Emerging Trends, Issues, and Challenges in Big Data and Its Implementation Toward Future Smart Cities

Secure Multimedia Big Data in Trust-Assisted Sensor-Cloud for Smart City

Chunsheng Zhu, Lei Shu, Victor C. M. Leung, Song Guo, Yan Zhang, and Laurence T. Yang

The authors reviewed the recent work on multimedia big data and SC. They observe three critical issues that affect the success of secure multimedia big data in TASC. With that, motivated by addressing the identified critical issues, they introduce two types of TASC: TASC-S and TASC-M.

Abstract

Lately, with the prevalence of digital devices and social network applications, the explosive growth of multimedia big data poses many challenges for users to obtain them securely in various application scenarios. In this article, investigating secure multimedia big data application in trust-assisted sensor cloud (TASC), which is one kind of SC for smart city, the recent work about multimedia big data and SC is reviewed first. Further, the critical issues that affect the success of secure multimedia big data in TASC are identified. With that, motivated by addressing the identified critical issues, this article proposes two types of TASC: TASC-S (TASC with a single trust value threshold), and TASC-M (TASC with multiple trust value thresholds). Finally, with extensive simulation results about TASC-S and TASC-M as well as SC without trust assistance (SCWTA), the following insights into secure multimedia big data in TASC are achieved: the throughput of TASC-S and TASC-M can both be generally higher than that of SCWTA; the throughput of TASC-S can trend with tuned trust value threshold; and the throughput of TASC-M can fluctuate with the same trust value thresholds.

Introduction

Recently, as a unique branch of big data that represents the explosive growth of data from a variety of sources happening in our society, multimedia big data is utilized to describe the huge amounts of multimedia data produced with the prevalence of cameras, mobile devices, social media, the Internet, and so on. Particularly, multimedia big data has the following features. First, it is unstructured, heterogeneous, and multimodal. Second, it has cognition, which bridges the semantic gap between low-level features and high-level semantics. Third, it typically has real-time delivery. Fourth, it is acquired, processed, and analyzed efficiently and scalably. Multimedia big data technology greatly boosts a lot of multimedia applications/services (e.g., multimedia search, multimedia advertisement). Meanwhile, the boom of multimedia big data poses many challenges for users to achieve them securely in various application scenarios. For instance, as discussed in [1], in terms of secure multimedia big data sharing in social networks, substantial potential risks (e.g., illegal copying, illegal distribution, misappropriation) could exist for maliciously utilizing the multimedia big data. In such cases, security mechanisms are needed to ensure the security of multimedia big data with respect to its source identity, content integrity, privacy, and so on.

In this article, studying secure multimedia big data application in trust-assisted sensor cloud (TASC) [2] which is one kind of sensor cloud (SC) for smart city [3], we review the recent work about multimedia big data and SC first. Further, we identify the critical issues that affect the success of secure multimedia big data in TASC. Then, triggered by addressing the identified critical issues, we propose two types of TASC:

- TASC-S (TASC with a single trust value threshold)
- TASC-M (TASC with multiple trust value thresholds)

Eventually, with extensive simulation results about TASC-S and TASC-M as well as SC without trust assistance (SCWTA), we observe the following insights into secure multimedia big data in TASC:

- The throughput of TASC-S and TASC-M can both be generally higher than that of SCWTA.
- The throughput of TASC-S can trend with tuned trust value threshold.
- The throughput of TASC-M can fluctuate with the same trust value thresholds.

The main contributions of this article are as follows:

- This article is the first work that explores secure multimedia big data application in TASC. This clearly demonstrates the novelty of this work compared to other works on multimedia big data and SC.
- Induced by addressing the observed critical issues that influence the success of secure multimedia big data in TASC, this article puts forward two types of TASC (i.e., TASC-S and TASC-M). With extensive simulation results on TASC-S and TASC-M as well as SCWTA, this article obtains three insights into secure multimedia big data in TASC.
- The remainder of this article is organized as follows. We present the preliminaries about TASC, We review the recent work about multimedia big data and SC. The identified critical issues that affect the success of secure multimedia big
data in TASC are illustrated. The proposed TASC-S and TASC-M are introduced. Evaluation of TASC-S and TASC-M as well as SCWTA is conducted. This article is then concluded.

**Preliminaries About TASC**

**SC**

As an essential component of the Internet of Things (IoT) [4], which aims to connect everything, SC is a new paradigm that integrates the wireless sensor network (WSN) and the cloud for smart city. Specifically, as shown in Fig. 1, SC includes three basic entities: the WSN, the cloud, and the users. The WSN, consisting of sensor nodes, is for gathering and transmitting various sensory data (temperature, humidity, motion, video, etc.) to the cloud. The cloud consists of data centers and is for storing and processing the received sensory data (e.g., multimedia big sensory data) as well as further delivering the processed sensory data to the users on demand. Therefore, with SC, the WSN and the cloud can complement each other. For example, the utility of the WSN can be enhanced by serving multiple applications via the cloud, while the services that the cloud offers can be enriched by offering the service the WSN provides. Moreover, the users are able to conveniently have access to their desirable sensory data (e.g., multimedia big sensory data) from the cloud anytime and anywhere if there is an Internet connection. All these features are desired for smart city, which strategically incorporates various networks and computing platforms to offer desirable services for people.

