ZT-BDS: A Secure Blockchain-based Zero-trust Data Storage Scheme in 6G Edge IoT

Chenchen Han[1], Gwang-Jun Kim[2*], Osama Alfarraj[3], Amr Tolba[3], Yongjun Ren[4]

[1] School of Computer Science and Mathematics, Fujian University of Technology, China
[2] Department of Computer Engineering, Chonnam National University, South Korea
[3] Department of Computer Science, Community College, King Saud University, Saudi Arabia
[4] School of Computer and Software, Nanjing University of Information Science & Technology, China
18036803672@163.com, kgj@chonnam.ac.kr, oalfarraj@ksu.edu.sa, atolba@ksu.edu.sa, renyj100@126.com

Abstract

With the rapid development of 6G communication technology, data security of the Internet of Things (IoT) has become a key challenge. This paper first analyzes the security issues and risks of IoT data storage in 6G, and then constructs a blockchain-based zero-trust data storage scheme (ZT-BDS) in 6G edge IoT to ensure data security. Under this framework, an improved scratch-off puzzle based on Proof of Recoverability (PoR) is firstly constructed to realize distributed IoT data storage, which can reduce resource consumption compared with other existing schemes. Secondly, the accumulator is used to replace the Merkle trees to store IoT data in the blockchain. Since the accumulator can provide not only membership proof, but also non-membership proof, the proposed blockchain-based data storage scheme is more secure. Thirdly, PoW is replaced by an improved PoR scheme as the consensus protocol. On the one hand, PoR can verify the integrity of data, which will further enhance the security of IoT data; on the other hand, the proposed PoR is composed of polynomial commitment, which can reduce bandwidth with the aid of the aggregation function of polynomial commitment. Experimental comparisons show that our scheme has better bandwidth and storage capacity.

Keywords: Blockchain, Zero-trust, 6G edge network, Polynomial commitment, Proof of recoverability

1 Introduction

With the integration of the IoT and 5G, IoT devices have improved in terms of throughput and network transmission delay [1]. Today 5G is gradually being commercialized, and a new generation of communication technology is developing towards 6G based on Beyond 5G (B5G) [2]. However, the advancement of communication technology will inevitably bring about an explosive growth of data, and bring challenges to data security and management. The data throughput required by the 6G network will be 100 times that of 5G, and the number of access points for edge devices will reach the order of hundreds of millions, which places high standard on data storage security [3].

The data storage scheme constructed by the blockchain can improve the security and reliability of IoT data storage [4-5]. The blockchain can be viewed as a large, distributed ledger where all transactions need to be completed by all nodes in the network, and the nodes work together to monitor the legitimacy of the transactions. The open management of blockchain is also convenient for its daily maintenance. The traditional PoW algorithm in the blockchain is gradually abandoned because of its high overhead. As a potential replacement, PoR has been used to construct new blockchain storage scheme [6-7]. But in their scheme, storage overhead and communication bandwidth are still relatively high. In addition, some of the existing solutions are not suitable for large-scale application scenarios. Ren et al. [8-12] had proposed to construct a blockchain-based data storage scheme in multiple cloud environment, mainly applied in smart homes, but without considering larger scale application scenarios. To avoid above situation, we have made improvements in the consensus algorithm and storage mechanism in this paper. The contributions of this paper are as follows:

(1) This paper first analyzes the IoT data security and risks in 6G, and then proposes to build a zero-trust data storage scheme (ZT-BDS) by using blockchain.

(2) The unbounded dynamic accumulator is used to replace Merkle tree to store IoT data of blockchain. Due to the accumulator can provide not only membership proof but also non-membership proof, the proposed data storage scheme is more secure.

(3) To address the problem of inefficiency and unsuitability of PoW for storing data, this paper proposes to replace PoW with PoR. PoR can verify data integrity and further improve data security. Our PoR is constructed by polynomial commitment.

(4) This paper analyzes and compares the blockchain-based zero-trust storage scheme with the previous schemes. The experimental results show that the scheme in this paper has better bandwidth and excellent storage performance.

The rest of this paper is structured as follows. The section 2 analyzes the storage security issues and risks in 6G edge IoT and then introduces the related work of the ZT-BDS. In the section 3, we give the specific framework of our ZT-BDS and the concepts of polynomial commitment and PoR. Storage schemes are compared and analyzed in Section 4. Finally, we conclude in section 5.

*Corresponding Author: Gwang-Jun Kim; E-mail: kgj@chonnam.ac.kr
DOI: 10.53106/160792642022032302009

2 Related Work

2.1 Data Security and Risk in 6G Edge IoT

The improvement of communication technology has brought about explosive growth of data, and the security and risks of IoT data are also increasing [13-14]. IoT data security in 6G edge network can be summarized as follows:

(1) Data Heterogeneity. IoT data may come from different systems, networks and devices. Devices may have high latency and different versions, which will cause heterogeneity problems. There are also efficiency and security issues in cross-device operations.

