Chapter 13
Performance Evaluation of Aggregate Signatures in Healthcare Environments

Saddam Hussain
https://orcid.org/0000-0003-1523-1330
Universiti Brunei Darussalam, Brunei

Ali Tufail
Universiti Brunei Darussalam, Brunei

Abdul Ghani Haji Naim
Universiti Brunei Darussalam, Brunei

ABSTRACT

The healthcare sector presents many prospects for the implementation of Healthcare WSNs. The utilization of online data exchange within the healthcare sector not only improves operational effectiveness but also mitigates temporal limitations. However, it is encountered with a significant concern over data privacy, and security to the personal health-related data. The digital signature is widely employed in the digital world to ensure the preservation of integrity and privacy. An aggregate signature scheme can associate several signatures on different messages with a single signature. This particular characteristic offers significant advantages within a context characterized by restricted bandwidth and limited processing resources. This study provides a comprehensive evaluation and comparison of aggregate signature schemes in the healthcare environment. We examine their primary features, contributions, security aspects, and performance efficiency. The analysis incorporates the available aggregate signature schemes employed in healthcare.

INTRODUCTION

The deployment of the Internet of Things spans in various fields, including industry, agriculture, transportation, logistics, medicine and healthcare respectively (M. Liu, Wang, Zhang, Long, & Qin,

DOI: 10.4018/979-8-3693-2109-6.ch013

2024). The rapid development of wireless communication and sensor technologies has resulted in a considerable increase in IoT applications based on Wireless Sensor Networks (WSNs). Healthcare wireless sensor networks are considered to be one of the most significant uses of the Internet of Things (IoT) in the medical business. For the aim of providing real-time monitoring and data collection, it is conceivable to implant medical sensors into the bodies of patients or to place them on the surfaces of their bodies. Following that, the information acquired is sent to medical professionals so that they may carry out monitoring, diagnosis, and treatment procedures in a manner that is both accurate and efficient (Wang et al., 2022). In accordance with the findings of the C R I R Institute ((2023), 2023), it is anticipated that the market for medical sensors will be worth a total of $1866.3 million from the years 2022 and 2028. In recent years, there has been a proliferation of health applications built for smart phones (Martínez-Ballesté, Pérez-Martínez, & Solanas, 2013), (Aranki, Kurillo, Yan, Liebovitz, & Bajcsy, 2016). These applications are specifically engineered to gather critical health information, including pulse rate and blood pressure. The information gathered by the sensors is transmitted to a cloud-based server, where medical facilities have deployed their data processing services. An analysis of the data is conducted with the intention of improving the standard of medical care delivered to the patients. Patients prefer hospitals to deliver their assistance in a manner that is not only highly efficient but also protects their identities (Mehmood, Natgunanathan, Xiang, Poston, & Zhang, 2018).

Subsequently, the healthcare professional receives the patient's medical information obtained through healthcare wireless sensor networks via a wireless link susceptible to tampering, loss, or forgery by malicious entities (Qiao, Yang, Zhou, Yang, & Zhang, 2023), (Bahache, Chikouche, & Mezrag, 2022). The presence of the security vulnerability compromises the integrity and authenticity of the patient. The security of patients' medical information, the diagnostic and therapeutic processes of medical practitioners, and potentially the patients' lives could be compromised (Al Ameen, Liu, & Kwak, 2012). In light of this, it is essential to employ security techniques that are both secure and efficient in order to ensure the integrity and authenticity of the data. Digital signatures have the ability to guarantee the authenticity and integrity of data (J. N. Chen et al., 2020),(T.-Y. Wu, Chen, Wang, & Wu, 2019),(C.-M. Chen, Xiang, Liu, & Wang, 2019), (T.-Y. Wu, Tsai, & Tseng, 2012). In a digital signature scheme, the private key of the signer is needed to generate a signature, and the public key of the signer is needed to verify a signature. The signer is the only one who holds the private key, and thus it is the only one who can generate a valid signature. However, conventional digital signature techniques, employed for the integrity and authenticity of data become less efficient when used in a large-scale healthcare WSNs due to its minimal computational capabilities. Hence, a data aggregation with signature will be vital in healthcare WSNs.

Aggregate signature is a cryptographic primitive. It allows for the efficient transmission and verification of signatures. In 2003 at Eurocrypto, (Boneh, Gentry, Lynn, & Shacham, 2003) introduced the notion of aggregate signature. Aggregate signature can be used to accomplish the transmission, verification and authentication of multiple signatures. In the aggregate signature primitive, n separate messages are signed by n distinct signers individually. Following that, the outputs of the n signatures are combined into a single aggregate signature as shown in Figure 1. Additionally, it is feasible to verify numerous signatures at the same time, which results in a decrease in the amount of communication overhead and computation time that is associated with the verification process. It displays an exceptional level of efficiency in real time. The utilization of aggregate signature in healthcare WSNs has the potential to enhance the efficiency of communication but also lower the computational

A Survey of Unsupervised Learning in Medical Image Registration
Xin Songand Huan Yang (2022). *International Journal of Health Systems and Translational Medicine (pp. 1-7).*
www.irma-international.org/article/a-survey-of-unsupervised-learning-in-medical-image-registration/282701