Poster Abstract: Threshold Cryptography-based Authentication Protocol for Remote Healthcare

Qipeng Xie[1,2,5], Zhihe Zhao[3,4], Linshan Jiang[6], Siyang Jiang[4], Salabat Khan[5], Weizheng Wang[7], Kaishun Wu[5]
[1]Zhejiang Lab, HangZhou, China, [2]PQC Technologies Limited, China
[3]ThingX Technologies Limited, Hong Kong SAR, [4]Chinese University of Hong Kong, Hong Kong SAR
[5]Hong Kong University of Science and Technology (Guangzhou), Guang Zhou, China
[6]National University of Singapore, Singapore, [7]City University of Hong Kong, Hong Kong SAR

ABSTRACT

With the advancement of the Internet of Medical Things (IoMT) and cryptographic technologies, remote healthcare services have become more widespread, presenting new challenges for patient privacy and data security. Conventional security mechanisms, such as centralized authentication and key distribution systems, are susceptible to single points of failure and significant management burdens, potentially leading to compromised authentication centers and internal security threats. In response, this study presents a threshold signature algorithm, it uses Distributed Key Generation (DKG) that distributes private keys without the need for a trusted key distributor, requiring the cooperative signature of at least two nodes for authentication. This approach not only circumvents the risk of single points of failure but also enhances the system's robustness and efficiency. The experimental results validate its prospective utility in safeguarding remote healthcare data.

KEYWORDS

Threshold Cryptography, Authentication Protocol, IoMT.

ACM Reference Format:
Qipeng Xie[1,2,5], Zhihe Zhao[3,4], Linshan Jiang[6], Siyang Jiang[4], Salabat Khan[5], Weizheng Wang[7], Kaishun Wu[5] . 2023. Poster Abstract: Threshold Cryptography-based Authentication Protocol for Remote Healthcare . In *The 23tht ACM Information Processing in Sensor Networks (IPSN '24), MAY 13-16, 2024 HONG KONG, CHINA.* ACM, New York, NY, USA, 2 pages. https://doi.org/xxxx

1 INTRODUCTION

The advancement of IoT and encryption technologies has transformed healthcare through the creation of the Internet of Medical Things (IoMT) [3], enhancing healthcare by offering immediate and efficient services. However, widespread digital sharing of health data raises significant privacy and security concerns for patient information. Although remote medical services offer substantial convenience, authentication brings new challenges. The issues of inadequate identity verification and unauthorized access to data are prevalent. Current security methods, such as traditional authentication protocols [1], often lack clarity in permission hierarchies. For instance, physicians can access patient information directly from hospital databases, and similarly, attackers that compromise medical IoT devices could potentially obtain patient data from hospital systems. To mitigate these vulnerabilities, research has proposed threshold signature schemes based on Shamir's Secret Sharing [4]. However, these schemes require a trustworthy third party (dealer) to distribute key shares, which makes the system susceptible to fraud by the dealer and participants. Addressing the challenge of a trusted third party, existing Threshold Signature Schemes (TSS) protocols [2] are computationally intensive due to complex Zero-Knowledge Proofs (ZKPs) and commitment schemes, rendering them impractical for resource-constrained medical IoT devices. Therefore, a lightweight TSS tailored for low-power embedded devices is urgently needed. In response to these challenges, this poster introduces an innovative and efficient threshold signature protocol that operates without the need for a dealer, designed explicitly for the IoMT environment. It is designed to meet the computational constraints of low-power embedded devices while ensuring system security and robustness.

2 BACKGROUND & MOTIVATION

In the field of telemedicine, IoMT devices are crucial for delivering contemporary healthcare services by capturing and transmitting real-time patient data. This data is sent through edge servers to clinicians for diagnosis and stored in hospital databases. Nevertheless, during transmission, the data is vulnerable to security threats like man-in-the-middle and replay attacks, risking the confidentiality and integrity of sensitive patient information. To address these security vulnerabilities, there is an urgent need for a lightweight security mechanism that can ensure the secure transmission of data while accommodating the limited computational resources of IoMT devices. Threshold Signature Schemes (TSS) offer a potential solution by distributing the key across multiple participants, requiring collective involvement to complete the verification process. Furthermore, the adoption of TSS can enhance device authentication strength, prevent identity spoofing and replay attacks, and mitigate the risks of internal threats and privilege escalation attacks through fine-grained access control policies.

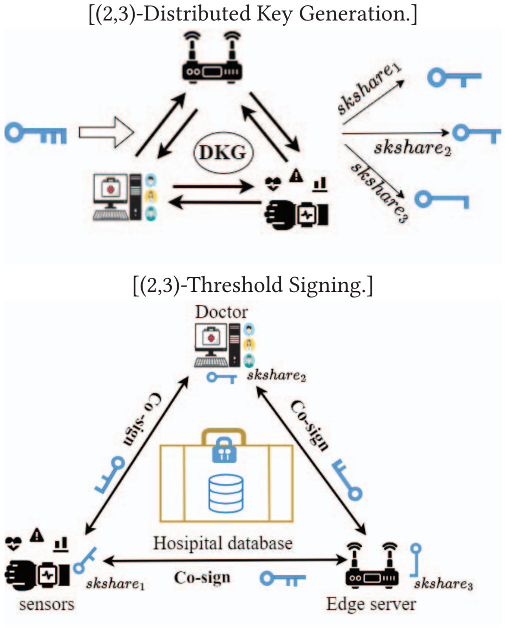
3 SYSTEM DESIGN

In the context of remote medical services, our proposed protocol delineates the interaction between four principal entities, as illustrated in Figure 1: 1) Sensors, 2) Edge server, 3) Hospital server, and 4) Hospital database. Each with distinct functionalities outlined

IPSN '24, MAY 13-16, 2024, HONG KONG, CHINA

ACM ISBN xxx…$15.00
https://doi.org/xxxx

979-8-3503-6201-5/24/$31.00 ©2024 IEEE
DOI 10.1109/IPSN61024.2024.00052



[(2,3)-Distributed Key Generation.]

