Novel Data Protection for Bounded-Error IoT with Blockchain Smart Contract

Yu-Kai Tseng[1*], Chia-Hui Wang[2], Ray-I Chang[1]

[1]Dept. of Engineering Science and Ocean Engineering National Taiwan University Taipei, Taiwan
[2]Dept. of Computer Science and Information Engineering Ming Chuan University Taoyuan, Taiwan
[*]Corresponding Author: Email: [a]r07525116@ntu.edu.tw

2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII) | 978-1-7281-9333-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICKII50300.2020.9318935

Abstract

Due to the rapid development of IoT systems and applications, a large amount of sensors' data has been generated. Processing and analyzing these data provide users with better applications in diversity. However, current wireless sensing nodes still have a significant issue of power consumption. As the application requirements usually have bounded-error tolerance in IoT systems, our previous research proposed bounded-error data compression to extend the lifetime of IoT system. Meanwhile, the IoT data storing and sharing often rely on the third party service providers. It created another issues of data privacy. To solve these problems, this paper proposes a bounded-error IoT (BIoT) data privacy protection scheme via blockchain smart contract to provide secure data storing and sharing. BIoT not only extends the lifetime of IoT systems, but also provides different levels of service quality in privacy protection according to the agreement of the rights and payment in smart contract. Experimental results demonstrate that BIoT can prolong the IoT system lifetime with data privacy protection.

Keywords: bounded-error, IoT privacy, blockchain, quality of protection

Introduction

The Internet of Things (IoT), integrating information technology (IT) and operational technology (OT), can be applied in various fields for personal, enterprise and public applications including eHealth/smart healthcare [1], smart manufacturing [2], smart transportation [3], via sensor devices. With the rapid development of these IoT applications, a huge and varied sensor data has been generated. Moreover, applying the data mining on these data fosters more diversified and convenient applications for end users. Therefore, all the people, company and government consider the sensor data as the important asset for different purposes. The users pay much more attention to privacy issues as the larger amount of data is collected and delivered by IoT devices.

In various IoT systems, due to their applied technologies and some barriers in hardware, the sensing data often differ from the original and real values such as analog to digital or environmental noise. However, this error should be limited (i.e. bounded-error) to avoid the excessive error to jeopardize the credibility of IoT applications. The bounded-error should follow some defined standards. For examples, National Taiwan Central Weather Bureau (NTCWB) tolerates the bounded-error of 0.1°C [4] of the temperature sensing value of meteorological observation stations or ASHRAE standards [5], while refrigerators and air-conditioners tolerate the bounded-error of 0.5°C in temperature. As the application requirements usually have bounded-error tolerance in a real IoT system, our previous research proposed the compression schemes for different bounded-error data [6] to reduce the power consumption of IoT communication for extending IoT system lifetime.

Smart contract is a computer program or a transaction protocol which is automatically executed to control or document legally relevant events and actions according to the contract or agreement of service [7]. The smart contract is coupled and deployed with the blockchain to each peer node on the Internet even if it's trustless. Blockchain technology ensures that the smart contract code cannot be changed after deployment and that the results in each node run the same smart contract in an undeniable agreement. Moreover, the result of execution is verified by all peer nodes. Thus, smart contract coupled with the blockchain preserves the immutable, deterministic and distributed features.

In this paper, we enhance the protection of the privacy of sensor data through bounded-error concept to blockchain smart contract towards building a big sensor data market through Ethereum [8] blockchain technology. With the proposed bounded-error IoT data privacy protection scheme (called BIoT), the different bounded-errors are given and based on their authority and payment when a third party wants to access the sensor data. Using privacy protection preserved in the data precision from different bounded-errors, different levels of service quality for data mining are provided. The method in this study ensures that IoT service providers, third parties and users not only conduct data transactions without trusting each other, but also protect the privacy of IoT data and access users. Furthermore, users can be encouraged to provide various IoT data in their applications, so that researchers and enterprises provide more solutions for IoT applications.

Related Work

IoT devices sense, collect and share large amounts of data from things over Internet, which is challenging for security and privacy [9]. Since big sensor data are usually stored in a third-part cloud server, it is an issue for both of users and third parties how to ensure that the third party can carry out various users' data mining on the server to provide different users' IoT applications with protecting their data privacy from each other.

Besides, as it is difficult to supply persistent power for the wireless sensors in IoT, the reduction of the power consumption of resource-constrained sensor nodes has become a significant research topic to effectively extend the lifetime of IoT system. Since the data transmission consumes the most power [10][11] in sensors, many data compression mechanisms were used to extend the lifetime of IoT systems.