(2) Data Integrity. The integrity of IoT data is to guarantee that sensor data has not been tampered with or forged. IoT data can be maliciously attacked in production, transmission and storage.

(3) Data Availability. The availability of IoT data means that users can obtain data anytime and anywhere. If data cannot be obtained in time, users will not be able to analyze the data.

2.2 6G Edge Network

Edge computing is a distributed computing architecture that transforms large-scale services that were originally processed entirely by central nodes into decentralized edge nodes [15-16]. Distributed settings bring many beneficial features to edge computing, such as low latency and mobility. These characteristics make it suitable for delay-sensitive application scenarios [17-18]. 6G is the abbreviation for sixth-generation communication technology. Although 6G is still in its infancy and there is no formal definition, researchers are already discussing some of its characteristics that distinguish it from 5G. These discussions centered on whether 6G is necessary to conduct some forward-looking research on 6G [19-20]. We call the edge network that uses 6G to communicate as the 6G edge network [21-28].

3 Our Proposed ZT-BDS Scheme

3.1 The Blockchain-based Zero-trust Data Security Storage Framework

Figure 1 is the framework of our proposed four-layer data storage scheme for 6G edge IoT, which is described in detail as follows. Our scheme refers to the framework of edge network.

Perception layer. The perception layer includes sensors of various IoT devices. One of the best examples is our mobile phone, which can have many built-in sensors, such as position sensors, attitude sensors, and even temperature sensors. Similar to other schemes, the main purpose of the perception layer is to collect data. These sensors upload the collected IoT data to edge devices in real time via the 6G wireless communication.

Edge layer. The edge layer is composed of various IoT edge devices. Each device can be regarded as a node, and they form an edge network. Edge devices can provide computing power and storage space on the side close to the data source. In other words, each device can provide computing power for the entire edge network. They work together to use 6G wireless communication to upload the final data to the blockchain. However, each node can also build a local private chain to store local sensitive data.

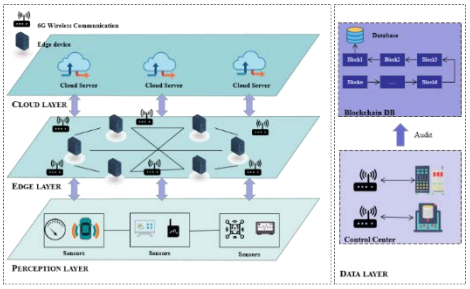


Figure 1. Framework of our proposed Blockchain-based Zero-trust data storage scheme in 6G edge network

Table 1. Notations

Symbol	Description
ID_p	Puzzle ID of each epoch.
$id \parallel i$	An explicit string combination of a λ-bit string id
$Seed$	Pseudo-random number family key
$\oplus/\otimes$	Addition /multiplication on group G.
$\boxplus/\boxtimes$	Addition /multiplication on Z_q.
$\odot$	Exponentiation operations on group G
PRF	Pseudo-random functions.
n	The number of encoded blocks.
s	The number of elements of each block.
l	The number of blocks used to verify.
n'	The total number of segments.
Ξ	The number of segments users stored.
λ	Secure parameter.
E	The size of each segments.

Cloud layer. The cloud layer consists of cloud servers, which provide services for edge devices. Generally, there is more than one cloud server that provides services for edge devices. The advantage of using multiple cloud service providers is to avoid the problem that data cannot be recovered after one of the cloud service providers has a problem. Benefiting from the characteristics of edge computing, our scheme no longer relies too much on cloud computing, which improves the security of data and the efficiency of data transmission.

Data layer. In our framework, the data layer includes a data center and a control center. The data center is composed of a blockchain database (BlockDB for short), which is used to store IoT data. Here, an accumulator is used to replace Merkle tree to form a new blockchain database. The responsibility of the control center is to manage edge devices, analyze, and audit data on the chain. Here we can also delegate some permissions to temporary managers. However, the communication between the control center and the edge device also uses 6g network.

Before introducing the specific scheme, Table 1 explains the symbols to be used below.

