International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Homomorphic Encryption & A Novel Key Management Technique to Support Data Aggregation in Mobile Sensing

Farhat Afshan[1], Shameem Akther[2]

[1&2]Department Of Computer Science and Engineeing,
[1&2]Visvesvaraya Technological University
[1]Master Of Technology, [2]Associate Professor
[1&2]Khaja Bamda Nawaz College of Engineering Gulbarga, Karnataka, India

Abstract: ***The proliferation and ever-increasing capabilities of mobile devices such as smart phones give rise to a variety of mobile sensing applications. This paper studies how an untrusted aggregator in mobile sensing can periodically obtain desired statistics over the data contributed by multiple mobile users, without compromising the privacy of each user. Although there are some existing works in this area, they either require bidirectional communications between the aggregator and mobile users in every aggregation period, or have high-computation overhead and cannot support large plaintext spaces. Also, they do not consider the Min aggregate, which is quite useful in mobile sensing. To address these problems, we propose an efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique to support large plaintext space. We also extend the sum aggregation protocol to obtain the Min aggregate of time-series data. To deal with dynamic joins and leaves of mobile users, we propose a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave. Evaluations show that our protocols are orders of magnitude faster than existing solutions, and it has much lower communication overhead.***

Keyword: Mobile sensing, Privacy, data aggregation

1. Introduction

Mobile devices such as smart phones are gaining popularity and are rapidly becoming the central computer and communication device in people's lives. Most smart phones consist of embedded sensor such as camera, microphone, GPS accelerometer, ambient light and so on. The data generated by this sensor provide opportunities to make sophisticated inferences about not only people but also surroundings. This enables various mobile sensing applications such as environmental monitoring, traffic monitoring, healthcare and so on an example for health care is that the average amount of daily exercise done by a person can be measure by motion sensors. In many scenarios aggregation statistics needs to be computed the data that has been contributed by the multiple mobile users.

Although aggregation statistics computed from time series data are very useful in many scenarios, the data from the user are privacy sensitive and users do not trust any single third party aggregator to see their data values. For instance, to monitor the propagation of new flu, the aggregator will count the number of users infected by the flu.

Most previous works on sensor data aggregation assume a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Several recent works consider the aggregation of time-series data in the presence of an untrusted aggregator. Rastogi and Nath use threshold Paillier cryptosystem to build such an encryption scheme. To decrypt the sum, their scheme needs an extra round of interaction between the aggregator and all users in every aggregation period, which means high communication cost and long delay. Moreover, it requires all users to be online until decryption is completed, which may not be practical in many mobile sensing scenarios due to user mobility and the heterogeneity of user connectivity. Rieffel et.al. propose a construction that does not require bidirectional Communications between the aggregator and the users, but it has high computation and storage cost to deal with collusions in a large system. Shi et al also propose a construction for sum aggregation, does not need the extra round of interaction. However, the decryption in their construction needs to traverse the possible plaintext space of the aggregated value, which is very expensive for a large system with large plaintext space.

In mobile sensing, the plaintext space of some application can be large. For example carbondioxide levels can range from 350 ppm outdoors to over 10, 000 ppm in industrial workplace. Hence, in applications that continuously monitor the carbon dioxide levels that people are exposed to in their daily life, the plaintext space can reach 104. Under this plaintext space, for a large system with one million users, the construction requires 30 seconds to decrypt the sum on amodern64-bit desktop PC. Its computation overhead is too high for an aggregator to run real-time monitoring applications with short aggregation intervals and to collect multiple aggregate statistics simultaneously. Moreover, none of these existing schemes considers the Min aggregate of time-series data, which is also important in many mobile sensing applications.

In this work we propose a new protocol for mobile sensing to obtain the sum aggregate of time-series data in the presence of an untrusted aggregator. Our protocol employs an additive Homomorphic encryption and a novel key

Licensed Under Creative Commons Attribution CC BY

management scheme based on efficient HMAC to ensure that the aggregator can only obtain the sum of all users' data, without knowing individual user's data or intermediate result. In our protocol, each user only needs to compute a very small number of HMACs to encrypt her data (decrypt the sum). Hence, the computation cost is very low, and the protocol can scale to large systems with large plaintext spaces, resource constrained devices, and high aggregation loads. Anothernice property of our protocol is that it only requires a single round of user-to-aggregator communication. Based on the sum aggregation protocol, we propose a protocol to obtain the Min aggregate. To our best knowledge, this is the first privacy-preserving solution to obtain the Min of time-series data in mobile sensing with just one round of user-to-aggregator communication. Our protocols for Sum and Min can be easily adapted to derive many other aggregate statistics such as Count, Average, and Max.

