Yes, the witness is considered to be a valid proof. Generally, this is performed by all parties of the accumulator manager to verify the correct update of the accumulator manager.

⑧Check: It is a random algorithm. Take element group G_i, accumulated value A_i, acc, and witness W as input, and return Yes or No. Usually, the algorithm will be executed by parties outside the accumulator manager to verify that the manager updates the accumulator correctly. If it is Yes, then W is considered to be a valid proof, and the update operation using the new accumulated value as the accumulated value is valid. Otherwise, the witness W is invalid.

4.4 Accumulator Scheme Based on Hash Tree

The batch update dynamic accumulator proposed in this paper is realized by Merkle hash tree and combined with RSA accumulator. The program contains eight parts {*Setup*, *AccVal*, *Wit*, *Verify*, *Add*, *Del*, *UpdWit*, *Check*}. This scheme accumulates the corresponding accumulated value $X=\{A_1, A_2, \ldots A_n\}$ through the element group set $G=\{G_1, G_2, \ldots G_n\}$, the accumulated value is used as the leaf of the Merkle Tree, and accumulated into the accumulated value acc. And this solution can also add and delete elements in batches.

4.4.1 Specific Scheme

①*Setup*: When the security parameter k is input, the anti-collision hash function H of k security is sampled from H_k. Set to run with a time polynomial of k. The accumulator manager will save the accumulated value and the G_i element group.

②*AccVal*: The element group set $G=\{G_1, G_2, \ldots G_n\}$ is accumulated by the RSA accumulator to the corresponding accumulated value $X=\{A_1, A_2, \ldots A_n\}$, where $G_1=\{x_1, \ldots x_m\}$, $G_2, \ldots G_n$ also has n different elements. The computation is as follows: $A_1=g^{r(x_1)r(x_2),\ldots r(x_n)} \bmod N$. $A_2, \ldots A_n$ are solved in the same way. If A_i is not a power of 2, copy the last value of A_i until A_i is a power of 2, taking 4 element groups as an example, as shown in Figure 4. Use the accumulated value with A_i as its leaf hash function H and return the root acc. Accumulated value $acc=(H...(H(H(H(A_1, A_2), \ldots H(A_3, A_4)...)$.

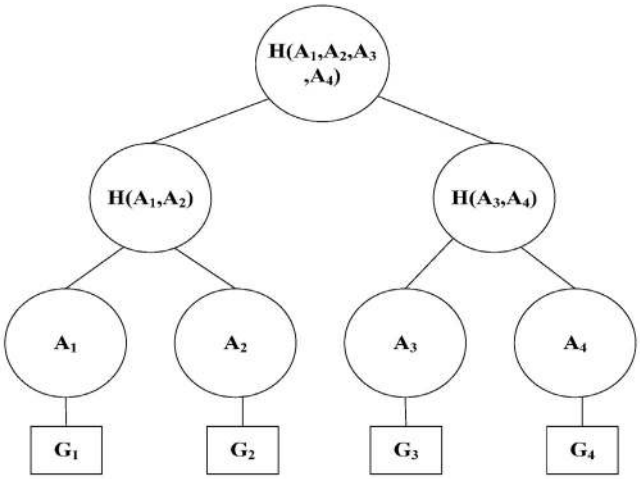


Figure 4. Improved accumulator

③ *Wit*: On the input element group G_i, the computation of the witness is as follows: First, the witness $H=(W_1, W_2)$. The calculation formula of witness W_1 in the first part is as follows: $W_1=g^{\Pi_{x_j \in X: x_j \neq x_i} r(x_j)} \bmod N$. Obtain the witness of each element in the G_i element group. W_2 is the path and location of the accumulated value A_i of the element group G_i to be verified in the Merkle Tree.

④*Verify*: The element group G_i, two accumulated values A_i, acc and the witness W is input. Witness W thinks it is (W_1, W_2). Recalculate whether the given element group G_i belongs to the accumulated value A_i and whether A_i belongs to acc. If yes, return Yes, otherwise return No.

