Smart Intelligent Computing and Communication Technology
V.D. Ambeth Kumar et al. (Eds.)

doi:10.3233/APC210014

A Reliable Cloud Based Framework for Large Scale Urban Sensing Systems

K.R.Jansi[a,1], G.K.Sandhia[b] and Dr.S.V.KasmirRaja[b]
[a,1]*Assistant Professor, Dept of CSE, SRM Institute of Science and Technology, Kattankulathur*
[b]*Research Supervisor, Dept of CSE, SRM Institute of Science and Technology, Kattankulathur*

Abstract: The rising usage of smartphones and sensing models in today's life induces the development of large scale urban sensing networks in communication concepts. With the efficient implementation of people centric mobility models, the personal communication devices of people are acting as the sensor nodes that are capable of sensing the human behaviours and participating in framing the smart protocol designs for smart cities. Without the involvement of mobile users or people, the new protocols for mobility management, traffic management, environmental sensing and other applications become futile. The proposed cloud based model improves the reliability and scalability of the system with its multiple cloud servers design. The single point of failure can be resisted since many cloud servers belonging to a provider is used. So the framework remains fault tolerant in the presence of any server attacks. A standard homomorphic based encryption scheme is used for providing data confidentiality and also data is transferred anonymously improving the privacy of the system. The data aggregation process is supported by the model protecting the user's privacy. The performance analysis for the proposed framework is done in terms of design goal analysis and computation cost analysis.

Keywords- cloud framework, reliable, urban sensing, fault resistance

1. Introduction

In the past decade of communication technology over sensor networking and computations has provided an inclination in the field of wireless networking and communications. The researchers have developed the most effective wireless sensor networking with collection of embedded devices with resource constraints. The networking model has been applied for some specified applications in the field of industries and scientific developments includes weather forecasting, forest monitoring,military applications and for some other preventive maintenance. However these issues and applications are significant, the present tininess and consequent preamble of sensor Networks into general electronic devices such as PDAs, mobiles

[1] K.R.Jansi,Dept of CSE, SRM Institute of Science and Technology, India;
Email: jansik@srmist.edu.in

and MP3 players, etc., has directed new trends of application prospects. Based on the appropriate architectural Framework of sensor platforms, the networks are influenced to solve issues on urban-scales or afford global data access to the common people. Simultaneously, the public are treated as individuals or in social groups can use this kind of networks for employing with some personal attention. With that note, a new technology has been developed as mobile people centric sensing. In the People Centric Sensing Networks (PCSN)[1], people based environmental sensing and acquisition of sensed data. Moreover, it can be defined as the combine mobility of people themselves that permits both observation coverage of huge public area with time and makes people as a curator of the device that observe required data about the life based patterns and communications [2]. This network can also be technically termed as opportunistic sensing networks that handle with events and communications between people.

2. Related works

This section narrates the existing works that are available in providing secured framework and also schemes on providing privacy during data aggregation in PCSN is discussed. Prisense [5] is the privacy preserving data aggregation model developed for people centric sensing networks. The model worked on the basis of data slicing and mixing method. Furthermore, the model used three strategies for node head selection, Random cover selection process, 1-hop method and h-hop method. Verifiable Privacy-preserving Aggregation (VPA) [6] worked on data slicing and data mixing process to handle the privacy of user provided data and for shared data integrity. VPA approach also performed both additive and non-additive functions of data aggregation. The VPA model was performed with several rounds with two way communications between the aggregation server and the sensors. This might process with higher transmission delays in the defined network. Also, when found a node failure or link failure, the model was not efficient to process with fault tolerance. Further, the model was not attacks resistive. The survey work presented in [7], [8] and [9] discussed about the adversaries and countermeasures for various attacks on urban sensing network. The attack models and mitigation techniques were discussed with effective data distribution strategies[11].