2. Related Work

N.D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A.Doryab, E. Berke, T. Choudhury, and A. Campbell "Bewell: A Smartphone Application to Monitor, Model and Promote Wellbeing, "Proc. Fifth Int'l ICST Conf. Pervasive Computing Technologies for Healthcare, 2011. A key challenge for mobile health is to develop new technology that can assist individuals in maintaining a healthy lifestyle by keeping track of their everyday behaviors. Smartphones embedded with a wide variety of sensors are enabling a new generation of personal health applications that can actively monitor, model and promote wellbeing. Automated wellbeing tracking systems available so far have focused on physical fitness and sleep and often require external non-phone based sensors. In this work, we take a step towards a more comprehensive smartphone based system that can track activities that impact physical, social, and mental wellbeing namely, sleep, physical activity, and social interactions and provides intelligent feedback to promote better health. We present the design, implementation and evaluation of BeWell, an automated wellbeing app for the Android smartphones and demonstrate its feasibility in monitoring multi-dimensional wellbeing. By providing a more complete picture of health, BeWell has the potential to empower individuals to improve their overall wellbeing and identify any early signs of decline.

Z. Zhu and G. Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services," Proc. IEEE INFOCOM, 2011. Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. APPLAUS can be implemented with the existing network infrastructure and the current mobile devices, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that our scheme, besides providing location proofs effectively, can significantly preserve the source location privacy.

Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012. In disruption tolerant networks (DTNs), selfish or malicious nodes may drop received packets. Such routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been proposed to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes. To address the problem, we propose a distributed scheme to detect packet dropping in DTNs. In our scheme, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. We also propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior.

K. Fall "A delay-tolerant network architecture for challenged internets", Proc. SIGCOMM, pp.27 -34 2003. Increasingly, network applications must communicate with counterparts across disparate networking environments characterized by significantly different sets of physical and operational constraints; wide variations in transmission latency are particularly troublesome. The proposed Interplanetary Internet, which must encompass both terrestrial and interplanetary links, is an extreme case. An architecture based on a "least common denominator" protocol that can operate successfully and (where required) reliably in multiple disparate environments would simplify the development and deployment of such applications. The Internet protocols are ill suited for this purpose. We identify three fundamental principles that would underlie a delay-tolerant networking (DTN) architecture and describe the main structural elements of that architecture, centered on a new end-to-end overlay network protocol called Bundling. We also examine Internet infrastructure adaptations that might yield comparable performance but conclude that the simplicity of the DTN architecture promises easier deployment and extension.

Licensed Under Creative Commons Attribution CC BY

W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", Proc. IEEE INFOCOM, pp.3119 -3127 2011. Data dissemination is useful for many applications of Disruption Tolerant Networks (DTNs). Current data dissemination schemes are generally network-centric ignoring user interests. In this paper, we propose a novel approach for user-centric data dissemination in DTNs, which considers satisfying user interests and maximizes the cost-effectiveness of data dissemination. Our approach is based on a social centrality metric, which considers the social contact patterns and interests of mobile users simultaneously, and thus ensures effective relay selection. The performance of our approach is evaluated from both theoretical and experimental perspectives. By formal analysis, we show the lower bound on the cost-effectiveness of data dissemination, and analytically investigate the tradeoff between the effectiveness of relay selection and the overhead of maintaining network information. By trace-driven simulations, we show that our approach achieves better cost-effectiveness than existing data dissemination schemes.

H. Yang, J. Shu, X. Meng and S. Lu "Scan: Self-organized network-layer security in mobile ad hoc networks", IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp.261 -273 2006. Protecting the network layer from malicious attacks is an important yet challenging security issue in mobile ad hoc networks. In this paper, we describe SCAN, a unified network-layer security solution for such network that protects both, routing and data forwarding operations through the same reactive approach. SCAN does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to the malicious nodes. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. In essence, SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. Through both analysis and simulation results, we demonstrate the effectiveness of SCAN even in a highly mobile and hostile environment.

3. Existing System

In the existing system the sensor data aggregation assumes a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Several recent works consider the aggregation of time series data in the presence of an untrusted aggregator. To protect user privacy they design encryption scheme in which the aggregator can only decrypt the sum of all users' data but nothing else. Use threshold paillier cryptosystem to build such an encryption scheme. To decrypt the sum, their scheme needs an extra round of interaction between the aggregator and all users in every aggregation period, which means high communication cost and long delay. Moreover it requires user to be online until decryption is completed, which may not be practical in many mobile sensing scenario due to user mobility and the heterogeneity of user connectivity.

