ITU

FACULTY OF COMPUTER AND INFORMATICS

DEPARTMENT OF COMPUTER ENGINEERING

Computer Communications
Report of Paper:

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

Emre Özdil - 150120138
Güneş Yurdakul - 150140141
Gamze Akyol - 150140142

Internet of Things (IoT) is the network of physical objects equipped with electronics, software and sensors. Prevalence of IOT brought demands for massive volumes of data storage and processing. Because of the resource constraints of IOT devices, cloud is needed outsourced storage and computation, which brings many security and privacy threats. In this article, the network architecture of cloud-based IoT and unique security and privacy requirements for 5G mobile technologies on cloud-based IoT are presented. Additionally, the incorrectness of most prevailing work is identified. Moreover, a solution to solve the challenging issues of secure packet forwarding and efficient privacy preserving authentication is proposed which is a new efficient privacy preserving data collection without public key homomorphic encryption is proposed.

MOTIVATION

Cloud-based IOT can be classified into static and mobile. Mobile cloud-based IOT is a more challenging issue, which is the reason this paper's main focus is security and privacy issues of mobile cloud-based IoT. The recent improvements in next generation mobile technologies such as fifth generation (5G) on IoT–cloud convergence has provided new information and made easier to work on security and privacy issues which have not been dealt with for years. The motivation behind the paper can be categorized into two main issues. First is the secure packet forwarding, finding convincing solutions to this issue is extremely significant in order to avoid security gaps can be exposed during routing process such as layer removing/adding attack and the second is developing a solution which provides privacy-preserving lightweight authentication and reduces both the computational and communication cost, since periodically aggregating and broadcasting passing service information brings a serious computational overhead.

NETWORK ARCHITECTURE OF CLOUD-BASED IOT

Mutual communication with each device and with the cloud can be done using IoT devices. IoT devices are always resource constrained, and if storage of the IOT device is available, the IoT device uses the store-carry-and-forward method. Communication done in IoT devices all by moving IOT users. Mobile IOT users often bundle and share packets within the communication range. There is no guaranteed connection due to mobility and short-range communication.

SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED IOT

For cloud-based IoT, security threats are the main focus. The unique security and privacy needs in cloud-based IoT are identity privacy, location privacy, node compromise attack, layer removing/adding attack, forward and backward security. The real identity of user should be kept in secret for mobile IoT. Hiding location is important in IoT. Nickname is a widely used adopted technique to hide location. It is not protected directly. In order to save from node compromise attacks, IoT devices changes with malicious ones by opponent. Layer removing attack means IoT users roam the packet routing path in a malicious way, increasing the total obtainable utility. Forward and backward security is needed due to the mobility and dynamic social group formulation in IoT. Security targets that should be accomplished for outsourced computation are input privacy, output privacy and function privacy.

SECURE PACKET FORWARDING IN CLOUD-BASED IoT

In cloud-based IoT delay tolerant network (DTN), securing packet forwarding from attacks is the main focus. There are some mechanisms which ensures the security which are:

-SMART: This scheme is a secure credit-based incentive scheme and is presented to promote packet forwarding collaboration among DTN nodes [1]. Unlike SMART, Lu et. al. proposed a protocol named Pi which is a secure and practical incentive protocol. Protocol Pi is based on charging and rewarding for packet delivery cooperation. However, these works do not consider the outsider threats. Also, layer adding collusion attack cannot be solved either in SMART or Pi [1, 2].

-TCBI: This mechanism is a threshold credit-based incentive mechanism [3]. Using this mechanism, node compromise attacks are blocked effectively and equality between IoT users is provided. This mechanism also optimizes IoT users' utility. An outsourced aggregated transmission evidence generation algorithm is used to block layer adding attacks. It also saves computational and communication costs well.

Figure 2 shows the benefits of proposed TCBI upon SMART according to computational cost and communication cost.