**Trust**

With different definitions regarding various fields, trust [2] is defined as “assured reliance on the character, ability, strength or truth of someone or something” by the Merriam-Webster Dictionary. Particularly in terms of wireless communications, trust can be defined as “trust of a node A in a node B is the subjective expectation of node A receiving positive outcomes from the interaction with node B in a specific context.” Generally, to evaluate the trust from node A to node B, node A needs to collect various evidences (e.g., maliciousness, selfishness, honesty) about node B, based on either direct interactions or information from third parties. Further, the trust value of node B is determined by utilizing a function or functions to convert the collected evidence into the trustworthiness (i.e., trust value).

**TASC**

Improving the quality of service (QoS) at which users obtain sensory data (e.g., multimedia big sensory data) from the cloud, TASC is a new kind of SC, recently proposed in [2]. Particularly, as presented in Fig. 2, the basic concept of TASC is incorporating trust into SC. In other words, the trusted sensors (i.e., sensors with trust values exceeding a threshold) are adopted in the WSN for collecting and transmitting sensory data to the cloud, while the trusted data centers (i.e., data centers with trust values exceeding a threshold) are utilized in the cloud to store, process, and further deliver the processed sensory data to the users on demand. With TASC, since the used sensors and data centers are assured and reliable sensors and data centers with trust values exceeding certain thresholds, the throughput and response time in which users achieve sensory data from the SC can be substantially improved.

**System Model of TASC**

Based on [2], the system model of TASC is presented as follows as an instance.

- The SC includes one WSN, one cloud, and θ users.
- In the WSN, there is one sink node s₀ and Δ normal sensor nodes sᵢ (1 ≤ i ≤ Δ). Normal sensor nodes transmit sensed sensory data to the sink node, and the data rate is rᵢ, kb/s.
- Regarding the cloud, there are Λ data centers dⱼ (1 ≤ j ≤ Λ), which store and process the sensory data received from the WSN.
- The θ users obtain the processed sensory data from the cloud.
- In addition, time is divided into Γ time epochs τₖ (1 ≤ k ≤ Γ). In each time epoch τₖ, each sensor node sᵢ has a trust value viₖ and each data center dⱼ has a trust value viₖⱼ.

**Recent Work About Multimedia Big Data and SC**

Regarding the authorization of multimedia big data, a framework is presented in [5] for the composition and enforcement of priva-
Regarding the trust value in TASC, since the neighbor node number and behaviors as well as energy consumption of sensor nodes and data centers are critical issues, they are incorporated together to determine the trust values of sensor nodes and data centers in TASC.


Researching the sensory data transmission of SC, a time and priority-based selective data transmission technique and a priority-based sleep scheduling technique are presented in [10] toward offering more useful data reliably from WSNs to mobile cloud. In terms of the energy efficiency of SC, two collaborative location-based sleep scheduling mechanisms are shown in [11] for prolonging the lifetime of WSNs integrated with cloud. Exploring the pricing of SC, five pricing models are introduced in [12] for SC, and they serve as guidance for future research with respect to pricing in SC. Concerning the framework of SC, a novel sensory data processing framework is proposed in [13] to integrate WSNs with mobile cloud, while transmitting desirable sensory data to mobile users in a fast, reliable, and secure way. Focusing on the application of SC, [14] investigates the integration of SC and power line communication and further envisions their applications and advantages.

To the best of our knowledge, there are only a few recent studies about the security of multimedia big data, and there is no recent work directly regarding TASC. Our work is the first that investigates secure multimedia big data application in TASC.

**Figure 2.** An example of TASC.

**ISSUES ABOUT SECURE MULTIMEDIA BIG DATA IN TASC**

Intuitively, the following critical issues can be obtained regarding the success of secure multimedia big data in TASC.

**NEIGHBOR NODE NUMBER OF SENSOR NODES AND DATA CENTERS**

This issue is related to whether there are sufficient sensor nodes in the WSN and whether there are sufficient data centers in the cloud to enable secure multimedia big sensory data in TASC. For instance, as shown in cases (a) and (a)' in Fig. 3, if there is only one neighbor node for a certain sensor node in the WSN and for a certain data center in the cloud, regardless of whether the utilization of that neighbor node could enable secure multimedia big sensory data, that neighbor node has to be utilized if needed. Moreover, it may happen that there is no neighbor node for an intermediate sensor node in the WSN and for an intermediate data center in the cloud, for a variety of reasons (e.g., deployment of SC, mobility of sensor node, workload of data center).

