International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 4 – APRIL 2018.

IDENTITY BASED ENCRYPTION SCHEME IN CROWDSENSING BASED ROAD MONITORING

Nivedha.A$^{\#1}$, Prashika .M$^{\#2}$, Preethi.R$^{\#3}$ and Indra . G^{*4}

[#]Department of Computer Science Engineering, R.M.K College of Engineering and Technology ,
Gummudipoondi , Chennai

[*] Asst. Prof., Department of Computer Science Engineering, R.M.K College of Engineering and Technology ,
Gummudipoondi , Chennai

***Abstract*: In cloud crowd-sensing systems, the value of crowd-sensed big data can be increased by incentivizing the users appropriately. Since data acquisition is participatory, crowd-sensing systems face the challenge of data trustworthiness and truthfulness assurance in the presence of adversaries whose motivation can be either manipulating sensed data or collaborating unfaithfully with the motivation of maximizing their income. In this paper, we propose road surface condition monitoring which increase traffic flow and road safety using fog computing. The fog nodes compose of conventional On-board Units (OBU) and Road Side Units (RSU) which used for monitoring the conditions on road surface. The road side information is generally collected and processed by cloud center. The acquisitioned data is further preserved using signcryption algorithms which enhances privacy of the data. The secured communication is achieved by key processing unit between OBU and RSU. Based on the key received by OBU, the information is encrypted and then forwarded to the Fog cloud. By doing so, our proposed model efficiently achieved the privacy of the data. Experimental results will prove the efficiency of the study.**

Keywords: Crowd-sensing, Road surface, Data Acquisition, Fog computing and Signcryption.

I. INTRODUCTION

In the Internet of Things (IoT) Era, crowd-sensing (MCS) has emerged from large-scale participatory sensing which requires an implicit collaboration between crowd-sensing platforms and sensing data providers, i.e. the participants [1], [2]. Participants act as service providers in crowd-sensing campaigns by only using their smart mobile devices such as smartphones, tablets and wearables. These devices are equipped with various built-in sensors such as GPS, camera, accelerometer, gyroscope and microphone. Furthermore, the widespread use of these devices unveils the potential of them being an integral part of the IoT sensing. As stated in [3], because the IoT consists of massive amount of uniquely identifiable heterogeneous devices with communication, sensing and computing capabilities, the IoT architecture faces several challenges concerning the acquisition, processing and storage of big data streams.

In 2015, more than 1.4 B units of smartphones were reported to be sold worldwide [4], while 232 M units of wearables were sold in 2015 with a projection of 322 M unit sale in 2017 [5]. Various phenomena such as air pollution, water quality, road condition for smart transportation, public safety and emergency preparedness can be collaboratively sensed through these devices in a participatory, or opportunistic manner[7]. Mobile crowd-sensing has been attracting the IT industry for various applications. A research consortium between IBM, University of Illinois and University of Minnesota has developed a middleware crowd-sensing platform which is called Citizen Sense. Google has developed a crowd-sensing application called Science Journal, which is available via Play Store [6]. Science Journal exploits various built-in sensors in smartphones to acquire data regarding users’ interests. The collected data undergoes real time analytics. Based on these phenomena, mobile crowd-sensing is listed as a critical component of the IoT.

Recently, researchers have started tackling data quality assessment especially in visual crowd-sensed data, and data quality-aware incentives in mobile crowd-sensing in order to avoid unnecessary rewards made to participants. As the advent of Internet of Things (IoT) concept enables mobile crowdsensing via built-in sensors of everyday mobile devices, uncertainty in the quality of crowd-sensed data is complicated since the recruited participants and their crowd-sensors are not professional/ dedicated. While the quality of sensory data can be modeled as a function of the sampling rate, in these scenarios, it can be any random number. In order to deal with uncertainty in these scenarios, online learning approaches have been proposed to acquire the statistical information. While the quality of sensory data can be modeled as a function of the sampling rate, in these scenarios, it can be any random number. In order to deal with uncertainty in these scenarios, online learning approaches have been proposed to acquire the statistical information about the sensing values throughout the sensor recruitment process. In [7], uncertainty propagation in distributed sensing has been modeled via Bootstrap-based methodology in order to improve system accuracy. Therefore, the integration of big data analytics into mobile crowd-sensing to improve the quality of the aggregated data – and consequently the quality of provided services – presents an important research area.

The rest of the paper is organized as follows: Section II describes the related work; Section III presents the proposed work; Section IV presents the experimental results and concludes in Section V.

II. RELATED WORK

This section describes the prior techniques introduced in privacy preserving models of crowd-sensing systems.

In [8], they present a comprehensive overview on urban sensing. Based on the role of users and how the user is involved in sensing tasks, two main approaches, namely participatory and opportunistic sensing are defined. Users are self-aware about sharing data with the others in participatory sensing but in opportunistic sensing, mobile devices are involved in the decision making process instead of the users.