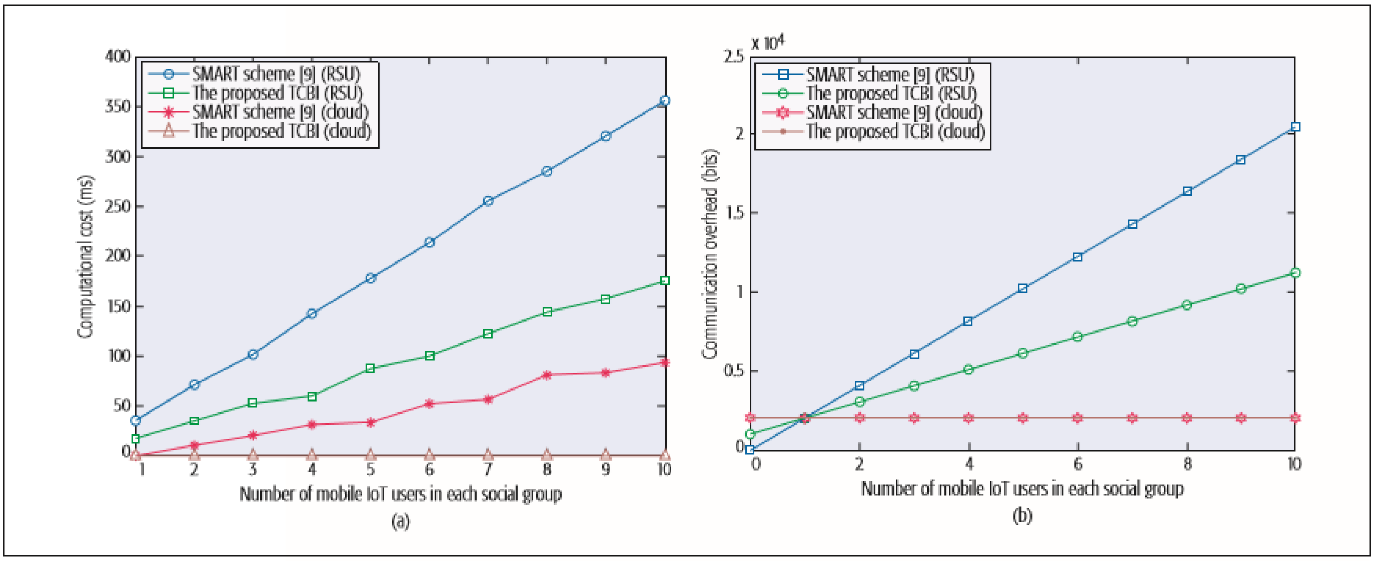

Figure 2. Efficiency comparison between SMART [9] and TCBI: a) computational cost; b) communication cost.

PRIVACY-PRESERVING AUTHENTICATION IN CLOUD-BASED IoT

This chapter focuses privacy in terms of identity/location privacy protection and lightweight authentication solutions in cloud-based IoT, both of them are important issues in privacy. **Public key infrastructure (PKI)** causes to the verification algorithm being inefficient and intolerable for the resource constrained IoT devices. Instead of this, **pseudonym technique** was proposed. For each user i, a public and secret key tuple is assigned (PK_i, SK_i). Key tuple is updated periodically to protect IoT user's real identity and driving route, but these updates can lead high complexity on the resource constrained IoT user's end.

A time efficient and secure communication scheme (TSVC) is proposed by Lin et. al. to do privacy protection in vehicular IoT. This scheme aimed to minimize both the signature generation and verification overhead and utilizes hash chain and message authentication code. 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 [4]. After that, Lin et. al. proposed an effective message authentication [5], but it cannot decrease the redundant or duplicate messages collected by a device using the same path, too.

There exist some other proposals except the solutions mentioned above, but they still did not solve the redundant packet problem. Moreover, these proposals presented above cannot survive from the physically dynamic tracking attack which is solved in multiple-pseudonym technique that is proposed in this article.

To solve the security issue, an efficient privacy preserving authentication scheme **SAVE** for location based service (LBS) in cloud-based IoT is proposed. This scheme is different from the previous work that saves verification cost from the receiver's view. This scheme proposes a novelty which is designed from the sender's aspect to simultaneously prevent duplicate LBS contents from aggregation. That is an efficient privacy-preserving LBS bundle filtering mechanism with dynamic social group formulation.

According to Figure 3 which is given below, LBS content filtering mechanism solves the redundant content problem, it deletes the redundant contents in IoT area. At the left part of the figure 3, V2 is an edge node, so there exists redundancy at this point. LBS content filtering mechanism solves this redundancy. At the right part of the figure 3, the vehicle groups are overlapping, so the groups are merged with each other to delete duplicate data.