3 Proposed Proof of Recoverability Based on Polynomial Commitment

3.2.1 The Proposed Polynomial Commitment

The first polynomial commitment scheme was proposed by Kate [29]. It was subsequently extended to the vector commitment scheme. The introduction of each algorithm and other definitions are described in the reference [29-30]. We added the update algorithm to the original scheme. Here is our scheme:

- Generate $(1^k, g, \mu)$: We denote the generation of bilinear groups by $\mathcal{G} = \langle e, G, G_T \rangle$. An element g is randomly chosen from the group G. μ is the private key and is not used in the following algorithm The algorithm also generates a set of $\langle g, g^{\mu}, \ldots, g^{\mu^n} \rangle$ and $PK = \langle \mathcal{G}, g, g^{\mu}, g^{\mu^2} \ldots, g^{\mu^n} \rangle$. The private key
- Commit (PK,$F(x)$): Enter the PK and compute the polynomial $F(x) \in Z_P$ with the commitment $\mathcal{C} = g^{F(\mu)} \in G$. The algorithm will output the commitment:

$$\mathcal{C} = \prod_{j=0}^{deg(F)} \left(g^{\mu^j}\right)^{F_j}. \quad \textbf{(1)}$$

- Open ($PK, C, F(x)$): Output thepolynomial $F(x)$.
- VerPoly (PK,$\mathcal{C}$, $F(x)$): Verify $\mathcal{C} = g^{F(\mu)}$ is valid. If for $F(\mathrm{x}) = \sum_{j=0}^{\deg(F)} F_j x^j$, there is $\mathcal{C} = \prod_{j=0}^{\deg(F)} (g^{\mu^j})^{F_j}$, output 1. Otherwise, output 0. Works if and only if $deg\ (F) \leq t$.
- Creatwit ($PK, \mathcal{C}, F(x)$): Input PK, index i, and check whether $i \in I$, otherwise output 0. Compute:

$$f_i(x) = \frac{F(x)-F(i)}{x-i} \in Z_p. \quad \textbf{(2)}$$

and output $\langle i, F(i), \omega_i \rangle$, where $\omega_i = g^{f_i(\mu)}$. The ω_i generated by this algorithm constitutes the set $W = \{\omega_1, \omega_2, \ldots, \omega_t\}$.

- VerEval ($PK, i, F(i), \omega_i$): Verify that $F(i)$ is a summation of the polynomial in index i committed by $\mathcal{C}$. Check if $i \in I$, otherwise the algorithm terminates. If the equation $e(\mathcal{C}, g) = e(\omega_i, g^{\mu}/g^i) e(g, g)^{F(i)}$ holds, output 1. Otherwise, output 0.
- Update ($PK, \frac{i^+}{i^-}, W$, I): The algorithm consists of two operations: *Add*: Enter the PK, the index set I, the witness set W and the index to be added i^+. Check if $i^+ \in I$, otherwise output 1. Calculate:

$$f_{i^+}(x) = \frac{F(x)-F(i^+)}{x-i^+} \in Z_p, \quad \textbf{(3)}$$

where $\omega_{i^+} = g^{f_{i^+}(\mu)}$. The new witness ω_{i^+} is then updated into W by updating the index set $\mathrm{I} \cup \{i^+\}$. *Delete*: The steps of Delete algorithm are similar to the Add algorithm. Enter the PK, the index set I, the witness set W and the index to be added i^-. Check if $i^- \in I$, otherwise output 0. Update the new index set $\mathrm{I}/\{i^-\}$ and remove the corresponding witness in W.

Correctness. The above scheme is correct because the following equation is true. The left and right hand can be deduced to be equal to $e(g, g)^{F(u)}$.

$$(\omega_i, g^{\mu}/g^i) e(g, g)^{F(i)} = e(g^{f_i(\mu)}, g^{(\mu-i)}) e(g, g)^{F(i)} \quad \textbf{(4)}$$

Theorem 4.1 *As long as the DL and t-SDH assumption holds in $\mathcal{G}$, the polynomial commitment scheme is a secure scheme.*

Proof. **Polynomial binding**. Suppose there are two polynomials $\mathrm{Z}_1(x), \mathrm{Z}_2(x)$ (which can be accepted by *VerPoly* algorithm) that an adversary $\mathcal{A}$ can use to break the polynomial binding property. We construct an algorithm $\mathcal{E}$ to cause $\mathcal{A}$ to compute the private key $SK = \mu$. For $\mathrm{Z}_1(x)$ and $\mathrm{Z}_2(x)$ generated by $\mathcal{A}$, $\mathcal{C} = g^{\mathrm{Z}_1(\mu)} = g^{\mathrm{Z}_2(\mu)}$.

For a polynomial $\mathrm{Z}_3(\mu) = \mathrm{Z}_1(\mu) - \mathrm{Z}_2(\mu) \in Z_P$, the corresponding commitment:

$$\mathcal{C}_{\mathrm{Z}_3(\mu)} = g^{\mathrm{Z}_3(\mu)} = \frac{g^{Z_1(\mu)}}{g^{\mathrm{Z}_2(\mu)}} = 1. \quad \textbf{(5)}$$

Therefore $\mathrm{Z}_3(\mu) = 0$. The factorial decomposition of $\mathrm{Z}_3(\mu)$ shows that μ is the root of the polynomial $\mathrm{Z}_3(\mu)$, and $\mathcal{E}$ can easily find $SK = \mu$ and solve the example of the n-SDH problem given by the system parameters.