3. Framework

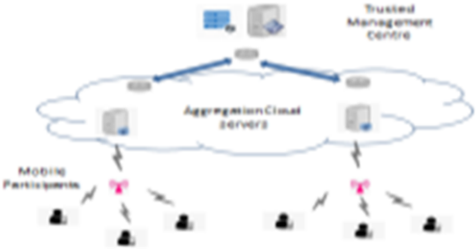

Figure 1. Reliable Framework for people centric sensing network

The system framework of the defined people centric sensing network is given in Figure 1. As mentioned in the Figure, the framework of the defined network contains trusted management centre, Aggregation cloud servers and mobile participants. The people centric sensing network is framed with number of mobile nodes that are connected with the access points. The access point's acts as a gateway to forward the data and also performs some aggregation functions. Further, there are number of cloud servers meant for handling the data in the cloud. They collude with each other cloud servers if there is task from trusted centre for summarization of data. So, aggregation service is also done by the cloud servers whenever statistical data is needed. The trusted management centre handles the mobile node registration in the network and authorization of cloud servers. They also act as security key distribution server and are assumed to be trusted entity. They provide the data obtained from mobile nodes to the data consumers and provides application oriented services based on requirements.

3.1 Execution phase of the Framework

3.1.1 Network Initialization and Authorization

Here, the network initialization is defined with variety of network mobile nodes and cloud servers and that is linked with the Internet to process proper network communication without failures. The network Initialization and Authorization functions are handled by the Trusted Authority centre. The network is initialized with installation of web or mobile application developed for the purpose of collecting urban sensing data. Then the network mobile participants and cloud servers are authenticated on request basis by the trusted authority. Once the entities have joined the network, the trusted authority distributes the security key to the authorized mobile nodes and cloud servers for secured communication over the network. It is explicit that the model provides authentication, data privacy and security over shared data using homomorphic encryption based key generation. Let us consider the basic additively homomorphic encryption scheme for providing privacy preserved data communication using the pseudo random function.

3.1.2 Key Initialization

The decryption key for the trusted authority centre is set using random selection of DecKey from $\{0, 1\}^{\lambda}$ where λ is the product of two times the length of the output bits sent from random function.The encryption key for the each mobile nodes is fixed as EncKey =random $_{K}$ (i) Where i represent the mobile participant node from 1 to n, the random function used belongs to the pseudo random function family.

3.1.3. Privacy preserving Encryption

The data sensed by each mobile participant is transmitted in encrypted form for secured data communication. Also to protect the privacy of user's data, homomorphic encryption method can be used. The mobile node encrypts the data with the key set using random function. A Homomorphic encryption method allows doing arithmetic computations in cipher text form. This makes the access points to do aggregation on cipher text making them unaware about the plain text user data. By this method, privacy of sensitive data shared by users is not revealed directly to any of the entities involved in the network communication. The encryption formula used is,

$$\text{Cipher} = \text{Encrypt}(\text{Msg}_i) = \text{Msg}_i + h(f_{\text{EncKey}}(\text{id})) \bmod M \qquad (1)$$
$$\text{Meta} = \{i\} \text{ and Cipher report} = \{\text{Meta, Cipher}\} \qquad (2)$$

Where $\text{Msg}_i$is the message sensed by ith mobile participant,h depicts the hash function and f depicts the pseudo random function,id represents unique message ID and M is the modulus.Along with the encrypted message of the plain text, Meta information is also sent and formed as a report. The Meta information about the reporting node is combined for forwarding the report.The access points can find the aggregation on ciphers obtained from various mobile participants. Additive aggregation operation on cipher text is implemented along with combining the list of Meta information received from mobile nodes. Finally the cipher report is prepared by the access points and now it is ready for forwarding purpose.

3.1.4. Secured Anonymous data communication

Anonymity can be achieved by hiding the relation of the identity of the sender and the receiver. This can be done by using Mix scheme for secured anonymous data communication in the network where there are many intermediate entities involved in the system. This standard scheme allows us to protect the data using RSA encryption methods. There are many intermediate nodes said as mix nodes along the network which forwards the message to the server. Finally, the trusted authority centre implements the decryption operation. Once the aggregated data is decrypted, the authority centre can now get the sum of plain text. The computation used for decryption is given in eqn 3 Where Aggregate is the final aggregated plain text, h depicts the hash function and f represents the pseudo random function, id represents unique message ID and M is the modulus. Aggregate = Decrypt (cipher) = cipher – Σ h (f_{EncKey}(id))) mod M (3)