4. Proposed System

In this work we make use of mobile users and the aggregator and we propose a new privacy preserving protocol to to obtain the sum aggregate of time series the protocol utilizes additive homomorphic encryption and a novel key management technique to perform efficient aggregation and novel key management technique is based on HMAC. We consider how an untrusted data aggregator cannot obtain the desired statistics over multiple participants 'data, without compromising each individual's privacy. We propose a construction that allows a group of participants to periodically upload encrypted values to a data aggregator, such that the aggregator is able to compute the sum of all participants' values in every time period The protocols implemented in our work for the protection of users inputs. The sum aggregation protocol does not expose the derivative data of any user, the aggregator cannot know the data value of it more secure of any specific user. One of the protocol is sum aggregation where the sum of the users inputs are calculated for each aggregation period. Based on the sum aggregation protocol we propose a protocol to obtain the min aggregation where the minimum value is provided based upon the inputs of user. A nice property of these protocols is that it requires a single round of user to aggregator communication. The first privacy preserving solution to obtain the time-series data in mobile sensing is the min aggregate. It needs one round of communication between the user and the aggregator. The sum and min aggregate protocols can easily be adapted to derive aggregate statistics such as count, average and max. The users may frequently join and leave in mobile sensing, so a scheme is employed to reduce the communication cost and the security is improved. The scheme is key generation where each user is allocated with the respective keys. The dynamic join and leave of each user also ensures the secrecy of the aggregate statistics. We also propose a scheme that employs the redundancy in security to reduce the communication cost of dealing with dynamic joins and leaves. In each time period, a mobile user sends her encrypted data to the aggregator via Wife, 3G or other available access networks. No peer-to-peer communication is required among mobile users, since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons. The efficient technique to achieve user's privacy is enhanced with the algorithms such as homomorphic encryption. The dynamic join of user and their leaving in online is effectively incremented with the users inputs. In the existing work there was a bidirectional communication between the mobile users and the aggregator by making use of homomorphic encryption algorithm and the novel key management technique that is based on HMAC (Hash Message Authentication Code) to achieve privacy preserving sum aggregation there is no two way communication between the mobile users and the aggregator and our scheme has much lower communication overhead then existing work.

Licensed Under Creative Commons Attribution CC BY

5. System Architecture

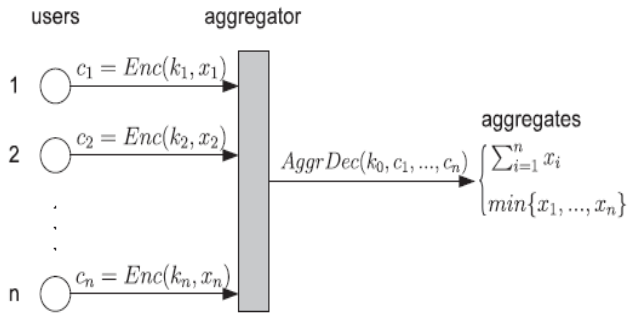

Figure 1: Our system model of time-series data aggregation

In figure 1, shows the mobile users and the aggregator there are multiple number of the mobile users as shown in the fig1 the aggregator wishes to get the aggregate statistics of multiple mobile users the time periods are numbered as 1, 2, 3 and so on. In every time period, each user i encrypts her data xi with ki and sends the derived cipher text to the aggregator. From the cipher texts, the aggregator decrypt the needed aggregate statistics using her or his aggregating capability k0.Two types of aggregate statistics are considered in this work, which are Sum and Min. Sum is defined as the sum of all users' data and Min is defined as the minimum value of the users' data. From Sum and Min, many other aggregate statistics can be easily derived, such as Count (i.e., the number of users that satisfy certain predicate), Average (which is derivable from sum, count). In each time period, a mobile user sends her encrypted data to the aggregator via Wi-Fi, 3G or other available access networks. No peer-to-peer communication is required among mobile users, since such communication is non-trivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons. Mobile users sends the data to the aggregator where the aggregator aggregate the data the data that has been contributed by the multiple participants mobile user sends the encrypted data to the aggregator and the aggregator decrypt the data. From the fig 1 we see that there is no bidirectional communication between the mobile users and the aggregator our work focuses on to protect the user data against an untrusted aggregator. We assume a key dealer that issues proper keys to the aggregator and users via a secure channel. For now, the key dealer is assumed to be trusted, and this assumption is relaxed. Our goal is to guarantee the privacy of each user's data against the untrusted aggregator, i.e., the aggregator obtains the aggregate statistics without knowing any individual user's data. We achieve this goal through protecting each user's data content with an encryption scheme, but not through providing source anonymity. Also, we guarantee that any party without an appropriate aggregator capability obtains nothing.