In [9] formulated a four-stage life cycle for mobile crowd-sensing applications with the following stages: Task creation, task assignment, individual task execution and crowd-data integration. In each stage, the following 4W1H framework is taken into account: What phenomena should be sensed, when and where the assigned task should be sensed, who is responsible for collecting data and how the sensing task is divided between users as well as how collected data is communicated to the recruiter.

In [10] provide various big data applications in smart cities, namely smart grid, smart health care, smart transportation and smart homes. TreSight is an example smart city big data application that uses Big Data Analytics (BDA) and Internet of Things (IoT) to form a recommendation system that aims to improve the smart tourism in the city of Trento, Italy. Furthermore, the output of data analytics can assist decision making processes. Cities like Malaga, Amesterdam and Boston are well-known cases for applying BDA techniques to model the behaviour of urban inhabitants. To cope with computing and storage limitations in handling crowdsensed big data, and improve data quality.

In [11] introduce a context-aware computing platform and a traffic assistant application on top of it to automate the collection and aggregation of large scale contextual data. Tranquilien [12] and Snips are real crowd-assisted applications that capture urban mobility patterns about users' daily habits, interactions and surroundings to organize the users' transportation activities and improve the urban services. ParticipAct is a real world experiment that provides architecture for analysis of large scale crowd-sensed data. ParticipAct provides big data post-processing facilities as multi-layered data views and the crowd-sensed data-sets are published for researchers. The incentive mechanism used in ParticipAct is a threshold-based technique which basically renews the leased plan upon completion of a specific number of sensing tasks.

In [13], proposed Sign-and-Encrypt-and-Prove based GS scheme with efficient revocation check (similar as SRBE). The scheme adopts a centralized online OCSP service for revocation checking. In most of the Sign-and-Encrypt and-Prove based GS schemes, RAs need to de-anonymize a signature to perform revocation. However, as every signature verification needs a consultation with OCSP server for revocation checking, the communication overhead between verifier and the OCSP server becomes onerous. Most importantly, it is undesirable to de-anonymize the signatures from benign users, which might encourage massive surveillance [47]. Conversely, in VLR based GS schemes such as ours, trusted authorities are assumed to de-anonymize (open) signatures only when the signer is suspected to be malicious. In [14], proposed a light-weight linking based GS scheme with efficient revocation checking. However, during revocation this scheme requires O(R) group operations by the group manager, which restricts the scheme to be used in dynamic crowdsensing-settings where short-lived pseudonyms are critical.

LR-based GS schemes [15-18] are known to be more practical than the other schemes. Some VLR-based GS schemes [19] support backward unlinkability. In general, these VLR-based GS schemes need O(R) expensive operations to do revocation checking. The authors in [20] presented a new GS scheme with probabilistic revocation (GSPR) that drastically improves the performance of revocation check, compared to the prior art. However, probabilistic revocation checking resulting in false positives (i.e., valid signatures mistaken as generated by revoked participants) may not be desirable in crowdsensing. Moreover, the experimental evaluation suggests that, revocation check mechanism of SRBE runs faster than GSPR.

III. PROPOSED WORK

This section presents the working procedure of the Intelligent Road Surface monitoring systems. The main objectives of the proposed model are:

- To develop an intelligent road monitoring systems.
- To monitor the road surface conditions for reducing traffic
- To enhance the security of the road safety using fog computing.

The proposed phases composes of four phases, namely,

A) *Formation of networks and sign generation:*

In our study, the Road Side Unit (RSU) is considered as the fog node. The fog nodes are generated on three areas, viz, North, South and Central. Each RSU is maintained by unique identity. For every RSU that enters the network, the signature key is generated. This signature key is further used for the encryption and decryption process. In similar way, an unique id with its signature key is generated for the On-Board Units (OBU).

B) *OBU send path details to fog node:*

On-board Unit (OBU) will generate the signature. OBU select the Destination and generate path and monitor all the required parameter in the path monitoring parameter like (Vehicle Speed, Drunk and Drive, Seat Belt, Jerk Level). Once the OBU Reach the Destination, OBU sends the sensed information and forwards the information to the region RSU. Before Sending any information to the RSU or Fog Node OBU need to encrypt the information to protect the OBU Privacy. For that purpose OBU will perform Signcryption i.e. OBU will encrypt the information and the signature on the content by giving the RSU name. RSU will receive the information and reverse the process and decrypt the information.

C) *Fog node update the path information:*

The RSU receives the information from its region. The encrypted data is decrypted by the OBU using the signature key. If both the signature keys are matched, then the original data is retained. Then, the decrypted information is transferred to the cloud admin. Main Responsibility of the Cloud Admin is to store and receive information from the region fog node. In addition to, any mobile user request for any path Admin will process the request and provide the corresponding path.

