Privacy Preserving: Slicer Based Scheme

Divya B Nair
PG Student
Department of Computer Science & Engineering
APJ Abdul Kalam Technological University, India

Jeena P Abraham
Assistant Professor
Department of Computer Science & Engineering
APJ Abdul Kalam Technological University, India

Abstract

Introduces privacy preserving scheme for participatory system for multimedia data. The main focus is to develop a security system for communication which provides privacy and quality preserving for participatory system with multimedia data using RSA and XOR encryption scheme. It is a coding based k-anonymous privacy preserving scheme. Which integrates a data coding technique and message transfer strategies? Maintaining high data quality, low communication and computation overhead.
Keywords: Data Exchange, Data Slicing, Privacy Preserving, X-OR

I. INTRODUCTION

Privacy Preserving for Participatory System (PS) is a web application system. The main focus is to develop a security system for communication which provides privacy and quality preserving for participatory system with multimedia data using RSA and XOR encryption scheme.Introduces privacy preserving scheme for participatory systems with multimedia data. It is a coding based k-anonymous privacy preserving scheme. However, the application of participatory system has a number of challenges. One of the major challenges is on privacy preservation. When a record sent to the service provider, is usually attached with spatio-temporal tags indicating the information of the data collected. However, a corrupt service provider may infer private information of the participants, such as identity, home and office addresses, traveling paths, as well as participants' habits and lifestyles, from the records. In turn, many users are reluctant to contribute their record if proper privacy preservation scheme is not applied. Without sufficient number of participants, participatory sensing applications cannot guarantee their quality of services at the expected level. Therefore, designing privacy preserving schemes for participatory system is highly important.

II. RELATED WORKS

A Slicing-Based K-Anonymous Privacy Preserving Scheme for participatory sensing system [8].With the popularity of mobile wireless devices with various kinds of sensing abilities, a new service paradigm named Participatory Sensing has emerged to provide users with brand new life experience. However, the wide application of participatory sensing has its own challenges, among which privacy preservation and multimedia data participatory sensing are two critical problems. Unfortunately, none of the existing works has fully solved the problem of privacy preserving participatory sensing with multimedia data.

Implementation of Cryptography For Privacy Preserving Data Mining [2],Privacy is one of the most important properties of an information system must satisfy, In which systems the need to share information among different, not trusted entities, the protection of sensible information has a relevant role. RSA is a strong encryption algorithm [5] that has stood a partial test of time. RSA implements a public-key cryptosystem that allows secure communications and "digital signatures", and its security rests in part on the difficulty of factoring large numbers. The authors urged anyone to attempt to break their code, whether by factorization techniques or otherwise, and nobody to date seems to have succeeded. This has in effect certified RSA, and will continue to assure its security for as long as it stands the test of time against such break-ins.

Encryption using XOR based Extended Key for Information Security – A Novel Approach [7], the explosive growth of information, places a high demand for Information Security. Information Security deals with securing the information from unauthorized access or misuse of information either intentionally or accidentally. Information may be represented in many forms like text, documents, audio, video, images or maps. The standard and widely used form is documents. The objective of our work is to secure information present in these documents especially in a shared environment like peer-to- peer environment. Using XOR operation to resolve the security issue by strengthening the confusion part and by using extended key characters for substitution.

Data Transfer over the Internet for Real Time Applications [3], a basic requirement in any successful application of a web-based system is efficient real-time processing and data transfer over the Internet. Efficient real time data exchange over the Internet plays a crucial role in the successful application of web-based systems. In this paper, a data transfer mechanism over the Internet is proposed for real time web based applications. The mechanism incorporates the eXtensible Markup Language (XML) and Hierarchical Data Format (HDF) to provide a flexible and efficient data format.In a significant number of real environments, real time web-based systems involve transferring and exchanging large amounts of numerical data over the Internet.

III. PROPOSED SYSTEM

Introduces privacy preserving scheme for participatory sensing with multimedia data. It is a coding based k-anonymous privacy preserving scheme. Which integrates a data coding technique and message transfer strategies? Maintaining high data quality, low communication and computation overhead. Many users are reluctant to contribute their record if proper privacy preservation scheme is not applied. SLICER, which is a coding, based k-anonymous privacy preserving scheme. A proper data slice exchanging strategy is applied, the contributor of each particular sensing record is hidden in a group of at least k participants. Here proposes a privacy preserving scheme for participatory system. Participants can share their data within a time bound. An XOR method is used to retrieve lost data. It reduces the processing time for large data resources.

Most users are not willing to join participatory applications, unless their sensitive information is well protected from both service provider and neighboring participants. The problem of privacy preserving in a semi-honest model, in which the adversary correctly follows the protocol specification, but attempts to learn additional information by analyzing the transcript of messages received during the execution .The attacks in the semi-honest model into two categories: external attack and internal attack. The external attack aims to obtain private information of participants by overhearing the message passing through the wireless communication network. Such attack can be prevented by end-to-end cryptographic schemes. Different from the external attack, designing a scheme to prevent the internal attack is much more challenging. The internal attack may come from two different kinds of entities, including the service provider and the participants.

Service provider's attack: The service provider has full access to the sensing records reported by the participants. It might infer considerable amount of sensitive information about the participants. In this work, we focus on protecting users' privacy against the service provider, while assuming that the service provider does not have other background or correlated information about participants. It is also important to consider the privacy protection of the content of multimedia data. Participants' attack: Participants may receive some records, when they serve as relays for other participants. Semi-honest participants might position themselves to some critical locations in order to collect sensitive information by pretending to be relays. In this work, we assume that the participants do not collude with the service provider, and there is no collusion among different participants.