Algorithm used in our system:

Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result, when decrypted matches the result of operation performed on the plaintext. Homomorphic encryption is the encryption scheme there are two types of encryption scheme that is symmetric encryption scheme and asymmetric encryption scheme. The protection of mobile agents by homomorphic encryption can be used in two ways: (i) computing with encrypted functions and (ii) computing with encrypted data. Computation with encrypted functions is a special case of protection of mobile agents. In such scenarios, a secret function is publicly evaluated in such a way that the function remains secret. Using homomorphic cryptosystems the encrypted function can be evaluated which guarantees its privacy. Homomorphic schemes also work on encrypted data to compute publicly while maintaining the privacy of the secret data. By making use of this algorithm we can protect the user privacy against an untrusted aggregator. In secret sharing schemes, parties share a secret so that no individual party can reconstruct the secret form the information available to it. However, if some parties cooperate with each other, they may be able to reconstruct the secret. In this scenario, the homomorphic property implies that the composition of the shares of the secret is equivalent to the shares of the composition of the secrets. Homomorphic encryption would allow chaining together of different services, for example a chain of different services from different companies could calculate tax, currency exchange rate, shipping on a transaction without exposing unencrypted data to each of those services.

6. Results and Discussion

There are various techniques used in the table**:**

Threshold paillier cryptosystem	The previous work was on threshold paillier cryptosystem that was based on encryption scheme in which it make use of mobile users and the aggregator where there was an extra round of interaction between the mobile users and the aggregator and it causes high computation overhead & long delays problems
Homomorphic encryption & Novel key management technique	In our work we make use of homomorphic encryption algorithm and novel key management technique that is based on HMAC by making use of this there is no bidirectional communication between the mobile users and the aggregator and hence the users data is protected against the untrusted aggregator.

Licensed Under Creative Commons Attribution CC BY

In the existing work we cannot protect the user privacy against an untrusted aggregator and also we cannot obtain the sum of all users' data. There was a two way communication between the mobile users and the aggregator which leads to long delays. In our work there is unidirectional communication between the mobile users and the aggregator and hence we can protect the user's data and we can obtain the sum aggregation that is sum of all users' data by making use of homomorphic encryption algorithm and a novel key management technique.

7. Conclusion

To facilitate the collection of useful aggregate statistics in mobile sensing without leaking mobile users' privacy, we proposed a new privacy-preserving protocol to obtain the Sum aggregate of time-series data. The protocol utilizes additive homomorphic encryption and a novel, HMAC-based key management technique to perform extremely efficient aggregation. Implementation-based measurements show that operations at user and aggregator in our protocol are orders of magnitude faster than existing work. Thus, our protocol can be applied to a wide range of mobile sensing systems with various scales, plaintext spaces, aggregation loads, and resource constraints. Based on the Sum aggregation protocol, we also proposed two schemes to derive the Min aggregate of time-series data. One scheme can obtain the accurate Min, while the other one can obtain an approximate Min with provable error guarantee at much lower cost. To deal with dynamic joins and leaves, we proposed a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave.

References

[1] N.D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A.Doryab, E. Berke, T. Choudhury, and A. Campbell "Bewell: A Smartphone Application to Monitor, Model and Promote Wellbeing, "Proc. Fifth Int'l ICST Conf. Pervasive Computing Technologies for Healthcare, 2011

[2] Z. Zhu and G. Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services," Proc. IEEE INFOCOM, 2011.

[3] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012. [4] K. Fall "A delay-tolerant network architecture for challenged internets", Proc. SIGCOMM, pp.27 -34 2003

[4] W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", Proc. IEEE INFOCOM, pp.3119 -3127 2011.

[5] H. Yang, J. Shu, X. Meng and S. Lu "Scan: Self-organized network-layer security in mobile ad hoc networks", IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp.261 -273 2006

[6] K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan "An acknowledgment-based approach for the detection of routing misbehavior in MANETs", IEEE Trans. Mobile Comput., vol. 6, no. 5, pp.536 -550 2007

Licensed Under Creative Commons Attribution CC BY