ISBN: 978-1-7281-9333-5

A. Blockchain Smart Contract to Protect Data

Because the blockchain technology allows its application to be implemented in a decentralized way without the trust of third parties, the decentralized application (DAPP) is an application that is mostly or entirely decentralized over peer to peer (P2P) network. All possible parts of the DAPP (i.e. frontend software, backend software, data storage) can be implemented in decentralized style.

There are three advantages of DAPPs over conventional APPs in centralized architecture: resiliency, transparency and censorship resistance. Thus, DAPP has no downtime and is available as long as the blockchain is running. Besides, any interaction between users and DAPP is stored in blockchain without interference from any centralized control.

Smart contracts are the most important part of DAPP, being used to store the business logic, state and calculations of decentralized application. However, blockchain technologies (Bitcoin, Ethereum, Hyperledger) provide trusted execution platform for smart contracts. For example, Ethereum smart contract has the feature of Turing complete, so makes the DAPP of the Ethereum blockchain gradually increase.

The combination of blockchain smart contract and IoT can develop diversified DAPPs for many industries [12]. It can provide the trust for large amount of sensing data that is continuously shared and exchanged by the IoT system and use smart contract to realize safe data transactions between users and third parties.

In the past, IoT data was usually stored in the third-party cloud server. The third-party service provider provided data query and analysis services. However, this caused users to worry about their own data privacy, which has also led to the creation of IoT data markets for data owners and third parties.

In Ref. [13], the blockchain IoT data market and a data review system based on Ethereum were proposed to ensure the integrity of user comments on data. Reference [14] proposed a new type of IoT infrastructure, using decentralized and trustless nature of the blockchain which let data access be managed by the blockchain. Combined with the fault-tolerant distributed data storage that resists DDOS, all of IoT end devices can be integrated with the architecture based on their computing and storage capabilities.

B. Bounded-Error to Prolong IoT Lifetime

Real applications allow a range of bounded-error to avoid excessive errors affecting the quality of sensed data because the data measured by the node cannot reach the accuracy in one hundred percent. Reference [15] proposed the bounded-error data compression for temporal correlation, spatial correlation and data correlation based on the special bounded-error feature of IoT. The bounded-error in the data during the compression process improves the compression rate and achieves the purpose of saving sensor power consumption [15][16][17]. It is different from lossy and lossless compression. Lossy compression has no predictable error bound with seriously distorted. Then, the expected data analysis effect cannot be achieved. Lossless compression ensures the integrity of the data, but its effect on reducing the amount of data transmitted is quite limited.

The bounded-error compression algorithms used in the IoT system are bounded-error Huffman coding (BEHC) [17] and bounded-error run length coding (BERLE) [17]. In the system offline first define the bounded-error according to the application, then use BEHC initial the codebook. The BEHC is based on the Huffman code (HC) [18]. Since each value with an error is regarded as a range, there is a greater chance that each data is regarded as the same data to improve the compression rate. After the codebook is generated, the bounded-error and codebook are sent down to the IoT device to execute bounded-error data compression.

As shown in Fig. 1, BERLE is based on the run length encoding (RLE) [19] compression theory in the process of IoT data transmission. By allowing a certain amount of error in advance, the range of overlap is taken from the allowable error range of each data. When the continuous data has an error, the range is considered to be the same when it has repetitions. This not only reduces the amount of data transmitted, but is also closer to real word applications.

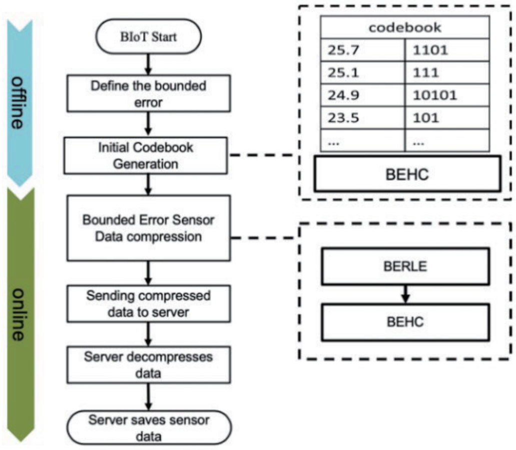


Fig. 1 Flowchart of bounded-error compression [20]

Then, bounded-error compression achieves the balance between compression rate and the data precision within the allowable error bound, not only reducing the data transmission, but also extending the sensor lifetime for IoT. Moreover, bound-error compression can be applied in online data query from IoT applications [21] to save more power for system lifetime than traditional online data query without bounded-error compression.

