International Journal of Advanced Engineering, Management and Science (IJAEMS) [Vol-4, Issue-3, Mar- 2018]
https://dx.doi.org/10.22161/ijaems.4.3.12 ISSN: 2454-1311

Automated Sensing System for Monitoring Road Surface Condition Using Fog Computing

Nafras Ameer B.A, Pradeep Kumar J, Kumaran V, Dinesh P, Mr. M. Dilli Babu, M.E.

Department of Information Technology, Panimalar Engineering College, Chennai, India

***Abstract*— *The principle point of this task is to build up an Intelligent Monitoring System used to screen the Road Surface Condition using Fog Computing that increases the road safety. Multiple solutions have been proposed which make use of mobile sensing, more specifically contemporary applications and architectures that are used in both crowd sensing and vehicle based sensing. Nonetheless, these initiatives have not been without challenges that range from mobility support, location awareness, low latency as well as geo-distribution. As a result, a new term has been coined for this novel paradigm, called, fog computing.*

***Keywords*—Certificateless aggregate signcryption (CLASC), fog computing, road surface condition monitoring system, security.**

I. INTRODUCTION

1.1 Overview of the Project

Great attention has been directed toward road surface condition monitoring in the recent past. As a matter of fact, this activity is of critical importance in transportation infrastructure management. In response, multiple solutions have been proposed which make use of mobile sensing, more specifically contemporary applications and architectures that are used in both crowd sensing and vehicle-based sensing. This has allowed for automated control as well as analysis of road surface quality. These innovations have thus encouraged and showed the importance of cloud to provide reliable transport services to clients. Nonetheless, these initiatives have not been without challenges that range from mobility support, locational awareness, low latency, as well as geo-distribution. As a result, a new term has been coined for this novel paradigm, called, fog computing. In this paper, we propose a privacy-preserving protocol for enhancing security in vehicular crowd sensing based road surface condition monitoring system using fog computing. At the onset, this paper proposes a certificate less aggregate signcryption scheme that is highly efficient.

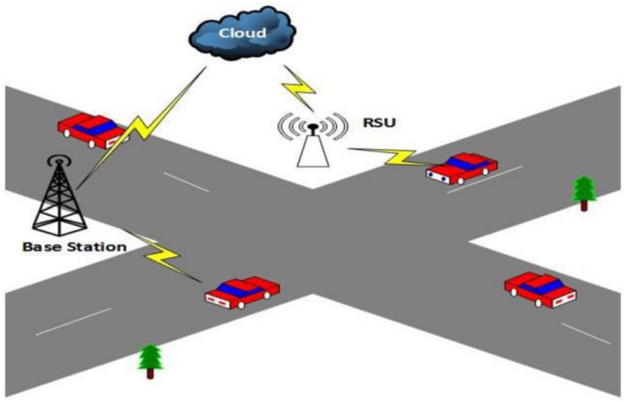


Fig.1: Cloud-based Architecture

On the basis of the proposed scheme, a data transmission protocol for monitoring road surface conditions is designed with security aspects such as information confidentiality, mutual authenticity, integrity, privacy, as well as anonymity. In analyzing the system, the ability of the proposed protocol to achieve the set objectives and exercise higher efficiency with respect to computational and communication abilities in comparison to existing systems is also considered.

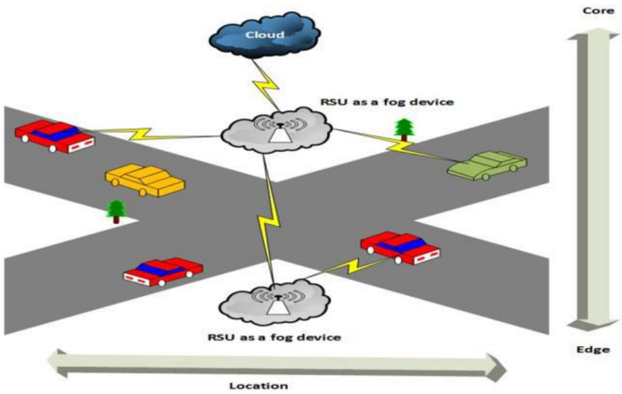


Fig.2: Fog-based Architecture

1.2 Existing System

The condition of road surfaces is considered as a major indicator of the quality of roads. As a matter of fact, classification of a road as either safe or dangerous, more often than not take into consideration the surface condition of the road. Conventionally, parameters such as potholes, bumps and slipperiness are considered as the distinguishing features of the quality of road surfaces.