Evaluation binding. Suppose there are two witnesses $\langle i, \mathrm{Z}(i), \tau_i \rangle$, $\langle i, \mathrm{Z}^*(i), \tau_i^* \rangle$ that can be computed by an adversary $\mathcal{A}$. We showed how to use $\mathcal{A}$ to construct an algorithm $\mathcal{E}$ that breaks the n-SDH hypothesis.

Algorithm $\mathcal{E}$ will generate an instance of n - SDH problem $\langle \mathcal{G}, g, g^{\mu}, g^{\mu^2}, \ldots, g^{\mu^n} \rangle$ as a public key to the $\mathcal{A}$. Adversary output: $\mathcal{C}$, $\langle i, \mathrm{Z}(i), \tau_i \rangle$, $\langle i, \mathrm{Z}^*(i), \tau_i^* \rangle$.We have

$$e(\tau_i, g^{\mu-i}) = e(\tau_i^*, g^{\mu-i}). \quad \textbf{(6)}$$

For $f_i = \log_g \tau_i, f_i^* = \log_g \tau_i^*$, we have

$$f_i(u-i) + Z = f_i^*(u-i) + Z^*. \quad \textbf{(7)}$$

As well as $\frac{f_i - f_i^*}{Z_i^*(i) - Z(i)} = \frac{1}{\mu - i}$. Algorithm $\mathcal{E}$ computes:

$$\left(\frac{\tau_i}{\tau_i^*}\right)^{\frac{1}{Z_i^*(i)-Z(i)}} = g^{\frac{f_i - f_i^*}{Z_i^*(i)-Z(i)}} = g^{\frac{1}{\mu-i}}, \quad \textbf{(8)}$$

and returns a $\langle -i, g^{1/(\mu-i)} \rangle$ as a solution to the problem instance n-SDH. From the above, the probability of success in solving the instance is the same as the probability of success for adversary.

Hiding. Suppose there exists an adversary $\mathcal{A}$ that can correctly compute the polynomial $Z(x)$ given t valid witness tuple $\langle i, \mathrm{Z}(i), \tau_i \rangle$. In other words, the adversary can destroy the hiding properties of the commitment. The following shows how to use $\mathcal{A}$ to construct an algorithm $\mathcal{E}$ to break the DL assumption.

Firstly, let $\langle g, g^{\nu} \rangle$ be an instance of the DL problem that $\mathcal{E}$ needs to solve. $\mathcal{E}$ randomly selects a number ν. This random number can be used to generate a public key $PK = \langle \mathcal{G}, g, g^{\nu}, g^{\nu^2}, \ldots, g^{\nu^n} \rangle$. Algorithm $\mathcal{E}$ sets $\langle r, F(r) \rangle$ as the evaluation of the polynomial $Z(x)$ at the index r. Then suppose $Z(0) = r$, and this is the answer to DL instance. Calculation of $g^{\mathrm{Z}(x)}$ using $n+1$ exponential evaluation: $\langle 0, g^{\nu} \rangle$ and $\langle r, g^{\mathrm{Z}(r)} \rangle$. Finally, $\mathcal{E}$ calculated $\tau_r = (g^{\mathrm{Z}(\nu)}/g^{\mathrm{Z}(r)})^{1/(\nu-r)}$ and send the PK and t-witness tuple $\langle r, \mathrm{Z}(\mathrm{r}), \tau_r \rangle$ to the adversary $\mathcal{A}$. Once the adversary returns the polynomial, $\mathcal{E}$ returns the constant term $Z(0)$ as the solution to the DL instance. Based on the above proof, the

probability of success for solving the DL instance is the same as the probability of success for adversary $\mathcal{A}$.

3.2.2 The Proposed Proof of Recoverability

PoR is an interactive proof of knowledge technology used to remotely audit the integrity of files stored in the cloud without having to keep a copy of the original file in local storage [31-32]. Below we briefly describe our proposed PoR. Denote a polynomial by $f_{\vec{m}(x)}$, which has a vector of coefficients of $\vec{m} = (m_0, \dots, m_{s-1})$. We have $f_{\vec{m}(x)} = \sum_{j=0}^{s-1} m_j x^j$. $\vec{w}$ represents the coefficient vector of the polynomial $\vec{w} = (w_0, \dots, w_{s-2})$. The private key consists of seed, the prime p, and two random elements α, τ, which can be expressed as $(p, seed, \alpha, \tau)$.