**BEHAVIORS OF SENSOR NODES AND DATA CENTERS**

This issue is related to whether the behaviors (e.g., data collection behavior, data transmission behavior) of sensor nodes in the WSN are positive enough and whether the behaviors (e.g., data storage behavior, data processing behavior, data delivery behavior) of data centers in the cloud are positive enough for enabling secure multimedia big sensory data in TASC. For instance, as shown in cases (b) and (b)' in Fig. 3, although there are several neighbor nodes for a certain sensor node in the WSN and for a certain data center in the cloud, the behaviors of these neighbor nodes might be too negative (marked with values lower than 0.5 for both sensor nodes and data centers) to be utilized for secure multimedia big sensory data.

**ENERGY CONSUMPTION OF SENSOR NODES AND DATA CENTERS**

This issue is related to whether the sensor nodes in the WSN and the data centers in the cloud have enough residual energy to enable secure multimedia big sensory data in TASC. For instance, as
shown in cases (c) and (c)' in Fig. 3, even when there are available neighbor nodes with positive enough behaviors for a certain sensor node in the WSN and for a certain data center in the cloud, the residual energy of these neighbor nodes probably are too low (marked with values lower than 5 J for sensor nodes and lower than 200 J for data centers) to be utilized for secure multimedia big sensory data.

**TASC-S AND TASC-M**

Motivated by the above observed critical issues that influence the success of secure multimedia big data in TASC, the proposed two types of TASC (i.e., TASC-S and TASC-M) are illustrated as follows considering the trust value and the trust value threshold, which are two fundamental elements in TASC.

**TRUST VALUE IN TASC**

Regarding the trust value in TASC, since the neighbor node number and behaviors as well as energy consumption of sensor nodes and data centers are critical issues regarding enabling secure multimedia big sensory data in TASC, they are incorporated together to determine the trust values of sensor nodes and data centers in TASC.

In particular, trust agents can be established to collect various pieces of evidence about the neighbor node number, behaviors, and energy consumption of sensor nodes and data centers. After the evidence is gathered, functions (e.g., multidimensional trust evaluation functions) can be utilized to convert the gathered evidence into the trust values of sensor nodes and data centers.

In such a way, the trust values of sensor nodes and data centers, various sensor nodes and data centers can be utilized in each time epoch to realize different QoS, regarding secure multimedia big sensory data in TASC.

**TASC-S**

With a single trust value threshold in TASC-S, the trust value thresholds for all the sensor nodes in the WSN and for all the data centers in the cloud are the same in each time epoch. For example, as shown in Fig. 4, the trust value threshold for each sensor node in the WSN is $v_1$, and the trust value threshold for each data center in the cloud is $V_1$ during that time epoch. In other words, only sensor nodes with trust values exceeding $v_1$ will be utilized in the WSN, and only data centers with trust values exceeding $V_1$ will be utilized in the cloud during that time epoch. In such a manner, the aim of TASC-S is to achieve scalable QoS with lower bound in terms of secure multimedia big sensory data in TASC.

**TASC-M**

With multiple trust value thresholds in TASC-M, the trust value thresholds for different sensor nodes in the WSN and for different data centers in the cloud vary in each time epoch. For example, as presented in Fig. 5, the trust value thresholds for the sensor nodes in the WSN are $v_1$, $v_2$, $v_3$, $v_4$, $v_5$, and $v_7$ during that time epoch. Meanwhile, the trust value thresholds for the data centers in the cloud are $V_1$, $V_2$, $V_3$, $V_4$, $V_5$, and $V_7$ during that time epoch. Thus, in the WSN, the utilized trusted sensor nodes are with trust values exceeding $v_1$, $v_2$, $v_3$, $v_4$, $v_5$, and $v_7$ during that time epoch. In the cloud, the utilized trusted data centers are with trust values exceeding $V_1$, $V_2$, $V_3$, $V_4$, and $V_7$ during that time epoch. In such a way, the target of TASC-M is to obtain scalable QoS without bound, with respect to secure multimedia big sensory data in TASC.
EvAluAtIon Performed in NetTopo [15] with SC’s throughput as the QoS metric, the evaluation is presented as follows regarding secure multimedia big data in TASC-S, TASC-M and SCWTA.

EvAluAtIon sEtup The SC consists of one WSN, one cloud, and 10 users [2]. Regarding the WSN, it includes one sink node and 100 normal video sensor nodes with a data rate of 1000 kb/s. The cloud includes 10 data centers. It is assumed that each time epoch is 1 s. In each time epoch, the sensor nodes and data centers have trust values which indicate the probabilities that secure multimedia big sensory data is successfully realized utilizing them, as illustrated earlier.