https://dx.doi.org/10.22161/ijaems.4.3.12 ISSN: 2454-1311

Thus systems for monitoring road conditions are critical to the improvement of safety in roads, lowering accident rates and protection of vehicles from getting damaged as a result of poor surface road conditions. Using advanced vehicular technologies especially vehicular communication combined with sensing technologies, road anomalies can be easily identified and dealt with. This is achieved using an advanced system for monitoring road surface condition.

1.3 Proposed System

We propose a Road surface Condition Monitoring System Using Fog Computing which consists of traditional OBU(On board Unit) and RSU as Fog Node. In General OBU is Responsible to monitor the road condition and forward the content to the cloud. While uploading the information to the cloud OBU must encrypt the information by using Signcryption. Control center is responsible for key generation to the OBU as well as rsu . OBU will encrypt the information by using the key provided by the control center and forward the information to the Fog cloud i.e.(RSU). Fog Node is Responsible to Verifying the truthfulness of an message and forward the information to the cloud . The Cloud will maintain the data whenever request received cloud process the data and provide the corresponding request.

II. PROPOSED ALGORITHM AND EQUATIONS

The proposed CLASC scheme is composed by the following six algorithms.

2.1 Setup

Given the security parameters k, and this algorithm is performed by the KGC as follows.

a) Chooses a cyclic additive group G of prime order q on elliptic curve, and P is an arbitrary generator of G.

b) Chooses a cyclic multiplicative group G_T of the same order q and a bilinear map ê: $G \times G \rightarrow G_T$.

c) Randomly selects a master private key $s \in Z_q^*$and compute the master public key $P_{pub} = sP$.

d) Selects four secure hash functions H_1: $\{0, 1\}^* \rightarrow Z_q^*$, $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^n$ here n is the bit-length of plaintexts, $H_3 : \{0, 1\}^* \rightarrow G$ and H_4: $Z_q^* \rightarrow G$.

e) Publishes the system parameter params = $(G, G_T, ê, P, q, P_{pub}, H_1, H_2, H_3, H_4)$ and the master private key s will be kept secure by the KGC.

2.2 Key-Generation

This algorithm is interactively performed by the user ID_i and KGC as follows.

a) The user ID_i randomly chooses $x_i \in Z_q^*$ as the secret value and computes a partial public key $Y_{ib} = x_i P$.

b) The user sends its identity and partial public key (ID_i, Y_{ib}) to the KGC.

c) The KGC then randomly selects $y_i \in Z_q^*$and compute another partial public key for the user $Y_{ia} = y_i P$, so the full public key for the user is (Y_{ib}, Y_{ia}).

d) The KGC computes the partial private key $D_i = y_i + s * Q_i$where $Q_i = H_1$ (ID_i), and D_i is sent securely to the user ID_i.

e) The user ID_i judges the validity of the partial private key by checking $D_i P = Y_{ia} + P_{pub} H_1$ (ID*i*).

Notably, these procedures finish three different algorithms which are: 1) *set-secret-value*; 2) *partial-privatekey-extract*; and 3) *set-public-key* of the proposed scheme. These algorithms generate public key (Y_{ib}, Y_{ia}) that is kept in the public tree by the KGC, and the full private key (x_i, D_i) is kept secret by the user.