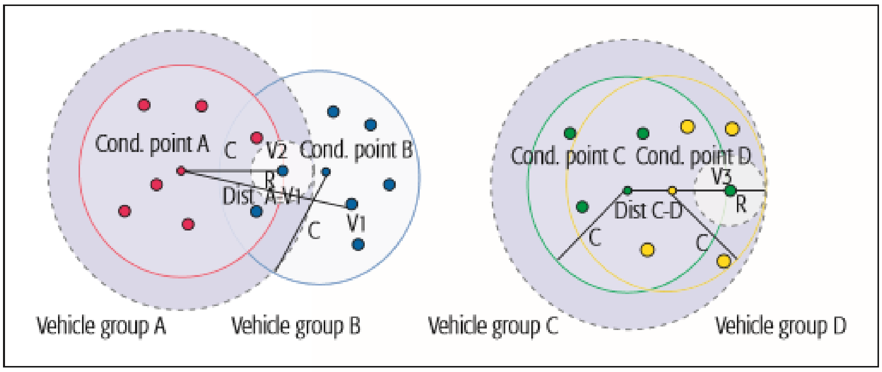

Figure 3. LBS content filtering mechanism with dynamic social group formulation in cloud-based IoT.

Besides, physically dynamic tracing attack also can be prevented with the SAVE scheme with two-levels of location privacy. At location privacy level 1, each IoT user's location is achieved by LBS system, but the IoT users cannot obtain each other's private location. At location privacy level 2, only result of distance comparisons can be achieved by IoT users, but the users still cannot obtain each other's exact location.

Figure 4 shows that the efficiency of the SAVE compared with existing mechanisms:

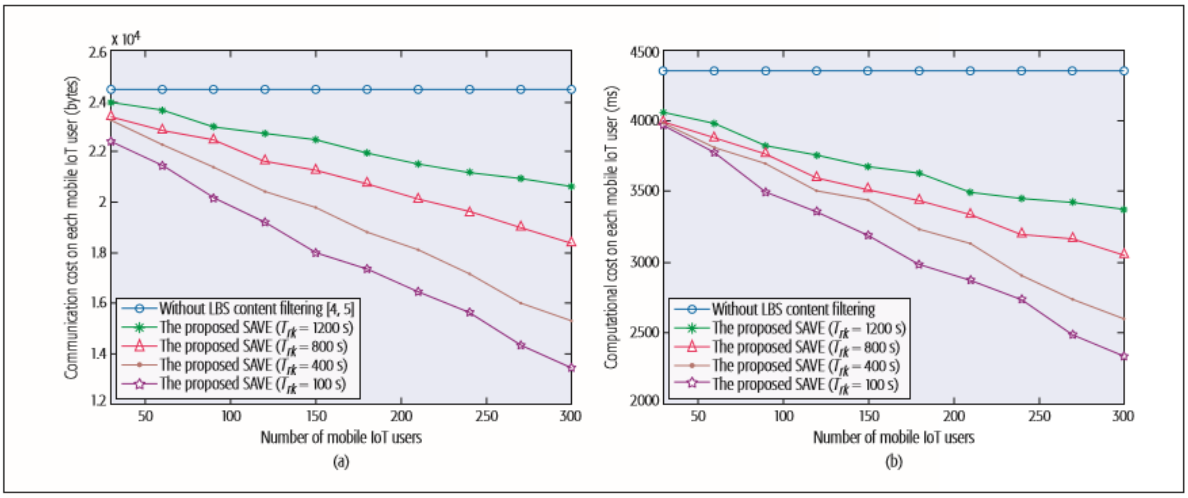

Figure 4. Efficiency of LBS content filtering mechanism in SAVE: a) communication cost; b) computational cost.

CONCLUSIONS AND OPEN RESEARCH ISSUES

In the conclusion part of the paper, five challenging open research issues for further research and corresponding convincing solutions are stated. The first issue is fine-grained cipher- text access control in cloud-based IoT and stated solution to this issue is designing a lightweight attribute-based encryption (ABE) [6]. Second issue is protection of location and query information of cloud-based IoT users, which can be solved by designing policy-hidden ABE exploiting the technique of a non-interactive proof system for bilinear groups [7]. Thirdly, the already proposed efficient privacy preserving technique in the previous sections was only exploited for secure data collection from single user, therefore extending proposed method is an open research issue. The fourth proposed research issue is privacy preserving outsourced data mining in cloud-based IoT. The last one is to extend the proposed efficient privacy preserving data aggregation method and construct a new framework without public key homomorphic encryption.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[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.*, "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*.

[7] J. Groth and A. Sahiai, "Efficient Noninteractive Proof Systems for Bilinear Groups," *Advances in Cryptology®EUROC- RYPT 2008*, Springer Berlin, 2008., pp. 415–32.