PoR requires the use of coding techniques (e.g. Reed-Solomon code). Given a private key and a data file $\mathcal{M}$, the coding algorithm can generate blocks of data $(\vec{m}_0, \dots, \vec{m}_{n-1})$. Each block $\vec{m}_i$ is a vector of group elements $m_{i,j} = (m_{i,0}, \dots, m_{i,s-1})$. The error erasure decoding can be used to recover the original data file $\mathcal{M}$ from any ρn number of blocks. Then we select a unique identifier id from the domain $\{0.1\}^{\gamma}$ and finally to the encoded file $\widetilde{\mathcal{M}}$, which can be expressed as $\{(i, \vec{m}_i, t_i): 0 \le i \le n-1\}$, where t_i is the authentication label:

$$t_i = PRF_{seed}(id \parallel i) + \tau f_{\vec{m}(\alpha)}. \quad \textbf{(9)}$$

At the proof stage, we use the identifier id, the code file $\widetilde{\mathcal{M}}$ and the challenge query $\mathcal{QC}$ to generate the proof ϖ:

$$\varpi = \prod_{j=0}^{s-2} \left(g^{\alpha^j}\right)^{\omega_j} = g^{f_{\vec{w}}(\alpha) mod\ q}. \quad \textbf{(10)}$$

Based on the algebraic properties of polynomial, we have $f_{\vec{w}}(x) = (f_{\vec{u}}(x) - f_{\vec{u}}(r))/(x - r)$, where $y = f_{\vec{u}}(r)$ is the evaluation of the polynomial $f_{\vec{u}}(x)$ at the point $x = r$, and r is a random number chosen by the data owner. $\vec{u} := (u_0, \dots, u_{s-1})$. The proof stage will output a ternary (y, ϖ, σ).

Finally, the verification algorithm outputs either an accept or a reject. However, the pseudo-random function can be used to achieve private verification, while the BLS signature can be used to achieve public verification. In the public verification scheme, the tag will be accompanied by a signature generated with a private key. The authentication label is represented as $t_i = \left(\mu^{id \| i} g^{f_{\vec{m}(\alpha)}}\right)$.

4 Comparison and Analysis

4.1 PoR Mechanism

According to Section 3.3.2, the communication overhead of our scheme is the size of the proof (the size of the ternary (y, ϖ, σ)). The storage overhead of the cloud server side is 1/s of the size of the data file, and s is the size of each file block. In addition to storing the data file, the cloud side has a public key of size (s+1)λ. In our scheme, only one public key is needed per user. The key generation algorithm in PoR requires s-group operations. Suppose a coded file with n blocks of size $ns\lambda$ bits, buy a block with s group elements, and each group element of size λ bits. Preprocessing the data requires addition and multiplication operations on ns groups, and n PRF to evaluate the value.

In Table 2, we compared the performance of our PoR with other scheme [33-36]. We compare the communication and storage overheads of the SW scheme and our PoR scheme in Figure 2. Our schemes are all built on elliptic curves and assume that the total file size is 1G. The communication bandwidth per verification for the PoR scheme in this paper remains constant as the storage overhead increases, while the communication bits decrease for the SW scheme as the storage overhead increases.

Table 2. Comparison of consensus algorithms

Scheme	Communication（challenge）	Communication（response）	Storage	Data pre-processing
SW [33]	$\mathcal{O}$（1）	$\mathcal{O}$（λ）	$(1+\frac{1}{s})\|F\|$	$sn\otimes + (s+2)n \odot$
DV [34]	$\mathcal{O}$（1）	$\mathcal{O}$（λ）	$(1+\frac{1}{s})\|F\|$	$lPRF + n(2 \boxtimes +2 \boxplus)$
XC [35]	$\mathcal{O}$（1）	$\mathcal{O}$（1）	$(1+\frac{1}{s})\|F\|$	$lPRF + n(2 \boxtimes +2 \boxplus)$
YY [36]	$\mathcal{O}$（1）	$\mathcal{O}$（1）	$(1+\frac{1}{s})\|F\|$	$sn\otimes + (s+2)n \odot$
This Paper	$\mathcal{O}$（1）	$\mathcal{O}$（λ）	$\|F\|/s$	$\|F\|/\lambda(\oplus + \otimes) + \|F\|/\lambda sPRF$

Table 3. Comparison of consensus algorithms

	Permacoin	Retricoin	This paper
Ticket	$(PK, \{F[r_i], \beta_i, \pi_{r_i}\}_{0 \le i < k})$	$(pk, s_0, s_1, l, \sigma, \mu, \{h_i\}_{0 \le i \le k})$	$\left(s, \mu, \Delta[r_i], \sigma_i, \psi_{r_i}\right)$
Storage Overhead（bits）	$256\lceil lgn' \rceil$	256	464
Bandwidth（bits）	$256 + \lambda + k(E + r + 256\lceil lgn' \rceil)$	$256 + 4\lambda + E + \lceil lg\Xi \rceil + kr$	3kλ + λ+440