In this paper, the concept of bounded-error is not only used to extend IoT system lifetime, but also to protect the privacy of sensor data via smart contract. The blockchain smart contract provides data with different precision to protect the privacy of IoT data for different user access, according to the authority and payment of users from the third party, within the given bounded-errors.

Proposed BIoT System Architecture

As shown in Fig. 2, BIoT consists of three main components including the IoT devices, the Interplanetary File System (IPFS) [22] and blockchain smart contract.

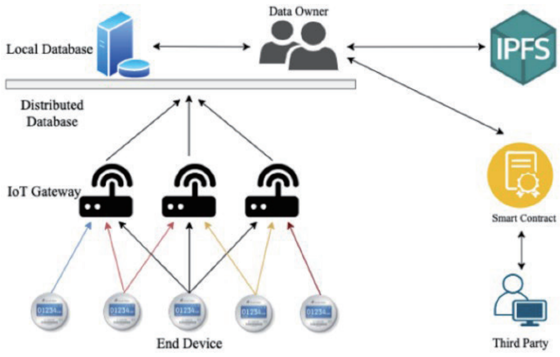


Fig. 2 Blockchain and bounded-error IoT system (BIoT)

A. IoT Device Component

In this paper, smart meter system [23] is considered as an example of end device to use LPWAN [24] as its system infrastructure. As shown in Fig. 2, LPWAN uses the star architecture where the system comprises two nodes, smart meter and IoT gateway. Gateway is responsible for collecting the sensor data of smart meter within the specific area and then sending data to the server through the Internet. In this paper, the data for compression is allocated for smart-meter for 30 minutes. We used our previous bounded-error compression scheme as shown in Fig. 1 to reduce the amount of actually transferred data, thereby reducing the amount of power consumed to extend the overall system's efficiency.

B. IPFS Component

Blockchain cryptocurrency is a decentralized ledger. Its decentralized, immutable and transparent features enable every participant to read the messages in the blockchain. In BIoT system when data owner wants to share or sale the IoT data, the data is processed to provide different users with different accuracies within the different bounded-errors according to the privacy of data owner. Therefore the data is encrypted and uploaded to IPFS. The IPFS generates a permanent hash value for BIoT system in subsequent query and reading. At this time, the data owner stores this hash value in the blockchain smart contract and gives a price or the list of allowed third party requesters according to the quality of the data. The applied smart contract in BIoT is introduced as follows.

C. Smart Contract Component

In the smart contract part of BIoT, we use the Solidity language [25] to write the blockchain contract, and use ganache [26] to simulate the deployment and execution of smart contracts on Ethereum. The smart contract includes the registration of IoT data, third-party request data, and authorization assignment functions. In the IoT data registration function, the contract allows the owner to give three different data accuracy levels: high, medium and low. The data owner stored the hash value of the data to share and trade IPFS into the smart contract and sets the price according to different accuracy levels. In addition, the data owner can also grant access to a third party through the BIoT authorization function. In the third-party requesting data function, the third party gives the public key and payment, and the smart contract is automatically completed the transaction according to its level of authorization and payment.

Experiments and Performance Results

The smart meter dataset on London city from Kaggle [27] was used to validate the proposed BIoT system. The dataset mainly contains the energy consumption measured from the smart meters every half hour in London housing. We used this dataset to prove that the proposed BIoT system can extend the lifetime of the IoT system for smart meter service with data privacy protection. We also used Etherscan [28] to demonstrate the query results of data transaction records between data owner and third party on the blockchain through the implemented smart contracts for privacy protection.

TABLE 1
FOUR TEST CASES FOR BOUNDED-ERROR ASSIGNMENT.

Cases	Bounded-error assignment
Case 1	January ~ December (all 0%)
Case 2	January ~ December (all 1%)
Case 3	Jan. ~ June (all 10%) & July ~Dec. (all 1%)
Case 4	January ~ November (all 10%) & December (1%)

We divide all smart meter dataset into 15 sections according to the total power consumption from all the smart meters through the year and select one dataset from each section for experiment. Regarding the power company's annual revenue settlement, we assumed that the last month (December) should preserve the least bounded-error for the highest revenue as possible. Thus, for setting the bounded-error values, we simply gave four different test cases (TABLE 1) to cost-effectively protect the smart meter data privacy and extend lifetime of the BIoT system. According to the experimental results shown in Fig. 3, while the allowable bounded-errors increases, Case 4 can save nearly 55% of the power consumption from Case1, and higher privacy protection can be achieved since the Case 4 has more significance in difference with original data.

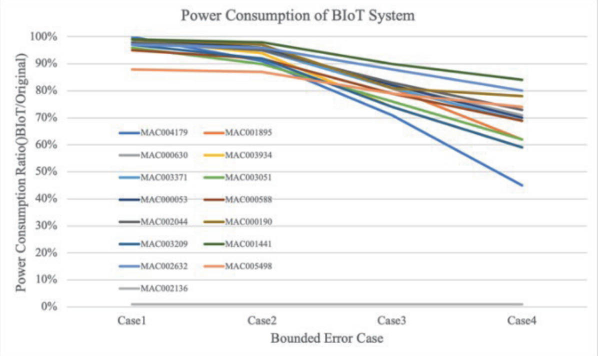
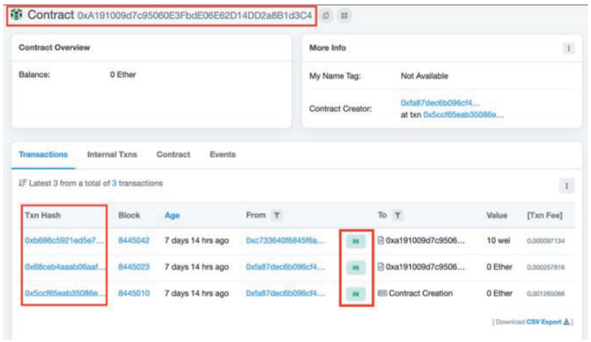


Fig. 3 Power consumption from 4 test cases of bounded-errors

Through the smart contract on the blockchain, the operations of both the data owner and the third party are recorded on the blockchain. Data owner can select one of bounded-errors given in Table 1 according to their allowable data accuracy to protect their own electricity privacy and extend the life of the system. When the data collection reaches a certain amount, the data can be sold on the blockchain. By setting the price and permissions of the data, it can give the data according to the amount and permissions set in the smart contract when a third party wants to request data. As shown in Fig. 4, both parties can interact with the smart contract deployed on the blockchain by the smart contract address in the top square box. Then, each

ISBN: 978-1-7281-9333-5

transaction of the smart contract can be queried from Etherscan, also reviewed whether the transaction is in-chain (IN) (successful transaction confirmed). Fig. 5 shows the transaction hash, block location, transaction completion time, transaction value, transaction fee and the wallet address of both parties to the transaction.



Contract 0xA191009d7c95060E3FbdE06E62D14DD2a8B1d3C4

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0xfa87dec6b096cf4...
at txn 0x5ccf65eab35086e...

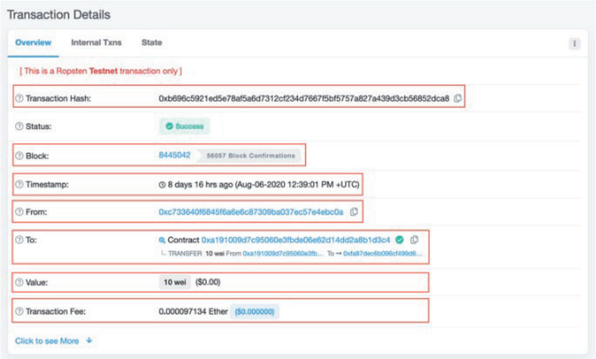
Transactions | Internal Txns | Contract | Events

Latest 3 from a total of 3 transactions

Txn Hash	Block	Age	From		To	Value	[Txn Fee]
0xb696c5921ed5e7...	8445042	7 days 14 hrs ago	0xc733640f6845f6a...	IN	0xa191009d7c9506...	10 wei	0.000097134
0x68ceb4aaab06aaf...	8445023	7 days 14 hrs ago	0xfa87dec6b096cf4...	IN	0xa191009d7c9506...	0 Ether	0.000257816
0x5ccf65eab35086e...	8445010	7 days 14 hrs ago	0xfa87dec6b096cf4...	IN	Contract Creation	0 Ether	0.001265066

[Download CSV Export]

Fig. 4 Smart contract on Etherscan



Transaction Details

Overview | Internal Txns | State

[This is a Ropsten Testnet transaction only]

Transaction Hash: 0xb696c5921ed5e78af5a6d7312cf234d7667f5bf5757a827a439d3cb56852dca8

Status: Success

Block: 8445042 56057 Block Confirmations

Timestamp: 8 days 16 hrs ago (Aug-06-2020 12:39:01 PM +UTC)

From: 0xc733640f6845f6a6e6c87309ba037ec57e4ebc0a

To: Contract 0xa191009d7c95060e3fbde06e62d14dd2a8b1d3c4
└ TRANSFER 10 wei From 0xa191009d7c95060e3fb... To → 0xfa87dec6b096cf499d6...