⑤*Add*: Given a set of elements $G^{\oplus}=\{x_1^{\oplus}, x_2^{\oplus}, \ldots x_l^{\oplus}\}$ as an insertion. It can be inserted in the original G_i group, or the inserted element group additionally forms a leaf of a Merkle Tree. If you insert the accumulated value corresponding to a certain element group, the computation is as follows: $A^+=A_i^{r(x_1^{\oplus}), r(x_2^{\oplus}), \ldots r(x_l^{\oplus})} \bmod N$. At this time, the accumulated value in the Merkle Tree also changes correspondingly, for example, inserting in the G_1 group, the computation is as follows: $acc'=(H...(H(H(H(A^+, A_2), \ldots H(A_3, A_4)...)$. The verification

computation for the newly inserted element group is as follows: $x^{\oplus}=x_1^{\oplus}x_2^{\oplus}\ldots x_l^{\oplus}$, $g^{\prod_{x_i^{\oplus}\in X\cup X^{\oplus}:x_i^{\oplus}\neq x_j^{\oplus}} r(x_i^{\oplus})} \bmod N$. And the path and location of A_i in Merkle Tree.

⑥*Del*: Delete an element set $G^{\ominus}=\{x_1^{\ominus}, x_2^{\ominus}, \ldots x_l^{\ominus}\}$ from a certain element group G_i. The number of deleted elements is less than the number of elements in the element group G_i. The accumulated value changes after deleting the element set, and the computation is as follows: $x^{\ominus}=x_1^{\ominus}x_2^{\ominus}\ldots x_l^{\ominus}$, $A^{\cdot}=A_i^{\backslash r(x_i^{\ominus})} \bmod N$. At this time, the accumulated value in the Merkle Tree also changes correspondingly, for example, inserting in the G_1 group, the computation is as follows: $acc'=(H...(H(H(H(A^{-}, A_2), \ldots H(A_3, A_4)...)$.

⑦*UpdWit*: When input element group G_i, accumulator value A_i, acc and update witness W, if $W=(W_1, W_2)$, the algorithm outputs Yes.

⑧*Check*: It is a random algorithm. Take element group G_i, accumulated value A_i, acc, and witness W as input, and return Yes or No. Usually, the algorithm will be executed by parties outside the accumulator manager to verify that the manager updates the accumulator correctly. If it is Yes, then W is considered to be a valid proof, and the update operation using the new accumulated value as the accumulated value is valid. Otherwise, the witness W is invalid.

4.4.2 Correctness

The correctness of the tree accumulator means that if the input element belongs to the element group set G_i, and if the corresponding witness W has been calculated using Wit and UpdWit, the verification process should pass. The scheme {*Setup*, *AccVal*, *Wit*, *Verify*, *Add*, *Del*, *UpdWit*, *Check*} is correct. Both AccVal and Wit algorithms will output the correct accumulated value and witnesses, and the Add and Del algorithms will output new accumulated values and witnesses. All the probabilities in *k* are negligible.

Proof: First, show that the Verify algorithm is correct for the accumulator. Suppose a certain input element group $G_i=\{x_1, \ldots x_m\}$, A_i is its corresponding accumulated value, and acc is the accumulated value of Merkle Tree leaves. due to:

$$A_i = g^{r(x_1)r(x_2),\ldots r(x_m)} \bmod N \tag{1}$$

$$acc=(H...(H(H(H(A_1, A_2), H(A_3, A_4))...) \tag{2}$$

$$W_i^{x_i} = g^{\prod_{x_j\in X:x_j\neq x_i} r(x_j)} \bmod N \tag{3}$$

and so,

$$\begin{aligned} W_i^{x_i} &= g^{\prod_{x_j\in X:x_j x_i} r(x_j)r(x_i)} \bmod N \\ &= g^{r(x_1)r(x_2)\ldots r(x_m)} \bmod N \end{aligned} \tag{4}$$

A_i traces the path and position in the Merkle Tree, showing that A_i is added to acc. In a tree-based accumulator, if the input element group is accumulated into the accumulated value A_i, and the accumulated value A_i is accumulated into the acc through the Merkle Tree, the witness can provide a valid proof for the input element group.