4.2 Storage Comparison

In this section, we compare the overhead of local data storage and the bandwidth for sending tickets between our scheme and the other two scheme [6-7]. Here we assume that all of our pairwise operations are done under an elliptic curve over a prime field, we make the parameter satisfy λ=128. In this setting, the size of segment, tag, p, signature, and μ are all 2λ bits. The size of the random string s_0, s_1 is λ bits. The

challenge set satisfies $|QC|=k=\lambda$. r is the size of the signature, about 896 bits. Since we generally assume that the cloud has nearly infinite computing power, we will only compare the user's local overhead in this section, and not the cloud server's overhead.

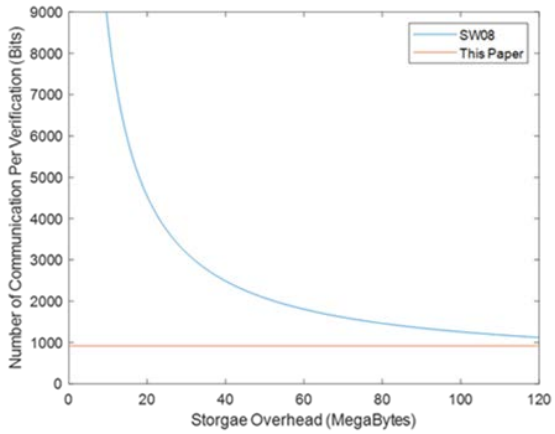


Figure 2. Comparison of PoR mechanism

4.2.1 Local Storage Comparison

The storage analysis of Permacoin and Retricoin is given in their paper, and we list it in Table 3. Suppose the user stores l file segments in the network. In our ZT-BDS, the data is outsourced to multiple cloud providers, and the user only stores the private key locally, which has a size of 3λ+80bits. According to the above setting, the size of the private key is 464 bits, which is fixed. The public key is also stored in the cloud. After comparison, the storage overhead of our scheme and Retricoin is constant as the number of data segment increases, while Permacoin scheme becomes larger as the data segment increases.

4.2.2 Bandwidth Comparison

In ZT-BDS, the node comes with a ticket as his stored proof. We use k to denote the base of the challenge set QC. The ticket is of the form $(s, \mu, \Delta[r_i], \sigma_i, \psi_{r_i})$. The public key is stored in the cloud server and does not need to be stored in the ticket. The size of the proof and signature is 3λ bits, and the size of the ticktet is $3k\lambda + 4\lambda + 440$bits according to the parameters set above.

The size of their tickets can be seen in Table 3. After the file is preprocessed, the processed file is split into blocks. Each block is usually divided into d sectors [37-38]. We have $n' = \left\lceil \frac{n}{d} \right\rceil$, $\Xi' = \left\lceil \frac{\Xi}{d} \right\rceil$, where n represents the total number of segments. Suppose $E = 2d\lambda$ bits. The communication bandwidth size of the two schemes is shown in Table 3.

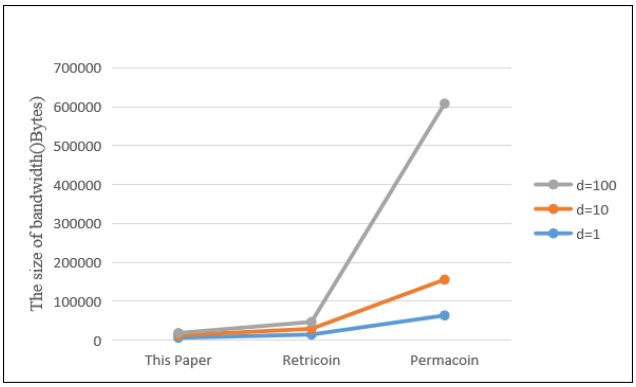


Figure 3. Bandwidth comparison

Assume that the total file F size is 1024GB and the node storage is 4GB. Figure 3 shows the comparison of the bandwidth sizes of the three schemes when $d = 1, d = 10$ and when $d = 100$. Upon comparison, our scheme is superior to the other two schemes.

5 Conclusion

Actively dealing with the rapid growth of IoT data security is an important challenge in the future 6G era. This paper proposes to use the PoR scheme based on updatable polynomial commitment instead of PoW to construct a ZT-BDS on the 6G edge of IoT to collect and store data. An improved scheme was constructed to implement distributed storage. The proposed PoR is used as a consensus algorithm in our scheme. Then the dynamic accumulator is used to store data instead of the Merkle tree. Experimental results show that our ZT-BDS has better storage and bandwidth capabilities. Future work will focus on privacy protection.