D) *User path request to admin:*

Configure the application to the server by providing appropriate IP address in the app, when the user login into the app user need to provide the username and password once the user login into the app user can search any path by providing the source and destination. Admin will receive the path request process the request and provide the appropriate result to the mobile user. Response from the also include all the necessary detail about the path like (number of hospital, petro pump, number of drunker in the road .etc) along withal the detail admin also provide the public transport between that route.

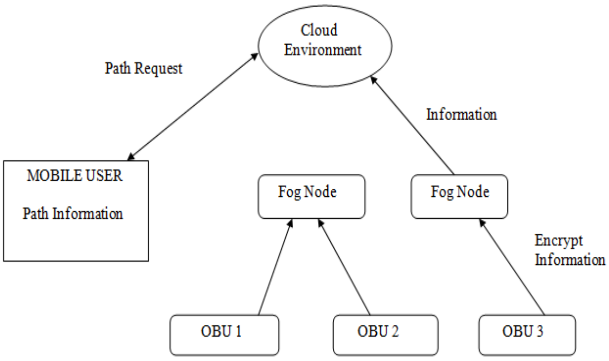

Fig. 3.1 System Architecture

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental analysis of proposed work. The objective of the study is to effectively utilize the fog nodes with reduced data loss and without compromising the accuracy of authentication. The following are the evaluation metrics analyzed:

a) Efficiency of keys:

While doing the protocol analysis, the processing cost taken by hash operation are eliminated. Since the validation algorithm involves scalar multiplication and bilinear pairing process, the proposed NG-KGP scheme effectively analyzes the message function with certain limitations. The length of public key and pairwise keys generation are done by point compression of group G1 which shows that the proposed scheme incurs fewer bits for key generation than the existing schemes.

b) Processing cost:

Generally, the processing cost is studied by the interchanging parameters of the sensor nodes. Since bilinear pairing is used for generating master keys and pairwise keys. Below the fig.4.2 represents the processing cost taken by analyzing the neighboring nodes. It is inferred that our proposed scheme includes lesser processing cost as the no. of neighboring nodes.

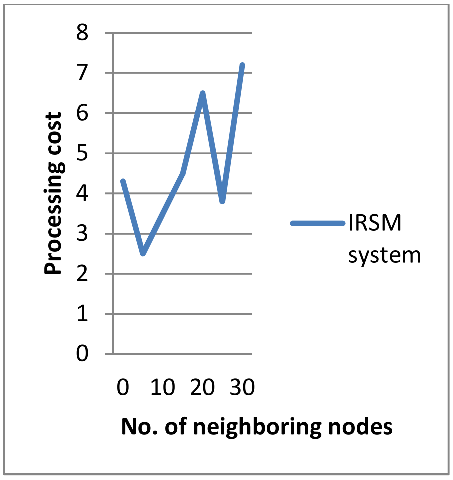

Fig.4.1 Processing cost analysis of NC-KGP scheme

c) Energy Consumption analysis:

Since the nodes are dynamic in nature, the secure communication depends on the energy consumed by the nodes using the updated neighboring nodes from the Base Station. Based on the storage of public keys, the energy analysis is done. From the fig.4.2, it is inferred that the bandwidth and energy of our proposed scheme is relatively small and suitable for WSN.

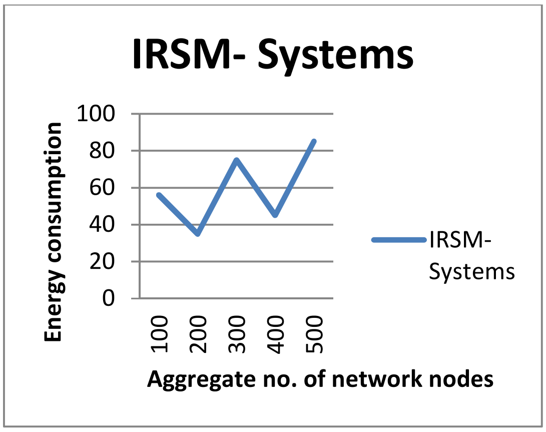

Fig.4.2. Energy consumption analysis

V. CONCLUSION

Crowd-Sensing (CS) systems has shown a great potential to make available sensing and computing of large volumes of data through smart phones, tablets and wearable technologies. Motivating users for sensing and reporting cloud data in a reliable manner is the key challenging issue for the success in CS platforms. In this paper, we propose an intelligent road surface monitoring systems which do data monitoring and data security service using fog computing. The major reason behind the fog computing model is to enhance the security by controlling the traffic systems. The RSU and OBU components are considered as fog nodes. The monitored data is preserved using signcryption algorithms for enhancing the security. Based on the key received by OBU, the information is encrypted and then forwarded to the Fog cloud. By doing so, our proposed model efficiently achieved the privacy of the data. Experimental results show the efficiency of the study.