When adding an input element group, for the newly added input element group $G^{\oplus}=\{x_1^{\oplus}, x_2^{\oplus}, \ldots, x_l^{\oplus}\}$, it is easy to verify the correctness in the same way; for its witness W_i is updated to W_i', the correctness of the display is as follows:

$$x_x^{\oplus}=x_1^{\oplus}x_2^{\oplus}\ldots x_l^{\oplus} \tag{5}$$

$$\begin{aligned} W_i^{\oplus x_i} &= g^{\prod_{x_i^{\oplus}\in X\cup X^{\oplus}:x_i^{\oplus}\neq x_j^{\oplus}} r(x_i^{\oplus})} \bmod N \\ &= A_i^{r(x_i^{\oplus})r(x_i^{\oplus})\ldots r(x_l^{\oplus})} \bmod N = A^{+} \end{aligned} \tag{6}$$

When A^{+} leaves in the Merkle Tree, calculate $acc'=(H...(H(H(H(A^{+}, A_2), \ldots H(A_3, A_4)...)$. For element deletion, you can Verify correctness in the same way.

4.4.3 Security

The security of the accumulator scheme is illustrated by an experiment in which the opponent plays the role of the user and tries to forge witnesses (that is, find valid witnesses for elements that do not belong to the set). In terms of security parameters, such opponents must succeed with a very low probability. If the opponent finds a set of elements $G_i=\{x_1, x_2, \ldots, x_n\} \subseteq X$, where X is the set of element groups, the element $x'\in X\setminus G_i$ and a witness W' can prove that x' has accumulated in the possibility in the accumulated value is negligible.

Merkle Tree accumulative set A_i. We limit the opponent, so he must select the element group G_i, A_i and acc for a series of effective operations, which can generate the accumulated value Acc. By noting that in the scenario we are considering, parties other than the accumulator manager can use the Check algorithm to externally verify the correctness of each update operation, it can be proved that this last restriction is reasonable. Therefore, as long as the adversary cannot cheat the Check verification, security can be guaranteed, that is, given an accumulator value acc before the change, the adversary cannot effectively generate the accumulator value after the change acc', the element group set G_i and the corresponding the

accumulated value A_i .

If the opponent A for all polynomial time has:

$$\begin{aligned}&\Pr[\xi \leftarrow Setup(\lambda);(G, X, x_i, W_i) \leftarrow A(\xi);\\ &x_i \notin X; acc \leftarrow acc(X) : Verity(acc, x_i, W_i)\\ &= true] \le negl(\lambda)\end{aligned} \tag{7}$$

Then the accumulator is secure.

First, perform an adding operation to add a new element group $G^{\oplus} / G^{\ominus}$ to obtain G' and the corresponding accumulated values A^+ and A^- . The corresponding accumulated value X of the element group $X = \{A_1, A_2, \ldots, A_n\}$. By updating or replacing the corresponding accumulated value A_i with the value A^+ / A^- , the new node value is obtained. During the witness update, it must be ensured that the new storage tree used to compute the new accumulated value has: the updated A_i is the changed node value and can only appear once.

5 Conclusion

This paper first analyzes the challenges of cyber-physical system data security, then analyzes the blockchain technology, and proposes a blockchain-based cyber-physical system data security storage mechanism. The data layer of the blockchain uses Merkel trees to store data, but Merkel trees cannot provide bulk add/delete and proof of non-membership. It accumulates the advantages of strongness, universality and compactness of the appliance. It can provide non-member proof, reduce data storage overhead, and better protect privacy. Therefore, this paper constructs an accumulator-based blockchain data storage. However, the traditional accumulator is not secure enough to update elements in batches. Therefore, in order to solve the problem of data storage expansion in the blockchain, an accumulator based on an improved hash function is proposed, combined with an RSA accumulator. It is not only secure, but also can add and delete elements in batches. Finally, the validity and security of the proposed scheme are proved.

Acknowledgments

We thank Researchers Supporting Project No. (RSP-2020/102) King Saud University, Riyadh, Saudi Arabia, for funding this research. This work is also supported by the National Key Research and Development Program of china (2019YFC1511000) and by the NSFC (61772454, 61772280, 62072249).

