SCIENCE CHINA
Information Sciences

• LETTER •

February 2024, Vol. 67, Iss. 2, 129102:1–129102:2
https://doi.org/10.1007/s11432-023-3828-7

A blockchain-based data auditing scheme with key-exposure resistance for IIoT

Pan YANG & Jingli REN*

Henan Academy of Big Data, Zhengzhou University, Zhengzhou 450052, *China*

Received 16 February 2023/Revised 25 June 2023/Accepted 6 July 2023/Published online 25 January 2024

The Industrial Internet of Things (IIoT) enables enterprises to collect data from end devices and outsource the data to cloud servers for flexible data sharing. Public auditing plays an important role in ensuring the integrity of the data. There are blockchain-based public auditing schemes that utilize smart contracts to achieve decentralized verification (such as [1]), but they are vulnerable to the key exposure attack. This means that most blockchain-based public auditing systems will become unreliable once the secret keys are exposed.

Key exposure occurs due to weak security awareness of data owners (DO) or other factors. For example, the key flow generation structure may be revealed because the attractor structure can be reconstructed from a low-dimensional time series [2]. There are protocols to make public auditing systems resist key exposure [3–5], but all of them rely on a specified third-party auditor (TPA) and cannot be directly extended to the decentralized protocols. The reasons are as follows: (1) the key exposure resistance is obtained by updating the key, which does not provide sufficient protection because key exposure is not always detected immediately by the DO; (2) some solutions enhance key exposure resistance by using the aggregation of the DO's private key and the TPA's private key, while there is no such TPA in the decentralized protocol (refer to [3, 4]). For the former, the key update provides forward security, i.e., the data-tag pairs are unforgeable after updating the secret key, but backward security is weak, i.e., the data-tag pairs are vulnerable until the key is updated. Although the preceding problem is handled in the latter case, the approach inevitably fails since the verifiers in a decentralized protocol are neither unique nor fixed.

In this study, we propose BAKER, a novel decentralized public auditing scheme with key exposure resistance. BAKER employs blockchain and smart contracts to provide efficient non-interactive public auditing, removing the need for trusted TPAs, providing forward and backward security against the key exposure attack, and supporting fair arbitration. Security and performance analyses indicate that BAKER is secure and efficient.

System model. There are five different entities in BAKER: IIoT, DO, cloud service provider (CSP), verifier, and blockchain (see Figure 1). Sensor-equipped IIoT devices collect enormous amounts of data and upload it to the CSP for long-term storage. The DO is an individual or organization with lots of IIoT devices. The CSP is a semi-trusted entity that provides storage services and generates integrity proof for hosted data, but it may conceal data corruption. The verifier is a blockchain peer who checks the proof by invoking the auditing chaincode in the blockchain network. We adopt the consortium blockchain in BAKER. There is a fully trusted management node (MN) on the blockchain that serves as a certificate authority while also arbitrating disputes during data auditing. Appendix B offers details on the BAKER workflow and deployment.

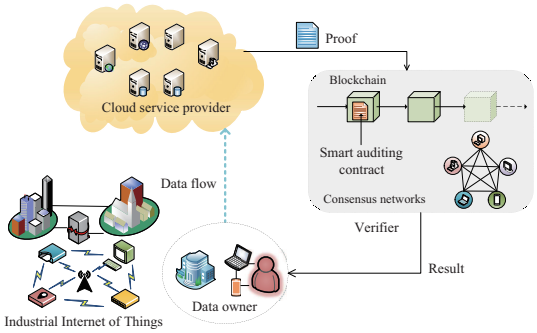

Figure 1 (Color online) System model.

BAKER design. The BAKER consists of six algorithms:

KeyGen. This algorithm is run by the DO with a security parameter κ as input to generate the private keys $x \in Z_p^*$, $\beta \in Z_p^*$ of the DO and the MN, respectively, the initial auditing secret key $\mathrm{SK} = H_1(t_0)^{\beta x}$, and public parameters $\mathrm{para} = (H_1, H_2, H_3, f, h, \mathcal{F}, g, u, g^{\beta}, R, \mathrm{spk})$.

TagGen. This algorithm is run by the DO. It takes as input the auditing secret key SK for the current time period t, the data block $m_{i,j}$, and the public parameters para and generates the authenticator $\sigma_i = (h_i \cdot u^{\sum_{j=1}^{s} \alpha_j m_{i,j}})^{\alpha} \cdot \mathrm{SK}$.