REFERENCES

[1] Sultan Basudan et al, “A Privacy-Preserving Vehicular Crowdsensing-Based Road Surface Condition Monitoring System Using Fog Computing”, IEEE Internet of Things, 4(3), 2017.

[2] C. Fiandrino et al., ‘‘CrowdSenSim: A simulation platform for mobile crowdsensing in realistic urban environments,’’ IEEE Access, vol. 5, pp. 3490–3503, 2017.

[3] A. D. Cartier, D. H. Lee, B. Kantarci, and L. Foschini, ‘‘IoT-big data software ecosystems for smart cities sensing: Challenges, open issues, and emerging solutions,’’ in Proc. 4th Int. Workshop Cloud IoT (CLIoT), 2016, pp. 1–10.

[4] Gartner. (2017). Worldwide Sales of Smartphones. [Online]. Available: http://www.gartner.com/newsroom/id/3609817

[5] Gartner. (2017). Worldwide Sales of Wearables. [Online]. Available: http://www.gartner.com/newsroom/id/3560517

[6] R. K. Ganti, F. Ye, and H. Lei, ‘‘Mobile crowdsensing: Current state and future challenges,’’ IEEE Commun. Mag., vol. 49, no. 11, pp. 32–39, Nov. 2011.

[7] W. Khan, Y. Xiang, M. Aalsalem, and Q. Arshad, ‘‘Mobile phone sensing systems: A survey,’’ IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 402–427, 1st Quart., 2013.

[8] Open Collaborative Research project involving IBM Research. (2016). Citizen Sense a Crowdsesing Application. [Online]. Available: http://researcher.watson.ibm.com/researcher/view_group.php?id=3011

[9] Google Inc. (2016). Google Science Journal. [Online]. Available: https://makingscience.withgoogle.com/science-journal/

[10] J. Liu, H. Shen, and X. Zhang, ‘‘A survey of mobile crowdsensing techniques: A critical component for the Internet of Things,’’ in Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN), Aug. 2016, pp. 1–6

[11] A. J. Jara, D. Genoud, and Y. Bocchi, ‘‘Big data for smart cities with KNIME a real experience in the smartsantander testbed,’’ Softw., Pract. Experim., vol. 45, no. 8, pp. 1145–1160, 2015.

[12] M. Habibzadeh, A. Boggio-Dandry, Z. Qin, T. Soyata, B. Kantarci, and H. Mouftah, ‘‘Soft sensing in smart cities: Handling 3Vs using recommender systems, machine intelligence, and data analytics,’’ IEEE Commun. Mag., to be published. [Online]. Available: http://nextconlab.academy/pubs/commag17.pdf

[13] M. Habibzadeh, Z. Qin, T. Soyata, and B. Kantarci, ‘‘Large scale distributed dedicated- and non-dedicated smart city sensing systems,’’ IEEE Sensors J., to be published, doi: 10.1109/JSEN.2017.2725638.

[14] Cisco. (2016). Cisco Visual Networking Index: Global Mobile Data TRAC Forecast Update 2015-2020 White Paper. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ visual-networking-index-vni/mobile-white-paper-c11-520862.html

[15] B. Guo, H. Chen, Q. Han, Z. Yu, D. Zhang, and Y. Wang, ‘‘Workercontributed data utility measurement for visual crowdsensing systems,’’ IEEE Trans. Mobile Comput., vol. 16, no. 8, pp. 2379–2391, Aug. 2017.

[16] D. Peng, F. Wu, and G. Chen, ‘‘Data quality guided incentive mechanism design for crowdsensing,’’ IEEE Trans. Mobile Comput., to be published, doi: 10.1109/TMC.2017.2714668.

[17] S. Yang, F. Wu, S. Tang, X. Gao, B. Yang, and G. Chen, ‘‘On designing data quality-aware truth estimation and surplus sharing method for mobile crowdsensing,’’ IEEE J. Sel. Areas Commun., vol. 35, no. 4, pp. 832–847, Apr. 2017.

[18] T. Hu, T. Yang, and B. Hu, ‘‘A data quality index based incentive mechanism for smartphone crowdsensing,’’ in Proc. IEEE/CIC Int. Conf. Commun. China (ICCC), Jul. 2016, pp. 1–6.

[19] K. Han, C. Zhang, and J. Luo, ‘‘Taming the uncertainty: Budget limited robust crowdsensing through online learning,’’ IEEE/ACM Trans. Netw., vol. 24, no. 3, pp. 1462–1475, Jun. 2016.

[20] V. Freschi, S. Delpriori, E. Lattanzi, and A. Bogliolo, ‘‘Bootstrap based uncertainty propagation for data quality estimation in crowdsensing systems,’’ IEEE Access, vol. 5, pp. 1146–1155, 2017.