References

[1] J. Herwan, S. Kano, R. Oleg, H. Sawada, N. Kasashima, Cyber-physical System Architecture for Machining Production Line, *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, St. Petersburg, Russia, 2018, pp. 387-391, DOI: 10.1109/ICPHYS.2018.8387689.

[2] K. D. Singh, S. K. Sood, 5G Ready Optical Fog-assisted Cyber-physical System for IoT Applications, *IET Cyber-Physical Systems: Theory & Applications*, Vol. 5, No. 2, pp. 137-144, June, 2020.

[3] D. Cao, Y. C. Jing, J. Wang, B. F. Ji, O. Alfarraj, A. Tolba, X. Ma, Y. Liu, ARNS: Adaptive Relay-node Selection Method for Message Broadcasting in the Internet of Vehicles, *Sensors*, Vol. 20, No. 5, pp. 1338, March, 2020.

[4] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah, G. Kim, A PSO based Energy Efficient Coverage Control Algorithm for Wireless Sensor Networks, *Computers Materials & Continua*, Vol. 56, No. 3, pp. 433-446, 2018.

[5] D. Cao, B. Zheng, B. F. Ji, Z. B. Lei, C. H. Feng, A Robust Distance-based Relay Selection for Message Dissemination in Vehicular Network, *Wireless Networks*, Vol. 26, No. 3, pp. 1755-1771, April, 2020.

[6] S. Li, S. Zhao, P. Yang, P. Andriotis, L. Xu, Q. Sun, Distributed Consensus Algorithm for Events Detection in Cyber-physical Systems, *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 2299-2308, April, 2019.

[7] A. Burg, A. Chattopadhyay, K. Lam, Wireless Communication and Security Issues for Cyber-physical Systems and the Internet-of-Things, *Proceedings of the IEEE*, Vol. 106, No. 1, pp. 38-60, January, 2018.

[8] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, W. Hong, A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems, *IEEE Access*, Vol. 8, pp. 54371-54401, March, 2020.

[9] C. P. Ge, W. Susilo, J. D. Wang, Z. Q. Huang, L. M. Fang, Y. J. Ren, A Key-policy Attribute-based Proxy Re-encryption without Random Oracles, *The Computer Journal*, Vol. 59, No. 7, pp. 970-982, July, 2016.

[10] A. Gu, Z. Yin, C. Fan, F. Xu, Safety Framework Based on Blockchain for Intelligent Manufacturing Cyber Physical System, *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, 2019, pp. 1-5.

[11] A. Shukla, S. K. Mohalik, R. Badrinath, Smart Contracts for Multiagent Plan Execution in Untrusted Cyber-physical Systems, *2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*, Bengaluru, India, 2018, pp. 86-94,.

[12] A. B. Masood, H. K. Qureshi, S. M. Danish, M. Lestas, Realizing an Implementation Platform for Closed Loop Cyber-physical Systems Using Blockchain, *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, 2019, pp. 1-5.

[13] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, J. Wang, Blockchain-enabled distributed Security Framework for Next-generation IoT: An Edge Cloud and Software-defined Network-integrated Approach, *IEEE Internet of Things Journal*, Vol. 7, No. 7, pp. 6143-6149, July, 2020.

[14] Y. J. Ren, F. J. Zhu, P. K. Sharma, T. Wang, J. Wang, O.

Alfarraj, A. Tolba, Data Query Mechanism Based on Hash Computing Power of Blockchain in Internet of Things, *Sensors*, Vol. 20, No. 1, pp. 207, January, 2020.

[15] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, S. W. Kim, Smart Contract Privacy Protection Using AI in Cyber-physical Systems: Tools, Techniques and Challenges, *IEEE Access*, Vol. 8, pp. 24746-24772, January, 2020.

[16] C. Shang, X. Bao, L. Fu, L. Xia, X. Xu, C. Xu, A Novel Key-Value Based Real-time Data Management Framework for Ship Integrated Power Cyber-physical System, *2019 IEEE Innovative Smart Grid Technologies- Asia (ISGT Asia)*, Chengdu, China, 2019, pp. 854-858.