For TASC-S, the trust values for the sensor nodes in the WSN exceed a trust value threshold and the trust values for the data centers in the cloud exceed a trust value threshold. About TASC-M, the trust values for different sensor nodes in the WSN exceed various trust value thresholds and the trust values for the data centers in the cloud exceed various trust value thresholds.

• Scenario 1: Three tests are conducted, and each test has 100 different topologies for TASC-S, TASC-M, and SCWTA. In each test, the trust value thresholds for both sensor nodes and data centers are 0.5. Regarding TASC-M, the trust value thresholds for different sensor nodes and different data centers are random between 0.3 and 0.7.

• Scenario 2: Three tests are conducted, and each test has a specific topology for TASC-S. Particularly, in each test, the trust value threshold for the sensor nodes and the trust value threshold for the data centers are changed nine times from 0.1 to 0.9 for TASC-S.

• Scenario 3: Three tests are conducted, and each test has 10 different topologies for TASC-M. Particularly, in each test, different topologies have the same trust value thresholds between 0.1 and 0.9 for TASC-M.

EvAluAtIon rEsults The evaluation results in scenarios 1, 2, and 3 are presented in Fig. 6. Specifically, from Figs. 6a–6c, it can be observed that the throughput of SCWTA is generally lower than that of TASC-S and TASC-M. In other words, the throughput of TASC-S and TASC-M can both be generally higher than that of SCWTA. From Figs. 6d–6f, it can be seen that when the trust value threshold for TASC-S grows, the throughput of TASC-S is increased. Namely, the throughput of TASC-S can trend with tuned trust value threshold. From Figs. 6g–6i, ruleless throughput of TASC-M can be achieved with the same trust value thresholds.

conclusIon Concerning secure multimedia big data application in TASC for smart city, this article has reviewed the recent work on multimedia big data and SC first. Further, this article has observed three critical issues that affect the success of
secure multimedia big data in TASC. Motivated by addressing the identified critical issues, this article has introduced two types of TASC (i.e., TASC-S and TASC-M). Eventually, with extensive simulation results on TASC-S and TASC-M as well as SCWTA, this article has achieved three insights into secure multimedia big data in TASC:

- The throughput of TASC-S and TASC-M can both be generally higher than that of SCWTA.
- The throughput of TASC-S can trend with tuned trust value threshold.
- The throughput of TASC-M can fluctuate with the same trust value thresholds.

**Acknowledgement**

This work was supported by a Four Year Doctoral Fellowship from the University of British Columbia and funding from the Natural Sciences and Engineering Research Council of Canada, the ICICS/
TELUS People & Planet Friendly Home Initiative at the University of British Columbia, TELUS, and other industry partners. This work was partially supported by the MacEwan Engineering Research Center of Industrial Internet of Things under Grant No. 517018. This work was partially supported by the project IoTSec — Security in IoT for Smart Grids, with number 248113/O70, part of the IKTPLUS program funded by the Norwegian Research Council. This research is partially supported by the projects 240079/F20 funded by the Research Council of Norway.

REFERENCES


BIographies

Chunsheng Zhu (czhu@ece.ubc.ca), is a postdoctoral research fellow in the Department of Electrical and Computer Engineering, University of British Columbia, Canada. He received his Ph.D. degree in electrical and computer engineering from the University of British Columbia in 2016. His current research interests mainly include wireless sensor networks, cloud computing, the Internet of Things, social networks, and security.

Lei Shi (lei.shi@ieee.org) is a Lincoln Professor at the University of Lincoln, United Kingdom, and a Distinguished Professor at Nanjing Agricultural University, China. He is an Associate Editor of IEEE Transactions on Industrial Informatics, the IEEE Systems Journal, and IEEE Access. His research interests include wireless sensor networks and cloud computing.

Victor C. M. Leung (vleung@ece.ubc.ca) is a professor in the Department of Electrical and Computer Engineering and holder of the TELUS Mobility Research Chair, University of British Columbia. His research is in the areas of wireless networks and mobile systems. Dr. Leung is a fellow of the Royal Society of Canada, a Fellow of the Canadian Academy of Engineering, and a Fellow of the Engineering Institute of Canada.

Yan Zhang (yanzhang@ieee.org) is a professor in the Department of Informatics, University of Oslo, Norway. He is also a chief research scientist at Simula Research Laboratory, Norway. He is an Associate Technical Editor of IEEE Communications Magazine, and an Editor of IEEE Transactions on Green Communications and Networking and IEEE Communications Surveys & Tutorials. His current research interests include next-generation wireless networks leading to 5G, and green and secure cyber-physical systems.

Laurence T. Yang (flyang@stfx.ca) is a professor in the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, embedded and ubiquitous/pervasive computing, and big data. His research has been supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation.