Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions

3

Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos

The authors introduce the architecture and unique security and privacy requirements for the next generation mobile technologies on cloud-based IoT, identify the inappropriateness of most existing work, and address the challenging issues of secure packet forwarding and efficient privacy preserving authentication by proposing new efficient privacy preserving data aggregation without public key homomorphic encryption.

ABSTRACT

The Internet of Things is increasingly becoming a ubiquitous computing service, requiring huge volumes of data storage and processing. Unfortunately, due to the unique characteristics of resource constraints, self-organization, and short-range communication in IoT, it always resorts to the cloud for outsourced storage and computation, which has brought about a series of new challenging security and privacy threats. In this article, we introduce the architecture and unique security and privacy requirements for the next generation mobile technologies on cloud-based IoT, identify the inappropriateness of most existing work, and address the challenging issues of secure packet forwarding and efficient privacy preserving authentication by proposing new efficient privacy preserving data aggregation without public key homomorphic encryption. Finally, several interesting open problems are suggested with promising ideas to trigger more research efforts in this emerging area.

INTRODUCTION

The Internet of Things (IoT) is composed of physical objects embedded with electronics, software, and sensors, which allows objects to be sensed and controlled remotely across the existing network infrastructure, facilitates direct integration between the physical world and computer communication networks, and significantly contributes to enhanced efficiency, accuracy, and economic benefits [1, 2]. Therefore, IoT has been widely applied in various applications such as environment monitoring, energy management, medical healthcare systems, building automation, and transportation. Unfortunately, due to the resource constraints of IoT devices, they always delegate highly complex computation to the energy abundant cloud for considerably enhanced efficiency. However, both the inputs, outputs, and function of the underlying computation may be closely related to the privacy of IoT users, which cannot be exposed to collusion between malicious cloud servers and malicious IoT users. Therefore, how to design new efficient privacy-preserving solutions for next generation mobile technologies with IoT–cloud convergence is a crucial issue of great concern.

MOTIVATION

According to the functionality, cloud-based IoT can be categorized into static and mobile, the latter of which is more challenging in protocol design. Therefore, in this article, we mainly focus on the security and privacy issues and corresponding countermeasures in mobile cloud-based IoT. The fast development of next generation mobile technologies such as fifth generation (5G) on IoT–cloud convergence has cast light on types of security and privacy issues unaddressed for years.

The characteristics of resource-constrained short-range communication and mobility result in the unique features of packet forwarding in cloud-based IoT. Specifically, it lacks the end-to-end continuous connectivity between mobile IoT users (IoT users, nodes, and devices are used exchangeably in the rest of this article), and message delivery needs to be fulfilled by cooperation among a social group of IoT users directed toward the destination. However, selfish nodes would not be willing to participate in this energy-consuming task due to their limited resources unless they can obtain maximized gain from it. It is obvious that the more packets one IoT user transmits, the more benefit it will obtain. However, it would also be more likely to be selected as the compromise target by the adversary from the side channel attack through analyzing the packet flow around each IoT node and lose all earned utility. The reason is that if such an IoT node were compromised, the adversary would obtain more packets from one single attack, which we name target-oriented compromise. Therefore, it is required to design a secure incentive mechanism to stimulate collaboration for packet forwarding in cloud-based IoT. In addition, malicious IoT users could collude to illegally increase their utility by detouring the packet transmission routing. Until now, how to prevent a layer-adding attack in collaborative packet forwarding in IoT is still an open problem requiring convincing solutions.

On the other hand, cloud-based IoT has also provided a convincing platform to guarantee distributed location-based service (LBS) by periodically collecting and broadcasting certain kinds of passing service information such as all the restaurants satisfying the user's query conditions in the neighborhood and the traffic conditions for spe-

Digital Object Identifier:
10.1109/MCOM.2017.1600363CM

Jun Zhou, Zhenfu Cao, and Xiaolei Dong are with East China Normal University; Athanasios V. Vasilakos is with the National Technical University of Athens. Jun Zhou is the corresponding author.

0163-6804/17/$25.00 © 2017 IEEE

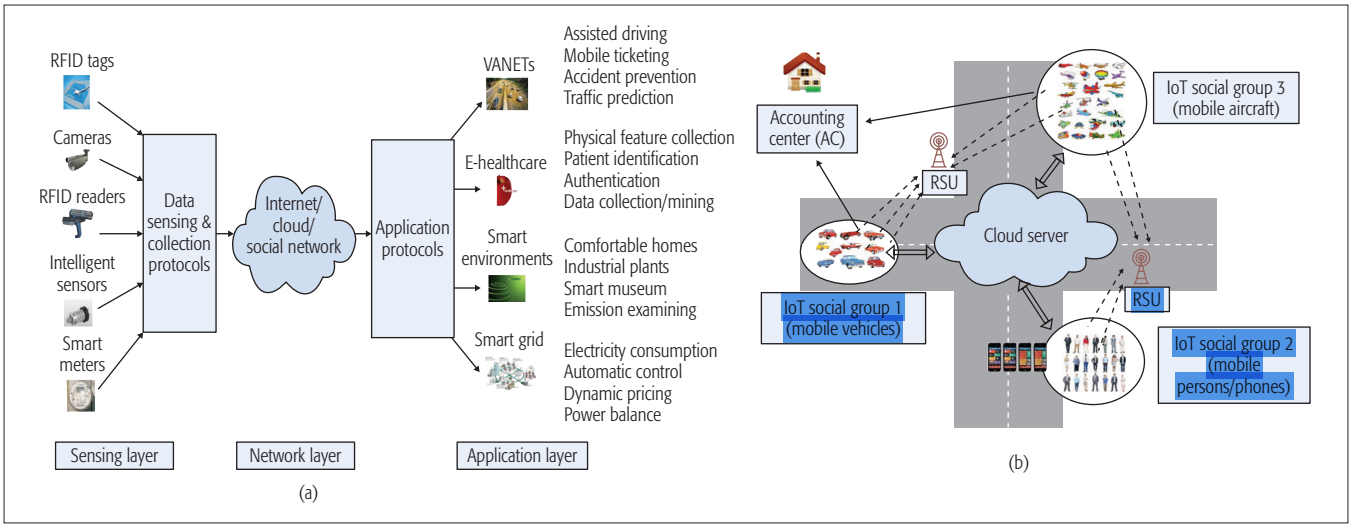

Figure 1. Network architecture of cloud-based IoT.

cific road sections during required time periods. Unfortunately, it actually faces various sophisticated attacks such as eavesdropping, modification, and repudiation. A malicious IoT user intends to forge its identity, manipulate the transmitted messages, and even to escape from crimes due to the lack of efficient tracking mechanisms. This false information would lead to other users' inconvenience and even disasters, which should be prevented from dissemination by designing effective authentication mechanisms in IoTs. Moreover, it is likely that mobile IoT users geologically in the neighborhood of each other would collect the information about the same event to generate considerably redundant packets. On the other hand, IoT users' conditional identity privacy and location privacy closely related to their private living habits should be well protected. Last but not least, it is reported that although appropriately powered, each resource-constrained IoT device is generally required to verify about 1000–5000 messages per second, the high computational complexity of which is still intolerable [5]. Therefore, it is required to propose privacy-preserving lightweight authentication with message content filtering to avoid duplicate packet transmission and reduce both the computational and communication cost.

Although several works have studied the security issues in IoT [3–5, 7, 9, 13] w.r.t. secure packet forwarding and lightweight message authentication, the challenging problems of the target-oriented compromise attack, the layer-adding collusion attack, and the privacy preserving message content filtering from generation still cannot be well addressed. Moreover, most of the existing work [3–5, 7, 9, 11, 13] considered the IoT and cloud computing system as independent entities. The researchers in IoT rarely took the cloud as an underlying primitive to execute the outsourced storage or outsourced computation for resource-constrained IoT users; while the studies on secure outsourced computation widely exploited public key homomorphic encryption, which is so computationally intensive that it cannot adapt well to the efficiency requirement for IoT users. In this article, we discuss the unique security and privacy challenges brought by the new architecture of IoT–cloud convergence and propose new convincing solutions to the above-mentioned challenging issues in cloud-based IoT.

Contributions

In this article, we first give an overview and the network architecture of cloud-based IoT. Then we identify the unique security and privacy requirements in cloud-based IoT, propose a new method of efficient privacy preserving data aggregation without exploiting public key homomorphic encryption, and further exploit it to address secure packet forwarding by designing outsourced aggregated transmission evidence to resist layer-adding attack and efficient authentication by devising outsourced privacy-preserving message filtering in cloud-based IoT. Finally, we suggest some future research directions with promising ideas.

Network Architecture of Cloud-Based IoT

In this section, the network architecture of cloud-based IoT is presented. It is assumed that mobile IoT users are generally categorized into social groups since the ones at specific times and locations are always moving in the same pattern such as the direction and velocity [2,10]. IoT devices allow both mutual communication with each other and with the cloud. Therefore, whenever two IoT users are moving into transmission range of each other, they can exchange packet bundles. In addition, IoT users in each group passing specific locations would generate duplicate/redundant bundles reporting similar events at an overwhelmingly high probability. Finally, the resource-constrained IoT devices such as sensors, RFID tags, cameras, and smart meters would outsource the computations of high complexity to the cloud for efficiency optimization [12]. Figure 1a demonstrates the sensing layer, network layer, and application layer in cloud-based IoT, while Fig. 1b shows the network model of mobile cloud-based IoT with the following unique characteristics.

Resource Constraints: IoT devices are always

Items	Internet of Things	Traditional networks
Node energy	Constrained	Abundant
Node mobility	High mobility	Static
Architecture	Self-organized	Hierachical
Communication range	Short	Long
Routing	Intermittent and dynamically constituted	Continuous end-to-end connection
Packet delivery mode	Cooperative, DTN type, and need incentive mechanism to stimulate	Guaranteed delivery

Table 1. Characteristic comparison between cloud-based IoT and traditional networks.

resource-constrained and comply with the store-carry-and-forward method of packet forwarding only when their storage is available. Computationally intensive tasks are intolerable by IoT nodes and must be outsourced to the cloud, both the storage and computational resources of which are assumed to be abundant. Therefore, the resource-constrained property requires lightweight protocol design for efficiency and practicability, especially on the IoT users' ends.

Mobility: Moving IoT users (i.e., vehicles and mobile electricity consumers) are dynamically categorized into multiple social groups according to their directions, velocities, and accelerations, and assumed to be uniformly distributed. All IoT nodes in each group are in communication range of each other, broadcast their collected content bundles on demand, and share a dynamically updated group key negotiated by all of them. The group leader is located at the group center, invulnerable to certain threats, and periodically updated due to dynamic group formulation.

Self-Organization: Mobile IoT users frequently collect and broadcast packet bundles within communication range of each other. The cloud intervenes only when computations of high complexity need to be delegated from resource-constrained IoT devices, but does not frequently participate in the distributed content bundle generation and authentication.

Short-Range Communication: Due to both the mobility and short-range communication, there is no guaranteed connection (routing) between the source and destination in mobile cloud-based IoT. All IoT users constitute a delay-tolerant network (DTN). Packet transmission is fulfilled through cooperation among IoT users, and the accounting center (AC) is responsible for charging and rewarding. Table 1 demonstrates the characteristic comparison between cloud-based IoT and traditional computer networks.

Security and Privacy Requirements for Cloud-based IoT

We mainly focus on the security threats for cloud-based IoT, especially in the aspects of secure packet forwarding with outsourced aggregated transmission evidence generation and efficient privacy-preserving authentication with outsourced message filtering. Besides the traditional data confidentiality and unforgeability, the unique security and privacy requirements in cloud-based IoT are presented:

Identity Privacy: Conditional identity privacy refers to the fact that the mobile IoT user's real identity should be well protected from the public; on the other hand, when some dispute occurs in emergency cases, it can also be effectively traced by the authority. The technique of pseudonyms has been widely adopted to achieve this target, but the periodically updated pseudonyms and certificates lead to intolerable computational cost for resource-constrained IoT nodes. More seriously, it cannot resist the physically dynamic tracing attack we identified for location privacy.

Location Privacy: Location privacy seems especially critical in IoTs, since the frequently exposed location privacy would disclose the living habit of the IoT user. The widely adopted technique is to hide its location through pseudonyms. However, since the location information is not directly protected, it cannot resist the physically dynamic tracing attack. Specifically, a set of malicious IoT users in collusion can be dispatched to the positions where the target IoT user occasionally visited, to physically record sets of real identities of passing nodes during specific time periods by observation or traffic monitoring video, and further identify the target IoT user's real identity. If the adversary knows that the target node with pseudonym pi_d occasionally visits n locations $Loc_1, Loc_2, ..., Loc_n$, n sets of nodes' real identities passing by these n locations $Veh_1, Veh_2, ..., Veh_n$ can be observed. The intersection would definitely reveal the target node's real identity and its private activities in other regions.

Node Compromise Attack: Node compromise attack means the adversary extracts from the resource-constrained IoT devices all the private information including the secret key used to encrypt the packets, the private key to generate signatures, and so on, and then reprograms or replaces the IoT devices with malicious ones under the control of the adversary. The target-oriented compromise attack means an adversary with global monitoring ability would select the IoT node holding more packets as the compromise target by watching the traffic flow around all nodes in IoT. Therefore, from one single compromise, it is likely that the adversary obtains more packets for recovering the original message or impeding its successful delivery by interruption.

Layer Removing/Adding Attack: The layer removing attack occurs when a group of selfish IoT users remove all the forwarding layers between them to maximize their rewarded credits by reducing the number of intermediate transmitters sharing the reward. On the contrary, the layer adding attack means colluding IoT users maliciously detour the packet forwarding path between them for increased credits by increasing the total obtainable utility.

Forward and Backward Security: Due to the mobility and dynamic social group formulation in IoT, it is necessary to achieve forward and backward security. The former means that newly joined IoT users can only decipher the encrypted messages received after but not before they join the cluster; while the latter means that revoked IoT users can only decipher the encrypted messages before but not after leaving.

Semi-Trusted and/or Malicious Cloud Security: For the convergence of the cloud with IoT, the security and privacy requirements for the cloud should be especially considered. The semi-trusted model means that the cloud would faithfully comply with the protocol specification, but try its best to extract secret information from the interactions with IoT users; while the malicious model means tht the adversary can arbitrarily destroy the protocol execution. Therefore, for outsourced computation, the following three security targets should be achieved:

- Input privacy: The data owner's individual inputs should be well protected even from collusion between the cloud and authorized data receivers.
- Output privacy: The computation result should only be successfully deciphered by authorized data receivers.
- Function privacy: The underlying function must be well protected from even the collusion of the cloud and malicious IoT users.

Table 2 demonstrates the main security and privacy threats in cloud-based IoT with the corresponding countermeasures.

Security threats	Countermeasure
Identity privacy	Pseudonym [4, 5, 9], group signature [5], connection anonymization [7, 13]
Location privacy	Pseudonym [4, 5, 9], one-way trapdoor permutation [6, 10]
Node compromise attack	Secret sharing [8, 10, 14], game theory [7], population dynamic model [10]
Layer removing/adding attack	Packet transmitting witness [9, 10, 13], aggregated transmission evidence [10]
Forward and backward security	Cryptographic one-way hash chain [4, 5]
Semi-trusted/malicious cloud security	(Fully) homomorphic encryption [11], zero knowledge proof [15]

Table 2. A taxonomy of main security threats in cloud-based IoT.

Secure Packet Forwarding in Cloud-Based IoT

We mainly focus on secure packet forwarding in cloud-based IoT DTNs, especially the techniques to address the kinds of attacks w.r.t. the bundle delivery, such as fairness for obtaining interest from transmitting packets, free riding attack, layer removing/adding attack, and node compromise attack identified earlier.

A secure credit-based incentive scheme, SMART, was presented to stimulate packet forwarding collaboration among DTN nodes [9]. Different from SMART, Lu *et al.* devised a secure and practical incentive protocol Pi addressing the fairness of charging and rewarding for packet delivery cooperation by adding some incentive on each bundle. Unfortunately, the existing work [9, 13] merely considered the outsider threats, leaving the target-oriented node compromise attack untouched. Consideration of the incentive schemes for multiple-copy algorithms is required to resist a single node compromise leading to the original message failing to be recovered. More significantly, the problem of layer adding collusion attack cannot be well addressed by either solution [9, 13].

To tackle the issue of compromise, by designing a modified model of population dynamics, a new threshold credit-based incentive mechanism, TCBI [10], is proposed in cloud-based IoT DTNs to efficiently resist node compromise attacks, stimulate packet transmission cooperation, optimize IoT users' utility, and achieve fairness among IoT users.

To resist layer adding attack, an outsourced aggregated transmission evidence generation algorithm is proposed by devising a new technique of secure outsourced data aggregation without public key homomorphic encryption. The sketch of the construction can be described as follows. First, each roadside unit (RSU) L encodes a randomness R using the one-way trapdoor permutation f, which is further adopted as the symmetric key to encrypt the individual velocities of all mobile IoT users passing by using an appropriately selected symmetric homomorphic mapping (SHM) instead of traditional public key homomorphic encryption. Then the cloud computes the aggregated velocity in the ciphertext domain and transmits the encrypted result to an AC, which can successfully decipher it as the aggregated packet transmission evidence by using secret key sk_f. Each mobile IoT node's velocity privacy is well protected by a blinding factor r_i added to SHM, and the layer adding attack is well resisted by the packet transmission evidence. It is noted that, different from the existing work exploiting public key homomorphic encryption to realize secure outsourced data aggregation, any public key encryption can be utilized only once in TCBI to achieve privacy preservation for n inputs on the resource-constrained IoT users' end, where both the computational and communication costs are dramatically saved. For simulation, ElGamal encryption is adopted to implement the one-way trapdoor permutation in the proposed TCBI. Figures 2a and 2b demonstrate the advantages of the proposed TCBI in computational cost and communication cost over the existing work (i.e., SMART [9]) exploiting Paillier's homomorphic encryption [11] as the primitive.

Privacy-Preserving Authentication in Cloud-Based IoT

For privacy-preserving authentication, we mainly focus on two aspects, the identity/location privacy protection and lightweight authentication solutions in cloud-based IoT.

Conditional identity privacy is traditionally achieved by a group signature [5]; however, the public key infrastructure (PKI) leads to the verification algorithm being inefficient and intolerable for the resource-constrained IoT devices due to the additional verification cost for the sender's public key certificate. To improve the efficiency, the pseudonym technique was proposed: Each IoT user is initialized with an anonymous public and secret key pair (PK_i, SK_i) in the registration phase, where the associated anonymous certificate is $Cert_i$ w.r.t. its pseudonym psm_i. The registration authority privately keeps a tuple composed of the IoT user's real identity and its pseudonym, and reveals this relationship when some disrup-

5

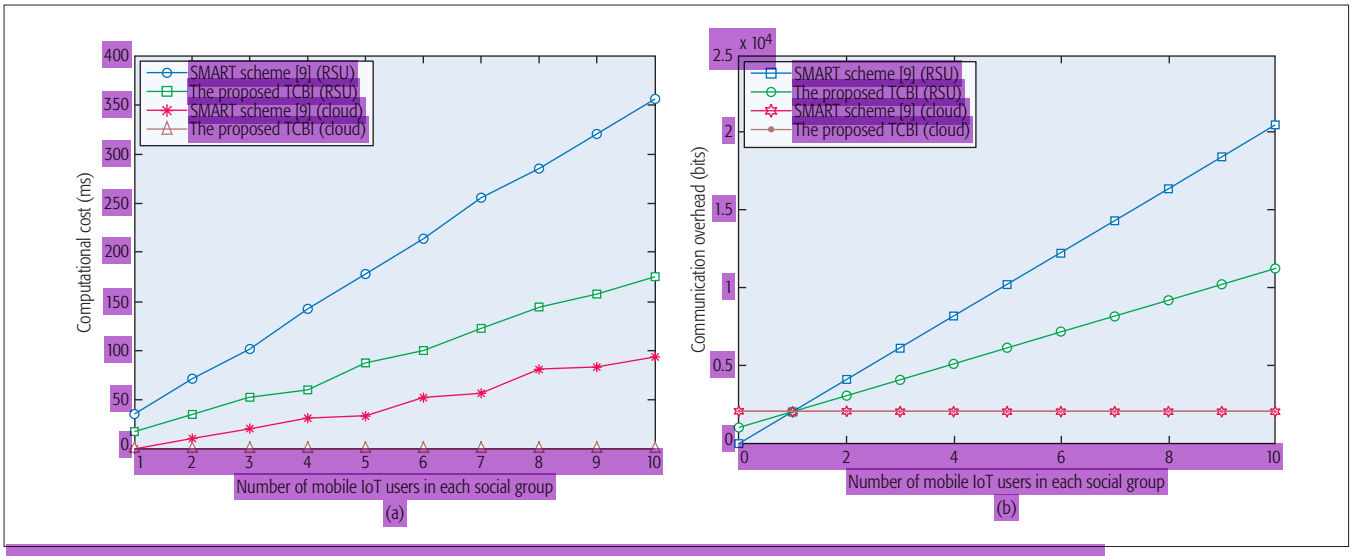

Figure 2. Efficiency comparison between SMART [9] and TCBI: a) computational cost; b) communication cost.

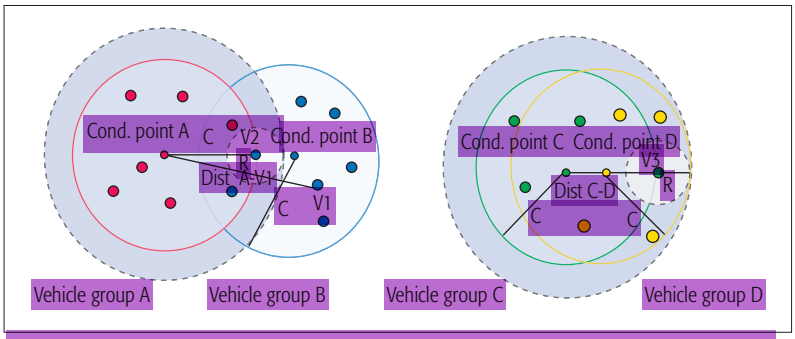

Figure 3. LBS content filtering mechanism with dynamic social group formulation in cloud-based IoT.

tion occurs. Each pair of keys has a short lifetime, which can be updated periodically to protect the IoT user's real identity and driving route from exposure. However, the frequent pseudonym updating would lead to intolerably high complexity on the resource-constrained IoT user's end.

X. Lin *et al.* proposed a timed efficient and secure communication (TSVC) scheme with privacy preservation in vehicular IoT [4]. By utilizing the techniques of hash chain and message authentication code, it aimed to minimize both the signature generation and verification overhead on the vehicle's side without compromising the underlying security and privacy requirements. However, the release delay of the private authentication key led to the construction only being appropriate for regular traffic events predefined in each time period. To overcome these shortcomings, Lin *et al.* proposed an efficient cooperative message authentication, also in vehicular IoT [5]. It minimized redundant authentication efforts from the receiver's aspect in that each message is verified by a single vehicle user, which reports afterward the verification result in its neighborhood. Unfortunately, the duplicate/redundant messages collected by vehicles passing the same road sections have not been reduced and still occupy a great deal of redundant bandwidth. More significantly, the intervention of an online trusted authority (TA) for token generation incurred considerable overhead.

Sen suggested privacy preserving authentication to verify the authenticity of the messages disseminated by IoT users by exploiting the technique of secure multiparty computation [7]. Roman *et al.* proposed a key management system for sensor networks in the context of IoT [8] to achieve both the forward and backward secrecy while IoT users join and/or are revoked from their current communication group. Recently, an efficient privacy-preserving relay filtering scheme, PReFilter, was proposed for DTNs in vehicular IoT communications [13]. It avoided junk packet delivery through setting and distributing an interest policy by message receivers for their friends, but still did not delete the redundant packets from the source. More seriously, all the constructions presented above cannot resist the physically dynamic tracking attack we identified in the multiple-pseudonym technique.

To address the challenging security issue, an efficient privacy-preserving authentication scheme SAVE for location-based service (LBS) in cloud-based IoT is proposed. Different from the existing work [5] which saved the verification cost from the receiver's view, an efficient privacy-preserving LBS bundle filtering mechanism with dynamic social group formulation is novelly designed from the sender's aspect to simultaneously prevent duplicate LBS contents from aggregation.

Let K, C, R, and $Dist_{x,y}$ be the number of independent IoT social groups, the maximum communication range between mobile IoT users, the IoT user's LBS content sensing range, and the distance between x and y, respectively, where x, y refer to either the IoT user's location or the condensing point (group center) position. Figure 3 shows the dynamic social group formulation in cloud-based IoT. There are four social groups, A, B, C, and D, denoted by red, blue, green, and yellow circles, respectively, with their own IoT users and condensing points at the group centers. From the left of Fig. 3, it is observed that IoT user V_2 belonging to social group B is located at the edge of social group A with $Dist_{V_2,CP_A} = C$. Additionally, the LBS content sensing domain of V_2 represented by the dashed circle with center

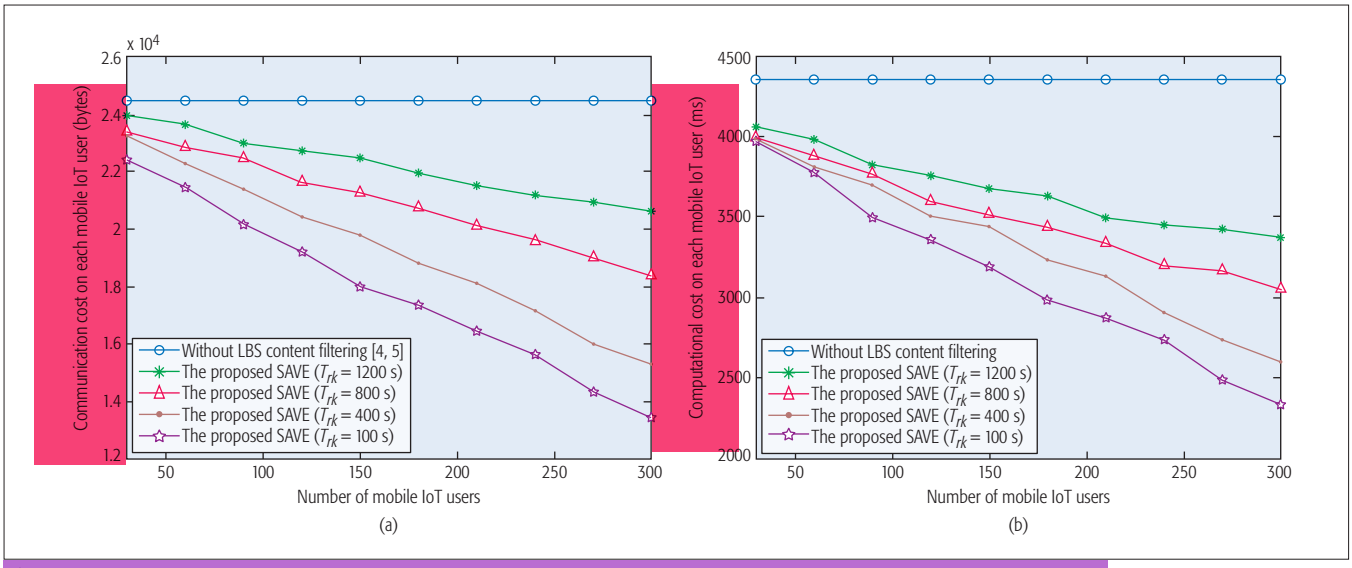

Figure 4. Efficiency of LBS content filtering mechanism in SAVE: a) communication cost; b) computational cost.

V_2 and radius R is just included in the LBS content sensing domain of IoT users belonging to group A represented by the dashed circle with center A and radius $C + R$. In other words, $Dist_{V_2,CP_A} \leq C$ means the LBS content collected by V_2 is invalid to social group A, since it overlaps the LBS content collected by mobile IoT users in group A, becomes redundant, and should be efficiently filtered at the sender V_2's aspect and prevented from further aggregation and dissemination in social group A.

From the right of Fig. 3, we focus on all the IoT users belonging to group C and located at the edge of group C (i.e., IoT user V_3 in Fig. 3). The LBS content sensing domain of IoT users in group C represented by the dashed circle with center C and radius $C + R$ just includes the domain of social group D when $Dist_{CP_C,CP_D} = C - (C - R) = R$. Therefore, $Dist_{CP_C,CP_D} \leq R$ means social groups C and D are required to be merged into a new one, since the LBS contents collected by them are extremely redundant, and all the LBS content collected by group D should be prevented from aggregation in group C to save both computational and communication costs on resource-constrained IoT users.

On the other hand, the physically dynamic tracing attack can be prevented to achieve two levels of location privacy. Location privacy level I means that each IoT user's private location can only be obtained for the LBS system at the network initialization phase and in the scenario of disputes, but not for other unauthorized IoT users. It can be achieved by the new technique of efficient privacy-preserving data aggregation presented earlier. Only the LBS system holding secret key sk_f can successfully decipher the authentic distances and allocate each IoT user to the corresponding group where the distance between the IoT user and the selected group center is the shortest.