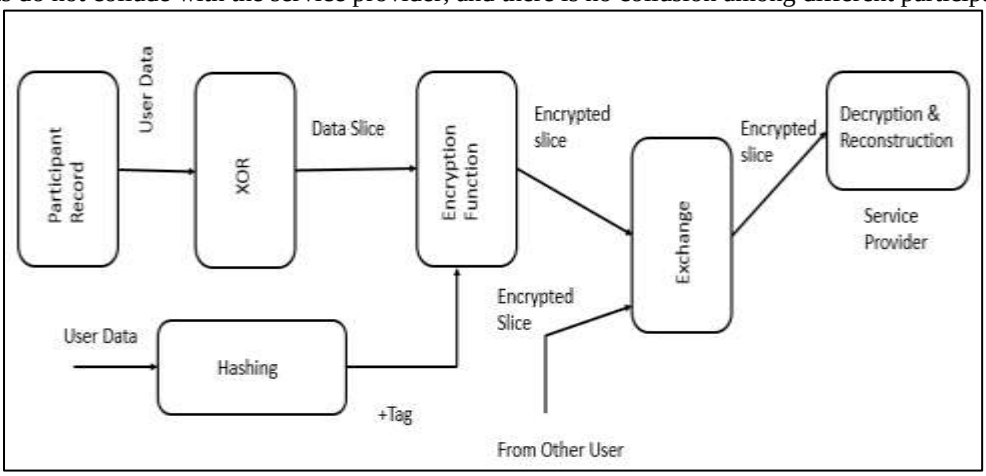

Fig. 1.1: System Architecture

The architecture diagram explains the privacy preserving system in detail. In which a registered user can send their data to the service provider. When a participant upload the data, then it can be sliced using an XOR method. The XOR method slice the recode to n number of slices. A hash function is performed to create a tag for each file, the tag will used to identify the slices in each record. Then the sliced data is transfer to an encryption function to encrypt the record .After the encryption function the encrypted record slices exchanged with the records of other participants in the privacy preserving system. Finally the encrypted data slices from the participants are received by the service provider. Then the service provider decrypt and reconstruct the original record.

IV. CONCLUSION

A coding-based privacy preserving scheme, namely SLICER, which is a k-anonymous privacy preserving scheme for participatory system with multimedia data. In this all multimedia data are split and encryption techniques performed and exchange the encrypted data between each users. SLICER integrates the techniques of slice transfer strategies, to achieve strong protection of participants' private information as well as high data quality and loss tolerance, with low computation and communication overhead. Design a coding based record coding scheme to encode each record into a number of data slices, each of which can be delivered to the service provider through the other participants or the record's generator herself.

REFERENCES

[1] Adi Armoni (2002), Data Security Management in Distributed Computer Systems, Informing Science Data Security, Volume 5 No 1.
[2] Anand Sharma, Vibha Ojha (2010), Implementation of Cryptography for Privacy Preserving Data Mining, International Journal of Database Management Systems (IJDMS) Volume.2 No.3.
[3] Cheng-Wei Dai, Shuang-Hua Yang, Roger Knott (2006), Data Transfer Over the Internet for Real Time Applications, International Journal of Automation and Computing Volume 4, 414-424.
[4] C. Cornelius (2008), AnonySense: Privacy-Aware People-Centric Sensing, 6th Int'l. Conf. Mobile Systems, Applications, and Services, 211–24.
[5] Evgeny Milanov (2009), The RSA Algorithm, Volume 3 June.
[6] Emiliano De Cristofaro (2013), Participatory Privacy: Enabling Privacy in Participatory Sensing, IEEE Network, January/February 2013.
[7] E. Anupriya, Sachin Soni (2013), Encryption using XOR based Extended Key for Information Security – A Novel Approach, International Journal on Computer Science and Engineering (IJCSE), February.
[8] Fudong Qiu, Fan Wu, Guihai Chen (2013), SLICER: A Slicing-Based K-Anonymous Privacy Preserving Scheme for Participatory Sensing, 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems.
[9] Himja Agrawal1, Prof. P. R. Badadapure (2016), A Survey Paper on Elliptic Curve Cryptography, International Research Journal of Engineering and Technology IRJET Volume: 03 Issue: 04.
[10] Haroon Shakirat Oluwatosin (2014), Client-Server Model, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1.
[11] Jing Shi, Rui Zhang, Yunzhong Liu, and Yanchao Zhang (2010), PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems, IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM
[12] P. Gilbert (2010), "Toward Trustworthy Mobile Sensing," 11 Wksp. Mobile Computing Systems and Applications, pp. 31–36.
[13] P. Senthil Vadivu, S. Nithya (2014), An Improved Privacy Preserving With Rsa And C5.0 Decision Tree Learning For Unrealized Datasets, International Journal of Science and Applied Information Technology ,Volume 3, No.1, January – February.
[14] R. Agrawal and R. Srikant (2000), Privacy-preserving data mining, In SIGMOD Conference, pages 439–450.
[15] R. L. Rivest, A. Shamir, and L. Adleman (1978), A Method for Obtaining Digital Signatures and Public- Key Cryptosystems Communications of the ACM Volume 21 February.