[(2,3)-Threshold Signing.]

Figure 1: Overview of threshold cryptography-based authentication protocol. Note that in the signing phase, any 2 of 3 *skshare* **can co-sign to reconstruct the original** *sk***.**

as follows: **Hospital's database:** A secure storage system that maintains patient records and accepts incoming data from remote physicians, contingent on proper authentication and authorization. **Hospital server:** They are the end-users in the remote healthcare infrastructure, responsible for analyzing the patient data received from IoMT devices via the edge server and making medical diagnoses. **Edge server:** It acts as an intermediary that facilitates secure data transmission between IoMT devices and remote physicians. The edge server also participates in the DKG process to generate a part of the private key. **Sensors:** Monitor patient health metrics and generate sensitive data. Each IoMT device initiates the protocol by establishing a secure connection to the edge server.

Our protocol involves IoMT devices, edge servers, and hospital servers (excluding hospital databases) in performing a (2,3)-Distributed Key Generation (DKG) as depicted in Fig.1 (a). This generates a unique secret key for each entity and a single public key, with each entity securely holding a private key share. This collective approach defends against cyber threats like single points of failure and third-party attacks. Specifically, any two entities, such as the hospital server and sensors, can use a (2,3)-threshold signing scheme (Fig.1 (b)) to generate a signature. This not only allows for key recovery if lost but also strengthens system security. Once the signature is verified, sensors can send confidential data to the hospital server for analysis. Upon successful signature validation, the sensors are authorized to transmit confidential patient data to the hospital server for health analytics.

4 PRELIMINARY RESULTS

We simulated the entire lifecycle of our TSS protocol in a local environment, employing an 8-core processor with Ubuntu 20.04. Three distinct processes represented the participating parties in the scheme, and inter-process communication was facilitated via sockets. We compare our approach with two baseline approaches, [1] and [2], which are the traditional authentication protocol without any protection and existing threshold signature protocol, separately.

The comparison results are displayed in Table I. In comparison to [1], our proposed method offers an enhanced level of security while maintaining a computational time that is within the same order of magnitude. Compared to [2], we observe a significant reduction in computation time from 11.9 seconds to merely 0.11 seconds. This substantial decrease not only attests to the lower computational complexity of our methodology but also indicates its suitability for deployment on resource-constrained IoMT devices. For the communication overhead, the signing phase in our approach costs more than the other two baselines. However, the 160kb in 13 seconds is acceptable in our IoMT application if we consider the additional protection.

Table 1: Performance evaluation on different authentication approaches.

	DKG (Ours)	Sign (Ours)	[1]	[2]
Computation Time	0.01s	0.1s	10.8ms	11.9s
Communication Time	0.02s	13s	17ms	4.7s
Communication Overhead	0.2kb	160kb	0.41kb	3.8kb

5 CONCLUSION AND FUTURE WORK

In conclusion, our work introduces a threshold cryptography-based authentication protocol for IoMT, leveraging a (2,3)-Distributed Key Generation to eliminate single points of failure and avoid the need for a trusted dealer. Our results indicate that the protocol operates efficiently within the constraints of IoMT devices, offering minimal communication overhead and reasonable computational demands. In the future work, we intend to deploy the proposed authentication protocol on real-world devices[5].

ACKNOWLEDGEMENT

This work is supported by the Project of DEGP (No.2023KCXTD042), Zhejiang Lab Open Research Project (No.K2022PDOAB01), the Foundation for Distinguished Young Talents in Higher Education of Guangdong Province„ (No. 2022KQNCX084) and the fund which aims to improve scientific research capability of key construction disciplines in Guangdong province "Light-weight federal learning paradigm and its application" (No:2022ZDJS058). We thank Xiaojun Xie for her effort on the early stage of this work.

REFERENCES

[1] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S Morteza Pournaghi, and Mohammad-Ali Doostari. 2020. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks* 177 (2020), 107333.

[2] Rosario Gennaro and Steven Goldfeder. 2018. Fast multiparty threshold ECDSA with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1179–1194.

[3] Weizheng Wang, Qiu Chen, Zhimeng Yin, Gautam Srivastava, Thippa Reddy Gadekallu, Fawaz Alsolami, and Chunhua Su. 2021. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet of Things Journal* 9, 11 (2021), 8883–8891.

[4] Keping Yu, Liang Tan, Caixia Yang, Kim-Kwang Raymond Choo, Ali Kashif Bashir, Joel JPC Rodrigues, and Takuro Sato. 2021. A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet of Things Journal* 9, 11 (2021), 8154–8167.

[5] Zhihe Zhao, Kai Wang, Neiwen Ling, and Guoliang Xing. 2021. Edgeml: An automl framework for real-time deep learning on the edge. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*. 133–144.