Location privacy level II must be achieved in the efficient privacy-preserving LBS bundle filtering phase. It means that only the distance comparison result for deciding duplicate/redundant LBS contents, but not each IoT user's private locations (driving route), can be obtained by unauthorized IoT users. Note that the distance comparison result between $Dist_{pid_i,CP_l}$ and C is the metric to decide whether the newly arrived message carried by IoT user pid_i is redundant to social group C with the condensing point CP_l. The privacy-preserving distance comparison can be realized by exploiting the technique of zero knowledge proof [15], where the real distance $Dist_{pid_i,CP_l}$ implying the position of IoT user pid_i would not be disclosed. To further guarantee data confidentiality, forward/backward security, and reduced communication overhead, the technique of self-healing group key distribution can be exploited to prevent the key establishment material from retransmission due to the packet loss from the mobility and short-range communication in cloud-based IoT. Figures 4a and 4b demonstrate the advantage of communication cost and computational cost on each IoT user in the proposed SAVE compared to the existing work [4, 5], reducing the authentication overhead from the receiver's aspect.

Conclusions and Open Research Issues

In this section, we conclude this article by identifying a series of challenging open research issues with convincing solution ideas.

1. The first problem is fine-grained ciphertext access control in cloud-based IoT. It is well known that LBS allows each mobile IoT user to obtain timely and useful responses from the server according to her/his query interest. Unfortunately, due to the "pay-per-use" manner of the LBS cloud server, only an IoT user entering the regions in which her/his corresponding LBS has been registered to the local server can successfully decipher the encrypted query responses. It is obviously observed that this problem can also be extended into the multiple dimension scenario and possesses wide applications in outer space security. Designing lightweight attribute-based encryption (ABE) [14] provides a convincing solution to this issue.

2. Besides data confidentiality, location privacy and query privacy for cloud-based IoT users in

3

Besides data confidentiality, location privacy and query privacy for cloud-based IoT users in LBS should also be well protected, since the moving rout exposure would reveal IoT users' living habits and the query privacy would disclose their private favorites.

LBS should also be well protected, since the moving route exposure would reveal IoT users' living habits, and the query privacy would disclose their private favorites. To address the challenging open problem, designing policy-hidden ABE exploiting the technique of a noninteractive proof system for bilinear groups [15] would give us a promising solution.

3. Our proposed efficient privacy preserving technique of one-way trapdoor permutation was only exploited for secure data aggregation from one single user. It is required to extend our proposed efficient privacy preserving technique to thwart the security and privacy threats in other types of cloud-based IoTs. For example, in smart grid IoT, it is also required to protect each user's real-time power usage from exposure while judging the peak/off-peak status by outsourced computing of the total power consumption of all power consumers in a specific region and comparing it to a predefined threshold. Therefore, how to extend our proposed new efficient privacy-preserving technique to achieve secure data aggregation from multiple users in other kinds of cloud-based IoT to meet their unique security requirements also considerably appeals to both the academia and the industry.

4. For the next generation mobile technologies such as 5G on IoT–cloud convergence, dramatically increasing batches of data are required to be processed with privacy preservation. Another interesting open research issue is privacy-preserving outsourced data mining in cloud-based IoT. For example in vehicular IoT, it is required for each vehicle user to monitor the real-time traffic conditions in its neighborhood, which can be exploited to infer the traffic status afterward (i.e., exploiting an appropriate curve fitting algorithm on the collected traffic data days before to forecast the traffic status during the same time period days after, or using the data hours before to infer the condition hours later in the same day) and recommend to corresponding vehicular users the most unobstructed route from source to destination. However, it is also required to protect the user's identity privacy and location privacy, guarantee the correctness of an outsourced mining result, and ensure that the result can only be accessed by authorized entities. Therefore, how to design verifiable outsourced data mining in the ciphertext domain becomes a challenging open problem.

5. For the security and privacy of cloud-based IoT w.r.t. big data, public key fully homomorphic encryption (FHE) undoubtedly suggests an alternative to generalized secure outsourced computation supporting both addition and multiplication operations in the ciphertext domain (i.e., not limited to secure data aggregation); however, to the best of our knowledge, despite great efforts on designing lightweight FHE, the huge volume of computational complexity still significantly impedes its wide application on resource-constrained users in cloud-based IoT. Fortunately, to construct a new generalized framework of lightweight secure outsourced computation by extending our proposed efficient privacy preserving data aggregation without public key homomorphic encryption would definitely contribute to the blooming of cloud-based IoT.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61373154, 61371083, 61632012, 61672239, and 61602180, in part by the NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization under Grant U1509219, and in part by the Natural Science Foundation of Shanghai under Grant 16ZR1409200.