Acknowledgements

This work was supported by the National Natural Science Foundation of China [No. 62072249, 61772280]. This work was funded by the Researchers Supporting Project No. (RSP-2021/102) King Saud University, Riyadh, Saudi Arabia.

References

[1] J. Wang, C. Jin, Q. Tang, N. N. Xiong, G. Srivastava, Intelligent Ubiquitous Network Accessibility for Wireless-Powered MEC in UAV-Assisted B5G, *IEEE Transactions on Network Science and Engineering*, Vol. 8, No. 4, pp. 2801-2813, October-December, 2021.

[2] J. Wang, H. Han, H. Li, S. He, P. K. Sharma, L. Chen, Multiple Strategies Differential Privacy on Sparse Tensor Factorization for Network Traffic Analysis in 5G, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 3, pp. 1939-1948, March, 2022.

[3] P. Yang, Y. Xiao, M. Xiao, S. Li, 6G wireless communications: Vision and potential techniques, *IEEE Network*, Vol. 33, No. 4, pp. 70-75, July/ August, 2019.

[4] Y. Ren, Y. Leng, Y. 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.

[5] S. Sun, R. Du, S. Chen, W. Li, Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain, *IEEE Access*, Vol. 9, pp. 36868-36878, February, 2021.

[6] A. Miller, A. Juels, E. Shi, B. Parno, J. Katz, Permacoin: Repurposing bitcoin work for data preservation, *35th IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2014, pp. 475-490.

[7] B. Sengupta, S. Bag, S. Ruj, K. Sakurai, Retricoin: Bitcoin based on compact proofs of retrievability, *Proceedings of the 17th International Conference on Distributed Computing and Networking*, Singapore, 2016, pp. 1-10.

[8] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang, Z. Almakhadmeh, A. Tolba, Multiple cloud storage mechanism based on blockchain in smart homes, *Future Generation Computer Systems*, Vol. 115, pp. 304-313, February, 2021.

[9] Y. Ren, J. Qi, Y. Liu, J. Wang, G. J. Kim, Integrity Verification Mechanism of Sensor Data Based on Bilinear Map Accumulator, *ACM Transactions on Internet Technology*, Vol. 21, No. 1, pp. 1-19, February, 2021.

[10] M. T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, *Computers & Security*, Vol. 78, pp. 126-142, September, 2018.

[11] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, M. A. Imran, Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment, *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 5791-5802, June, 2019.

[12] J. Wang, W. Chen, Y. Ren, O. Alfarraj, L. Wang, Blockchain Based Data Storage Mechanism in Cyber Physical System, *Journal of Internet Technology*, Vol. 21, No. 6, pp. 1681-1689, November, 2020.

[13] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, M. Zorzi, Toward 6G Networks: Use Cases and Technologies, *IEEE Communications Magazine*, Vol. 58, No. 3, pp. 55-61, March, 2020.

[14] N. Hassan, K. L. A. Yau, C. Wu, Edge computing in 5G: A review, *IEEE Access*, Vol. 7, pp. 127276-127289, August, 2019.

[15] B. Lorenzo, J. Garcia-Rois, X. Li, J. Gonzalez-Castano, Y. Fang, A Robust Dynamic Edge Network Architecture for the Internet of Things, *IEEE Network*, Vol. 32, No. 1, pp. 8-15, January-February, 2018.

[16] C. Ge, Z. Liu, J. Xia, L. Fang, Revocable identity-based Broadcast Proxy Re-encryption for Data Sharing in Clouds, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 3, pp. 1214-1226, May-June, 2021.

[17] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, V. Chang, A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment, *Journal of Medical Systems*, Vol. 42, No. 8, August, 2018.

[18] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, J. Zhang, Big data service architecture: A survey, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 393-405, March, 2020.

[19] W. Saad, M. Bennis, M. Chen, A vision of 6G wireless systems: Applications, trends, technologies, and open research problems, *IEEE network*, Vol. 34, No. 3, pp. 134-142, May/ June, 2020.

[20] Y. Ren, F. 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, Article No. 207, January, 2020.

[21] J. Wang, Y. Gao, C. Zhou, R. S. Sherratt, L. Wang, Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs, *CMC-Computers*, Materials & Continua, Vol. 62, No. 2, pp. 695-711, 2020.

[22] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, L. Fang, Secure Keyword Search and Data Sharing Mechanism for Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 6, pp. 2787-2800, November-December, 2021.

[23] J. Wang, Y. Zou, P. Lei, R. S. Sherratt, L. Wang, Research on recurrent neural network based crack opening prediction of concrete dam, *Journal of Internet Technology*, Vol. 21, No. 4, pp. 1161-1169, July, 2020.