[17] V. Maru, S. Nannapaneni, K. Krishnan, Internet of Things Based Cyber-physical System Framework for Real-time Operations, *2020 IEEE 23rd International Symposium on Real-Time Distributed Computing (ISORC)*, Nashville, TN, USA, 2020, pp. 146-147.

[18] J. Qi, J. Wang, Y. J. Ren, Y. Liu, G. Kim, Integrity Verification Mechanism of Sensor Data Based on Bilinear Map Accumulator, *ACM: Transactions on Internet Technology*, January, 2020, http://doi.org/10.1145/3380749.

[19] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao, J. Wang, Blockchain-based Systems and Applications: A Survey, *Journal of Internet Technology*, Vol. 21, No. 1, pp. 1-14, January, 2020.

[20] Y. J. Ren, Y. Leng, Y. P. Cheng, J. Wang, Secure Data Storage Based on Blockchain and Coding in Edge Computing, *Mathematical Biosciences and Engineering*, Vol. 16, No. 4, pp. 1874-1892, March, 2019.

[21] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, *IEEE Access*, Vol. 4, pp. 2292-2303, May, 2016.

[22] Y. J. Ren, Y. Leng, F. J. Zhu, J. Wang, H. J. Kim, Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network, *Sensors*, Vol. 19, No. 10, pp. 2395, May, 2019.

[23] W. Yu, T. Dillon, F. Mostafa, W. Rahayu, Y. Liu, Implementation of Industrial Cyber Physical System: Challenges and Solutions, *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, Taipei, Taiwan, 2019, pp. 173-178.

[24] J. Al-Jaroodi N. Mohamed, PsCPS: A Distributed Platform for Cloud and Fog Integrated Smart Cyber-physical Systems, in *IEEE Access*, Vol. 6, pp. 41432-41449, July, 2018.

[25] X. Jin, W. M. Haddad, T. Yucelen, An Adaptive Control Architecture for Mitigating Sensor and Actuator Attacks in Cyber-physical Systems, *IEEE Transactions on Automatic Control*, Vol. 62, No. 11, pp. 6058-6064, November, 2017.

[26] J. Wang, X. J. Gu, W. Liu, A. K. Sangaiah, H. J. Kim, An Empower Hamilton Loop Based Data Collection Algorithm with Mobile Agent for WSNs, *Human-centric Computing and Information Sciences*, Vol. 9, No. 1, pp. 1-14, May, 2019.

[27] J. Wang, W. B. Wu, Z. F. Liao, R. S. Sherratt, G. J. Kim, O. Alfarraj, A. Alzubi, A. Tolba, A Probability Preferred Priori Offloading Mechanism in Mobile Edge Computing, *IEEE Access*, Vol. 8, pp. 39758-39767, February, 2020.

[28] J. Wang, W. B. Wu, Z. F. Liao, A. K. Sangaiah, R. S. Sherratt, An Energy-efficient Off-loading Scheme for Low Latency in Collaborative Edge Computing, *IEEE Access*, Vol. 7, pp. 149182-149190, October, 2019.

[29] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, M. Tehranipoor, Introduction to Cyber-Physical System Security: A Cross-layer Perspective, *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 3, No. 3, pp. 215-227, July-September, 2017.

[30] J. Wang, H. Abid, S. Lee, L. Shu, Feng Xia, A Secured Health Care Application Architecture for Cyber-physical Systems, *Control Engineering and Applied Informatics*, Vol.13, No.3, pp.101-108, December, 2011.

[31] C. P. Ge, W. Susilo, Z. Liu, Z. Y. Xia, P. Szalachowski, L. M. Fang, Secure Keyword Search and Data Sharing Mechanism for Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, January, 2020, DOI: 10.1109/tdsc.2020. 2963978.

[32] C. P. Ge, Z. Liu, J. Y. Xia, L. M. Fang, Revocable identity-based Broadcast Proxy Re-encryption for Data Sharing in Clouds, *IEEE Transactions on Dependable and Secure Computing*, February, 2019, DOI: 10.1109/TDSC.2019. 2899300.