References

[1] Z. Sheng *et al.*, "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, 2013, pp. 91–98.
[2] X. Li *et al.*, "Smart Community: An Internet of Things Application," *IEEE Commun. Mag.*, vol. 49, no. 11, 2011, pp. 68–75.
[3] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, 2011, pp. 51–58.
[4] X. Lin *et al.*, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, 2008, pp. 4987–98.
[5] X. Lin and X. Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 62, no. 7, 2013, pp. 3339–48.
[6] J. Zhou *et al.*, "4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in m-Healthcare Social Networks," *Info. Sciences*, vol. 314, 2015, pp. 255–76.
[7] J. Sen, "Privacy Preservation Technologies in Internet of Things," *Proc. Int'l. Conf. Emerging Trends in Mathematics, Technology, and Management*, 2011.
[8] R. Roman *et al.*, "Key Management Systems for Sensor Networks in the Context of the Internet of Things," *Computer & Electrical Engineering*, vol. 37, no. 2, 2011, pp. 147–59.
[9] H. Zhu *et al.*, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Trans. Vehic. Tech.*, vol. 58, no. 8, Oct. 2009, pp. 4628–39.
[10] J. Zhou *et al.*, "Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs," *IEEE Trans. Info. Forensics and Security*, vol. 10, no. 6, 2015 , pp. 1299–314.
[11] P. Paillier, "Public Key Cryptosystems Based on Composite Degree Residuosity Classes," *Eurocrypt '99*, pp. 223–38.
[12] Y. Saleem, F. Salim, and M. H. Rehmani, "Resource Management in Mobile Sink Based Wireless Sensor Networks through Cloud Computing," in *Resource Management in Mobile Computing Environments*, Springer-Verlag, vol. 3, 2014, pp. 439–59.
[13] R. Lu *et al.*, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, Apr. 2010, pp. 1483–92.
[14] J. Zhou *et al.*, "TR-MABE: White-Box Traceable and Revocable Multi-Authority Attribute-Based Encryption and Its Applications to Multi-Level Privacy-Preserving e-Heathcare Cloud Computing Systems," *IEEE INFOCOM 2015*.
[15] J. Groth and A. Sahiai, "Efficient Noninteractive Proof Systems for Bilinear Groups," *Advances in Cryptology®EUROCRYPT 2008*, Springer Berlin, 2008., pp. 415–32

Biographies

Jun Zhou (jzhou@sei.ecnu.edu.cn) received his Ph.D. degree in computer science from Shanghai Jiao Tong University (SJTU) and joined East China Normal University in 2015. His research interests mainly include fine-grained ciphertext access control and secure outsourced computation.

Zhenfu Cao [SM'10] (zfcao@sei.ecnu.edu.cn) received his B.Sc. degree in computer science and technology and his Ph.D. degree in mathematics from Harbin Institute of Technology, China, in 1983 and 1999, respectively. His research interests mainly include number theory, cryptography, and information security. Since 1981, he has had more than 400 academic papers published in Journals and conferences. He was promoted to associate professor in 1987, became a professor in 1991, and is currently a Distinguished Professor at East China Normal University. He also serves as a member of the expert panel of the National Nature Science Fund of China. He is actively involved in the academic community, serving as Committee/Co-Chair and Program Committee member for several international conferences: IEEE GLOBECOM (since 2008), IEEE ICC (since 2008), and others. He is the Associate Editor of *Computers and Security* (Elsevier) and *Security and Communication*

Networks (Wiley), an Editorial Board member of *Fundamenta Informaticae* (IOS) and *Peer-to-Peer Networking and Applications* (Springer-Verlag), and a Guest Editor of *Wireless Communications and Mobile Computing* (Wiley), *IEEE Transactions on Parallel and Distributed Systems*, and others. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, and the Special Allowance by the State Council in 2005, and was a corecipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. He is also the leader of the Asia 3 Foresight Program (61161140320) and the key project (61033014) of the National Natural Science Foundation of China.

XIAOLEI DONG (dongxiaolei@sei.ecnu.edu.cn) is a Distinguished Professor at East China Normal University. After her graduation with a doctorate degree from Harbin Institute of Technology, she pursued her postdoctoral study at in SJTU from September 2001 to July 2003. Then, in August 2003, she joined the Department of Computer Science and Engineering of SJTU. Her primary research interests include number theory, cryptography, and trusted computing. Since 1998, she has published more than 80 academic papers. As the first author, she has two textbooks published by Science Press and China Machine Press respectively. Her "Number Theory and Modern Cryptographic Algorithms" project won the first prize of the China University Science and Technology Award in 2002. Her "New Theory of Cryptography and Some Basic Problems" project won the second prize of the Shanghai Nature Science Award in 2007. Her "Formal Security Theory of Complex Cryptographic System and Applications" won the second prize of the Ministry of Education Natural Science Progress Award in 2008. Currently, she hosts a number of research projects supported by the National Basic Research Program of China (973 Program), the special funds on information security of the National Development and Reform Commission and National Natural Science Foundation of China, and more. She is an Associate Editor of *Security and Communication Networks* (Wiley).

ATHANASIOS V. VASILAKOS (th.vasilakos@gmail.com) is currently a visiting professor at the National Technical University of Athens, Greece. He has served or is serving as an Editor for many technical journals, such as *IEEE TNSM*, *IEEE TSMC-PART B*, *IEEE TITB*, *ACM TAAS*, and *IEEE JSAC* Special Issues in May 2009, and January and March 2011. He is Chairman of the Council of Computing of the European Alliances for Innovation.