[24] J. Wang, C. Han, X. Yu, Y. Ren, R. S. Sherratt, Distributed Secure Storage Scheme Based on Sharding Blockchain, *CMC-Computers, Materials & Continua*, Vol.70, No. 3, pp. 4485-4502, October, 2021.

[25] J. Hu, K. Li, C. Liu, K. Li, A Game-Based Price Bidding Algorithm for Multi-Attribute Cloud Resource Provision, *IEEE Transactions on Services Computing*, Vol. 14, No. 4, pp. 1111-1122, July-August, 2021.

[26] B. Embrey, The top three factors driving zero trust adoption, *Computer Fraud & Security*, Vol. 2020, No. 9, pp. 13-15, September, 2020.

[27] J. Wang, X. 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 Science*, Vol. 9, No. 1, Article No. 18, May, 2019.

[28] B. Pu, K. Li, S. Li, N. Zhu, Automatic Fetal Ultrasound Standard Plane Recognition Based on Deep Learning and IIoT, *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 11, pp. 7771-7780, November, 2021.

[29] A. Kate, G. M. Zaverucha, I. Goldberg, Constant-size commitments to polynomials and their applications, *International Conference on the Theory and Application of Cryptology and Information Security*, Singapore, Singapore, 2010, pp. 177-194.

[30] D. Boneh, B. Bünz, B. Fisch, Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains, *Annual International Cryptology Conference*, Santa Barbara, CA, USA, 2019, pp. 561-586.

[31] J. Xu, E. C. Chang, Towards efficient proofs of retrievability, *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, South Korea, 2012, pp. 79-80.

[32] Y. Ren, F. Zhu, J. Wang, P. K. Sharma, U. Ghosh, Novel vote scheme for decision-making feedback based on blockchain in internet of vehicles, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 2, pp. 1639-1648, February, 2022.

[33] H. Shacham, B. Waters, Compact proofs of retrievability, *International Conference on Theory and Application of Cryptology and Information Security*, Melbourne, Australia, 2008, pp. 90-107.

[34] A. M. Dunn, O. S. Hofmann, B. Waters, E. Witchel, Cloaking malware with the trusted platform module, *20th USENIX Security Symposium*, San Francisco, CA, USA, 2011, pp. 1-16.
[35] J. Xu, E. C. Chang, J. Zhou, Towards Efficient Provable Data Possession in Cloud Storage, 2011. Available: https://eprint.iacr.org/2011/574.pdf
[36] J. Yuan, S. Yu, Proofs of retrievability with public verifiability and constant communication cost in cloud, *2013 International Workshop on Security in Cloud Computing*, Hangzhou, China, 2013, pp. 19-26.
[37] V. Gramoli, From blockchain consensus back to Byzantine consensus, *Future Generation Computer Systems*, Vol. 107, pp. 760-769, June, 2020.
[38] C. Liu, K. Li, K. Li, R. Buyya, A New Service Mechanism for Profit Optimizations of a Cloud Provider and Its Users, *IEEE Transactions on Cloud Computing*, Vol. 9, No. 1, pp. 14-26, January-March, 2021.

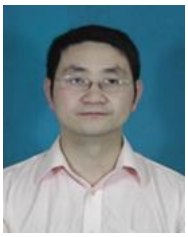
Biographies

Chenchen Han received his bachelor's degree from Taishan College of science and technology, Shandong University of science and technology, China, in 2019. He is currently working towards the master's degree with the School of computer science and Mathematics, Fujian University of technology. His research interests include applied cryptography and blockchain.

Gwang-Jun Kim received the B.E, M.E and Ph.D. degrees in computer engineering from Chosun University in 1993, 1995 and 2000, respectively. Now, he is a professor in computer engineering at Chonnam National University. His current research interests include the area sensor network, IoT, real-time communication and various kinds of communication systems.

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 with King Saudi University, Riyadh, Saudi Arabia. His current research interests include eSystems, cloud computing, and big data.

Amr Tolba received the M.Sc. and Ph.D. degrees from Menoufia University, Egypt, in 2002 and 2006, respectively. He is currently Professor of Computer Science at King Saud University (KSU), Saudi Arabia. His main research interests include socially aware networks, vehicular ad-hoc networks, IoT, intelligent systems, Big Data, recommender systems, and cloud computing.



Yongjun Ren received the M.S. degree from Hohai University, China, in 2004, and the Ph.D. degree from the Computer and Science Department, Nanjing University of Aeronautics and Astronautics, China, in 2008. He is currently serving as a full-time faculty with the Nanjing University of Information Science and Technology. His research interests include network security and applied cryptography.