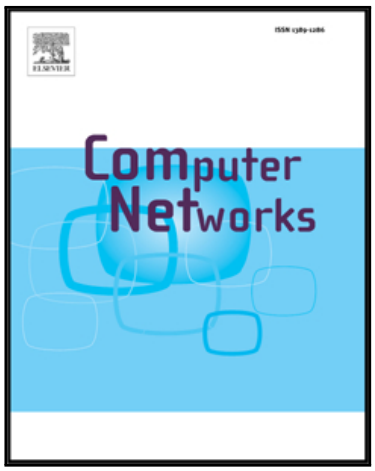

Practical Integrity Preservation for Data Streaming in Cloud-Assisted Healthcare Sensor Systems

Chi-Yuan Chen, Hsin-Min Wu, Lei Wang, Chia-Mu Yu

PII: S1389-1286(17)30243-8
DOI: 10.1016/j.comnet.2017.05.032
Reference: COMPNW 6226

To appear in: *Computer Networks*

Received date: 15 December 2016
Revised date: 14 April 2017
Accepted date: 31 May 2017

Please cite this article as: Chi-Yuan Chen, Hsin-Min Wu, Lei Wang, Chia-Mu Yu, Practical Integrity Preservation for Data Streaming in Cloud-Assisted Healthcare Sensor Systems, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.05.032

Practical Integrity Preservation for Data Streaming in Cloud-Assisted Healthcare Sensor Systems

Chi-Yuan Chen[1], Hsin-Min Wu[2], Lei Wang[3], and Chia-Mu Yu[4*]

[1]Department of Computer Science and Information Engineering, National I-Lan University, Taiwan
[2]Department of Computer Science and Engineering, Yuan Ze University, Taiwan
[3]Department of Biomedical Engineering, Shenzhen Institutes of Advanced Technology, Chinese Academy of Science, China
[4]Department of Computer Science and Engineering, National Chung Hsing University, Taiwan
*Corresponding Author
Email: chiyuan.chen@ieee.org; secret011179@gmail.com; wang.lei@siat.ac.cn; chiamuyu@nchu.edu.tw

***Abstract*—In this paper, we address the problem of integrity protection for data streaming in cloud-assisted healthcare sensor systems. First, we propose a novel data structure, called the arithmetic Merkle tree (AMT), as a candidate method for ensuring the flexibility of the tree structure. However, AMT is flawed by one-wayness and therefore cannot be applied directly. We consider integrating homomorphic encryption with the AMT, and propose two solutions, called the PAMT (partially homomorphic encryption-based AMT) and the FAMT (fully homomorphic encryption-based AMT). Our proposed PAMT outperforms the existing solution because of the implementation of widely used software that optimizes partially homomorphic encryption. However, although the design of our proposed FAMT includes fully homomorphic encryption, in the case of data archival applications, transferal of the computation burden to the cloud server renders it very lightweight. The theoretical analysis and simulation results also confirm the efficiency of our PAMT and FAMT solutions.**

***Index Terms*—Integrity Preservation, Healthcare, Sensors, Cloud Computing, Homomorphic Encryption.**

I. Introduction

Sensor-based systems have been implemented in numerous applications. For example, a large number of sensors have been deployed to collect environmental information of large areas (see, e.g., for a volcano [1]). Another example is vehicle sensor networks, where automobiles with vehicle sensors, as in the on-board diagnostic (OBD) system, can not only improve driving safety by periodically broadcasting the sensed vehicle information but also contribute to insurance premium negotiations by sending the real-time driver behavior to the central server of the drivers insurance company as additional risk analysis data. Among potential sensor-based applications, the most promising for the near future is healthcare monitoring systems [2]. The recent trend of people wearing smart watches for monitoring basic physiological conditions, such as sleep patterns, is just the beginning. One can imagine patients equipped with a variety of body sensors that enable their physicians to remotely monitor and retrieve their biomedical signals.

However, since the amount of data collected could be huge (e.g., the amount of physiological signals captured by a physiological sensor can easily reach close to 2.7 GB), individual sensors do not have sufficient processing power and storage to analyze the data and generate meaningful results. Therefore, cloud technology is introduced into the system to mitigate the processing and storage burdens, and then, the sensors can continue to collect data and transmit the data to the cloud server in a streaming fashion to compensate their limited resource. The system administrators, i.e., the individuals wearing the physiological sensors or their physicians, instead of directly accessing every raw data item from individual sensors, issue queries to the cloud server and conduct analysis only of the data of interest, resulting in a relatively low computation and bandwidth overhead.

A. Concern about Data Integrity

The underlying assumption of the above cloud-assisted sensor-based streaming data architecture is that the cloud server can be trusted. Nevertheless, either the cloud server may intentionally manipulate the sensed data resulting, for example, in financial loss or decision errors, or it may report a falsified query result to the querier as a result of misconfigurations or software/hardware errors. An incomplete query result for protected health information (PHI) may cause serious consequences, such as incorrect diagnoses and inappropriate treatment [3].

Hence, the development of mechanisms to address the problem of integrity preservation for data streaming (IPDS) in cloud-assisted body sensor-based healthcare systems is required. For brevity, throughout this paper, this entire problem is named IPDS. The details of the IPDS problem are described in Sec. II-A.

The design challenges involved in developing a security protocol for the IPDS problem are three-fold. First, usually wearable medical devices suffer serious resource constraints. In other words, their computation power and communication capability is limited, preventing the frequent use of heavy-weight cryptographic primitives in the security protocol. Second, the throughput of the user devices needs to be sufficient to match the data generation speed (e.g., the sample rate in medical applications needs to be sufficiently high). This is in fact related to the first constraint; since the device usually does