KeyUpdate. This algorithm is run by the DO and the MN. It takes the current time period t, the DO's private key x, the MN's private key β, and public parameters para as input and generates the auditing secret key $\widetilde{\mathrm{SK}}$.

AuthUpdate. This algorithm is run jointly by the DO and the CSP. The DO generates the authenticator update key auk and sends it to the CSP. The CSP generates the

* Corresponding author (email: renjl@zzu.edu.cn)

authenticator set $\widetilde{\Phi}$ for the current time period $t+1$ using the auk and the authenticator set Φ for the previous time period t.

ProofGen. This algorithm is run by the CSP. The CSP periodically traverses the auditing tasks of all DOs, and gets the public information τ. Then randomly select $c : 1 \leqslant c \leqslant n$ and $\eta_1, \ldots, \eta_s \in Z_p^*$ and generate the challenge $\{(s_i, v_i)\}_{i\in[1,c]}$. Compute $Q = \prod_{j=1}^{s} u_j^{\eta_j} \in G_1$, $\gamma = H_3(Q)$, $\mu_j = \eta_j + \gamma \sum_{i\in I} v_i \cdot m_{i,j}$ for $j = 1, \ldots, s$, and the aggregate authenticator $\sigma = \prod_{i\in I} \sigma_i^{v_i\gamma}$. Finally, the CSP submits a transaction proposal containing the proof $P = (\mathrm{FT}, \tau, c, Q, \mu = \{\mu_1, \ldots, \mu_s\}, \sigma)$ along with the auditing chaincode ID on the blockchain.

Verification. This algorithm is packaged into the auditing chaincode and run by verifiers. It takes as input the public parameters and the proof from the CSP and outputs the verification result as "True" or "False". "True" triggers a service fee transaction, at which point the CSP will receive the service fee due for this period from the DO, while "False" triggers a compensation transaction.

Furthermore, we design an arbitration mechanism to support fair transactions so that a framed CSP can apply for arbitration to the MN if a malicious DO tries to frame the CSP for compensation. Then submit a transaction proposal containing a new proof $P' = (\mathrm{FT}, \tau, c, \mu' = \{\mu'_1, \ldots, \mu'_s\}, \sigma)$ and the auditing chaincode ID on the blockchain. The MN announces the data are stored correctly if $e(g, \sigma') = e(v, \prod_{i\in I} h_i^{v'_i} \prod_{j=1}^{s} u_j^{\mu'_j}) \cdot e(R, H_1(t)^{\sum_{i\in I} v'_i})$ holds.

Details of the algorithms and arbitration can be found in Appendix C.

Security and performance. We formalize the security model and prove the correctness, soundness, key exposure resilience, privacy protection, and (ξ, θ) detectability of BAKER. Please refer to Appendix D for more details.

We analyze the communication and computational overhead of BAKER and simulate the time costs through on-chain and off-chain experiments, which indicate that BAKER is efficient and practical. Specific performance analyses and comparisons can be found in Appendix E.

Conclusion. We propose a non-interactive decentralized public auditing scheme for IIoT, BAKER, which eliminates the need for trusted TPAs while providing strong key exposure resistance. BAKER enables the DO to update the private key, auditing secret key, and authenticators without altering the public parameters. Furthermore, smart contracts and arbitration mechanisms ensure fairness. The security analysis demonstrates that BAKER has key exposure resistance, privacy preservation, and detectability. BAKER has nice performance advantages, according to theoretical and experiment results (off-chain and on-chain).

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 52071298) and Strategic Research and Consulting Project of Chinese Academy of Engineering (Grant No. 2022HENYB05).

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Wang H, Qin H, Zhao M H, et al. Blockchain-based fair payment smart contract for public cloud storage auditing. Inf Sci, 2020, 519: 348–362
2 Guo X X, Han W M, Ren J L. Design of a prediction system based on the dynamical feed-forward neural network. Sci China Inf Sci, 2022, 66: 112102
3 Yu J, Wang H Q. Strong key-exposure resilient auditing for secure cloud storage. IEEE Trans Inform Forensic Secur, 2017, 12: 1931–1940
4 Xu Y, Sun S, Cui J, et al. Intrusion-resilient public cloud auditing scheme with authenticator update. Inf Sci, 2020, 512: 616–628
5 Nithya S M V, Uthariaraj V R. Identity-based public auditing scheme for cloud storage with strong key-exposure resilience. Security Commun Networks, 2020, 2020: 1–13