2.3 Signcrypt

This algorithm is performed by a sender ID_i to signcrypt the message m_i with ID_R as a receiver. ID_i performs the algorithm as follows.

a) ID*i* randomly selects $r \in Z_q^*$ and compute $T_i = rP$.

b) Compute $Z_b = rY_{rb}$.

c) Compute $Z_a = r(Y_{ra}. + P_{pub}\ Q_i)$.

d) Compute $h_a = H_2$ ($\mathrm{ID}_R \| Y_{ra} \| Y_{rb} \| \Delta \| T_i \| Z_b \| Z_a$).

e) Compute $K_i = h_a \oplus m_i$.

f) Compute $h_b = H_3(\mathrm{ID}_R \| Y_{ra} \| Y_{rb} \| \Delta \| T_i | K_i \| Q_i | |Y_{ib} \| Y_{ia})$.

g) Compute $h_c = H_4$ (Δ).

h) Compute $\alpha_i = D_i h_c + r h_b + x_i h_c$.

i) Return the ciphertext $C_i = (T_i, K_i, \alpha_i)$.

2.4 Aggregate

This algorithm is performed by aggregator signcryption generator on the receiver ID_R as follows.

a) Compute $\alpha = \sum_{i=1}^{n} \alpha_i$

b) This algorithm outputs the aggregate ciphertexts $C = (T_1 \ldots T_n, K_1 \ldots K_n, \alpha)$.

2.5 Aggregate-Verify

This algorithm is run by a receiver ID_R and computes the following.

a) $h_b = H_3$ ($\mathrm{ID}_R \| Y_{ra} \| Y_{rb} \| \Delta \| T_i \| Z_b' \| Q_i \| Y_{ib} \| Y_{ia}$), for $i = 1, \ldots, n$.

b) $h_c = H_4$ (Δ).

c) Verify ê(α, P) = ê$(\sum_{i=1}^{n} Y_{ia} + P_{pub} Q_i, h_c)$ê$(\sum_{i=1}^{n} Ti, h_b)$ê$(\sum_{i=1}^{n} Y_{ib}, h_c)$.

If the above equation holds, this algorithm outputs true otherwise false.

2.6 Aggregate-Unsigncrypt

If the output of Aggregate-Verify algorithm is true, this algorithm is performed by the receiver ID_R as follows.

a) Compute $Z_b' = x_r T_i$.

https://dx.doi.org/10.22161/ijaems.4.3.12 **ISSN: 2454-1311**

b) Compute $Z'_a = D_r T_i$.

c) Compute $h'_a = H_2\ (\mathrm{ID}_R \| Y_{ra} \| Y_{rb} \| \Delta \| T_i \| Z'_b \| Z'_a)$.

d) Compute $m'_i = K_i \oplus h'_a$.

e) This algorithm outputs $\{mi\}_{i=1}^{n}$.

2.7 Correctness of the Signatures

$$\hat{e}\ (\alpha, \mathrm{P}) \ = \hat{e}\left(\sum_{i=1}^{n} \alpha_i, P\right)$$

$$= \hat{e}\left(\sum_{i=1}^{n} (D_i h_c \ + \ r h_b \ + \ x_i h_c\ ), P\right)$$

$$= \hat{e}\left(\sum_{i=1}^{n} D_i h_c, P\right) \hat{e}\left(\sum_{i=1}^{n} rP, h_b\right) \ \hat{e}\left(\sum_{i=1}^{n} x_i P, h_c\right)$$

$$= \hat{e}\left(\sum_{i=1}^{n} D_i P, h_c\right) \hat{e}\left(\sum_{i=1}^{n} T_i, h_b\right) \hat{e}\left(\sum_{i=1}^{n} Y_{ib}, h_c\right)$$

$$= \hat{e}\left(\sum_{i=1}^{n} (Y_{ia} \ + \ P_{\mathrm{pub}} Q_i, h_c)\right)$$

$$\times \ \hat{e}\left(\sum\nolimits_{i=1}^{n} Ti, h_b\right) \hat{e}\left(\sum\nolimits_{i=1}^{n} Y_{ib}, h_c\right)$$