[33] C. P. Ge, W. Susilo, L. M. Fang, J. D. Wang, Y. Q. Shi, A CCA-secure Key-policy Attribute-based Proxy Re-encryption in the Adaptive Corruption Model for Dropbox Data Sharing System, *Designs, Codes and Cryptography*, Vol. 86, No. 11, pp. 2587-2603, November, 2018.

[34] L. M. Fang, W. Susilo, C. P. Ge, J. D. Wang, Public Key Encryption with Keyword Search Secure against Keyword Guessing Attacks without Random Oracle, *Information Sciences*, Vol. 238, pp. 221-241, July, 2013.

[35] L. M. Fang, W. Susilo, Y. J. Ren, C. P. Ge, J. D. Wang, Chosen Public Key and Ciphertext Secure Proxy Re-encryption Schemes, *International Journal of Digital Content Technology and Its Applications*, Vol. 4, No. 9, pp. 151-160, December, 2010.

[36] H. Jeon, Y. Eun, A Stealthy Sensor Attack for Uncertain Cyber-physical Systems, *IEEE Internet of Things Journal*, Vol. 6, No. 4, pp. 6345-6352, August, 2019.

[37] J. Wang, Y. Q. Yang, T. Wang, R. S. Sherratt, J. Y. Zhang, Big Data Service Architecture: A Survey, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 393-405, March, 2020.

[38] J. Wang, Y. Gao, C. Zhou, R. S. Sherratt, L. Wang, Optimal Coverage Multi-path Scheduling Scheme with Multiple Mobile Sinks for WSNs, *Computers, Materials & Continua*, Vol. 62, No. 2, pp. 695-711, 2020.

[39] H. Jia, Y. Ding, R. Peng, Reliability Assessment of Data Storage in Cyber Physical Systems, *2018 3rd International Conference on System Reliability and Safety (ICSRS)*, Barcelona, Spain, 2018, pp. 62-66.

[40] J. Wang, W.C. Chen, L. Wang, R. S. Sherratt, T. Alhussain, O. Alfarraj, A. Tolba, Data Secure Storage Mechanism of Sensor Networks Based on Blockchain, *Computers, Materials & Continua*, Vol.65, No.3, pp.2365-2384, September, 2020.

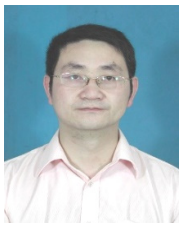
[41] J. Wang, Y. N. Tang, S. M. He, C. Q. Zhao, P. K. Sharma, O.

Alfarraj, A. Tolba, LogEvent2vec: LogEvent-to-vector Based Anomaly Detection for Large-scale Logs in Internet of Things, *Sensors*, Vol. 20, No, 9, pp. 2451, May, 2020.

Biographies

Jin Wang received the B.S. and M.S. degree from Nanjing University of Posts and Telecom., China in 2002, 2005 respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, he is a professor at Changsha University of Science and Technology. He has published more than 400 international journal and conference papers. His research interests mainly include wireless sensor network, network performance analysis and optimization. He is an IET Fellow, and senior member of IEEE.

Wencheng Chen received the B.S. degree in Ningde Normal University, China, in 2016. He is a postgraduate student in Fujian University of Technology, Fuzhou, China. His current research interests include blockchain and accumulators.



Yongjun Ren obtained the Ph.D. degree in the computer and science department at the Nanjing University of Aeronautics and Astronautics, China, in 2008. Now he is serving as a full time faculty in the Nanjing University of Information Science and Technology. His research interests include applied cryptography and blockchain.

Osama Alfarraj received the master's and Ph.D. degrees in information and communication technology from Griffith University, in 2008 and 2013, respectively. He is currently an Associate Professor of computer sciences at King Saudi University, Riyadh, Saudi Arabia. His current research interests include eSystems (eGov, eHealth, and ecommerce), cloud computing, and big data. He served as a Consultant and a member of the Saudi National Team for Measuring E-Government, Saudi Arabia, for two years.

Lei Wang is currently a professor in the School of Civil Engineering, Changsha University of Science and Technology, China, where he received his Ph.D. in 2008. His research interests include the intelligent construction and maintenance of structures, the structural durability, and the structural reliability.