3.1.5. Fault Resistance

There are many cloud servers in the system and they belong to the same cloud provider. Aggregation services also may be applied on the cloud servers for performing any aggregations. The main use of cloud servers are storage of huge data gathered from mobile participants. They collude with each other cloud servers if there is task from trusted centre for summarization of data. So, aggregation service is also done by the cloud servers whenever statistical data is needed. Otherwise, it provides the individual users data in cipher text whenever trusted authority demands for data once the task arrives. Multiple cloud servers are deployed in the framework for workload sharing and Fault tolerance. Also the data is stored in the encrypted form achieving data confidentiality and privacy. The single point of failure can be resisted since many cloud servers belonging to a provider is used. Let us consider an adversary attempting to compromise on a server, there are other cloud servers available to resist the communication of the network. The cloud servers are powerful entities and not much easy to compromise by any adversary. So, only minority of servers may be identified with risk, remaining percentage of servers may balance the load and resist on fault identified in the network.

4. Performance Evaluation

Security: The communication model set in the framework is encrypted and secured against internal and external attacks. The model is resistant to attacks such as eavesdropping, false data injection and collusion attack.Privacy: Users privacy is protected because of the use of homomorphic encryption methods for privacy preserving aggregation. Also anonymity is achieved with the extension of mix scheme for communication between the intermediate entities available in the system.Fault Tolerance: The design of multiple cloud servers to balance work load sharing and fault tolerance. They also perform aggregation operations based on request from the trusted authority centre.Computation Cost Analysis: The computation cost analysis includes the cost of addition and multiplication operation under Modulus. Then the cost for generation of random key using pseudorandom function family is included along with the cost of implementation of hash functions. The computation cost for decryption by the trusted authority to generate the aggregate is also calculated.

5. Conclusion

This paper proposes a cloud based framework for people centric urban sensing networks. The framework includes the mobile participants, aggregation cloud servers and trusted authority centre. The activities involved in transferring a data from mobile participants to application providers are divided into four phases such as Network Initialization and Authorization, Privacy preserving Encryption, Secured Anonymous data communication and Fault Resistance. A standard homomorphic based encryption scheme is used for providing data confidentiality and also data is transferred anonymously improving the privacy of the system. The cloud based network model improves the reliability of the system and also supports large scale sensing applications.

References

[1] A. T. Campbell, S. B. Eisenman ,N. D. Lane. The rise of people-centric sensing, IEEE Internet Computing. Vol.12(4),pages.12–21,2008.

[2] Marco Conti, Silvia Giordana.Mobile Ad Hoc Networking: Milestones, Challenges, and New Research Directions, IEEE Communications Magazine, Vol.52 (1), pages.85-96, 2014.

[3] R.K.Ganti, F.Ye, H.Lei. Mobile crowd sensing: current state and future challenges. In IEEE Communications Magazine, Vol.49(11), pages. 32-39,2011.

[4] J. Shi, Y. Zhang , Y. Liu. Prisense: privacy-preserving data aggregation in people-centric urban sensing systems. Proceedings of IEEE INFOCOM: San Diego, CA, USA, pages.1-9,2010.

[5] Zhang R, Shi J , Zhang Y.Verifiable privacy-preserving aggregation in people-centric urban sensing systems. IEEE Journal on Selected Areas in Communications, Vol. 31(9),pages.268–278, 2013.

[6] De CristofaroE,DiPietro R. Adversaries and countermeasures in privacy-enhanced urban sensing systems. IEEE Systems Journal,Vol.7(2), pages.311–322, 2013 .

[7] K.R.Jansi,S.V.KasmirRaja. A survey on Privacy Preserving data aggregation schemes in People centric sensing systems and wireless domains. Indian journal of science and technology, Vol 9(37), pages.1-7, 2016.

[8] ZilengWei,Baokang Zhao, Yujing Liu, JinshuSu, PPSENSE.A novel Privacy-Preserving system in people centric sensing networks. IEEE International conference on communications and Networking:China,2013.

[9] K.R.Jansi, S.V.KasmirRaja,G.K.Sandhia. Efficient privacy-preserving fault tolerance aggregation for people-centric sensing system. Springer. Service Oriented Computing and Applications.Vol.12(34), pages. 305-315, 2018.

[10] Arulprakash, M. Dynamic evolutionary information diffusion over mobile social networks . ARPN Journal of Engineering and Applied Sciences, 2016, 11(19), pp. 11457-11464.

[11] AnkitKumar et.al,. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm.Microprocessors and Microsystems, (https://doi.org/10.1016/j.micpro.2020.103352)