Value: 10 wei ($0.00)

Transaction Fee: 0.000097134 Ether ($0.000000)

Click to see More

Fig. 5 Detailed information of transaction

Conclusion

In this paper, we propose a novel bounded-error IoT system with data protection using blockchain smart contract. The proposed BIoT system not only extends the lifetime of IoT systems, but also provides different levels service quality in privacy protection for third parties according to the agreement of the rights and payment in smart contract.

Acknowledgement

This paper is partially supported by MOST Taiwan with grants 109-3116-F-002-002-CC1 and 108-2410-H-002-230-MY2.

References

[1] Chu, Yu-Hsien, et al. "UPHSM: Ubiquitous personal health surveillance and management system via WSN agent on open source smartphone," 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services. IEEE, 2011.

[2] Tao, Fei, et al. "Data-driven smart manufacturing," *Journal of Manufacturing Systems* 48 (2018): 157-169.

[3] Rathore, M. Mazhar, et al. "Efficient graph-oriented smart transportation using internet of things generated big data," 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE, 2015.

[4] C.R. Chu and Y.F. Chang. "Long-Term Surface Wind Speed Trends over Taiwan between 1961-2008," Department of Civil Engineering, National Central University.

[5] "Standard Method for Temperature Measurement," ed: ASHRAE, 2013.

[6] Chang, Ray-I., et al. "Bounded error data compression and aggregation in wireless sensor networks," Smart Sensors Networks. Academic Press, 2017. 143-157.

[7] Zheng, Zibin, et al. "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems 105 (2020): 475-491.

[8] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper 151.2014 (2014): 1-32.

[9] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems 82 (2018): 395-411.

[10] Y. Liang and W. Peng, "Minimizing energy consumptions in wireless sensor networks via two-modal transmission," ACM SIGCOMM Computer Communication Review, vol. 40, pp. 12-18, 2010.

[11] J. M. Rabaey, M. J. Ammer, J. L. da Silva, D. Patel, and S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking," Computer, vol. 33, pp. 42- 48, 2000.

[12] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[13] Park, Ji-Sun, et al. "Smart contract-based review system for an IoT data marketplace," *Sensors 18.10*(2018), 3577.

[14] Ozyilmaz, Kazim Rifat, and Arda Yurdakul. "Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks," IEEE Consumer Electronics Magazine 8.2 (2019): 28-34.

[15] L. Meng-Han, et al., " Error-bounded data compression using data, temporal and spatial correlations in wireless sensor networks," In 2010 International Conference on Multimedia Information Networking and Security (pp. 111-115). IEEE.

[16] C. Yu-Hao, et al., "Dynamic bounded-error data compression and aggregation in wireless sensor network," in Sensors, 2012 IEEE, 2012, pp. 1-4.

[17] L. Che-Lung, et al., "Concept of bounded error to improve wireless sensor network data compression," in SENSORS, 2014 IEEE, 2014, pp. 1240-1243.

[18] Sharma, Mamta. "Compression using Huffman coding," IJCSNS International Journal of Computer Science and Network Security 10.5 (2010): 133-141.

[19] Hauck, Edward L. "Data compression using run length encoding and statistical encoding," U.S. Patent No. 4,626,829. 2 Dec. 1986.

[20] Chang, Ray-I., et al. "Bounded-Error-Pruned Sensor Data Compression for Energy-Efficient IoT of Environmental Intelligence," Applied Sciences 10.18 (2020): 6512.

[21] J. Tsai, et al., "Distributed data query with dynamic bounded-error in wireless sensor networks," SENSORS, 2014 IEEE, Valencia, 2014, pp. 2008-2011.

[22] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561 (2014).

[23] Andreadou, Nikoleta, Miguel Olariaga Guardiola, and Gianluca Fulli. "Telecommunication technologies for smart grid projects with focus on smart metering applications," *Energies* 9.5 (2016): 375.

[24] Song, Yonghua, et al. "An Internet of energy things based on wireless LPWAN," *Engineering* 3.4 (2017): 460-466.

[25] Solidity language (https://solidity.readthedocs.io/en/v0.7.0/)

[26] Ganache (https://www.trufflesuite.com/ganache)

[27] Smart meters in London (https://www.kaggle.com/jeanmidev/smart-meters-in-london)

[28] Etherscan (https://etherscan.io/)