2.8 Correctness of the Decryption

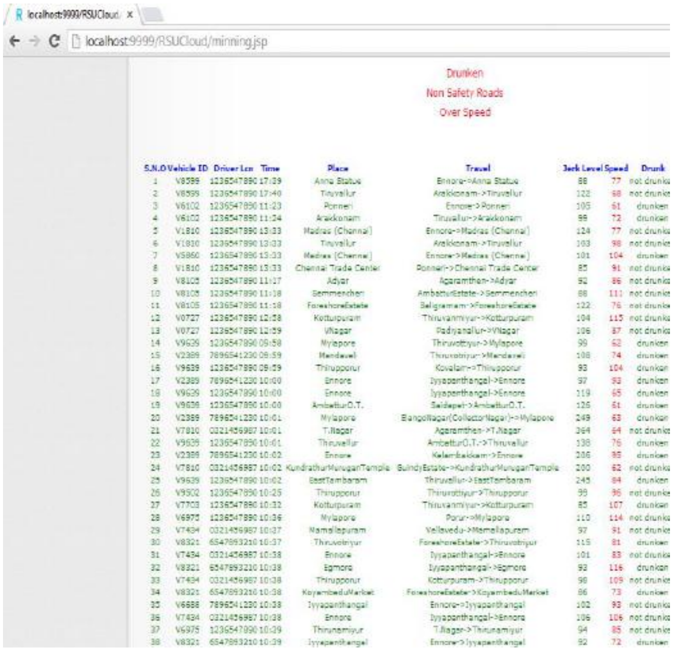
$m'_i = K_i \oplus h'_a$

$= H_2\ (Q_i \| Y_{ia}\ \| Y_{ib} \| \Delta \| Ti \| Z_b \| Z_a) \oplus \ m_i \oplus\ h'_a$

$= h_a \oplus \ m_i \oplus h'_a$

$= m_i$.

III. RESULTS AND DISCUSSION



S.N.O	Vehicle ID	Driver Lcn	Time	Place	Travel	Jerk Level	Speed	Drunk
1	V8599	1236547890	17:39	Anna Statue	Ennore->Anna Statue	88	77	not drunk
2	V8599	1236547890	17:40	Tiruvallur	Arakkonam->Tiruvallur	122	68	not drunk
3	V6102	1236547890	11:23	Ponneri	Ennore->Ponneri	105	61	drunken
4	V6102	1236547890	11:24	Arakkonam	Tiruvallur->Arakkonam	99	72	drunken
5	V1810	1236547890	13:33	Madras (Chennai)	Ennore->Madras (Chennai)	124	77	not drunk
6	V1810	1236547890	13:33	Tiruvallur	Arakkonam->Tiruvallur	103	98	not drunk
7	V5860	1236547890	13:33	Madras (Chennai)	Ennore->Madras (Chennai)	101	104	drunken
8	V1810	1236547890	13:33	Chennai Trade Center	Ponneri->Chennai Trade Center	85	91	not drunk
9	V8105	1236547890	11:17	Adyar	Agaramthen->Adyar	92	86	not drunk
10	V8105	1236547890	11:18	Semmencheri	AmbatturEstate->Semmencheri	88	111	not drunk
11	V8105	1236547890	11:18	ForeshoreEstate	Saligramam->ForeshoreEstate	122	76	not drunk
12	V0727	1236547890	12:58	Kotturpuram	Thiruvanmiyur->Kotturpuram	104	115	not drunk
13	V0727	1236547890	12:59	VNagar	Padiyanallur->VNagar	106	87	not drunk
14	V9639	1236547890	09:58	Mylapore	Thiruvottiyur->Mylapore	99	62	drunken
15	V2389	7896541230	09:59	Mandaveli	Thiruvotriyur->Mandaveli	108	74	drunken
16	V9639	1236547890	09:59	Thiruporur	Kovalam->Thiruporur	93	104	drunken
17	V2389	7896541230	10:00	Ennore	Iyyapanthangal->Ennore	97	93	drunken
18	V9639	1236547890	10:00	Ennore	Iyyapanthangal->Ennore	119	65	drunken
19	V9639	1236547890	10:00	AmbatturO.T.	Saidapet->AmbatturO.T.	125	61	drunken
20	V2389	7896541230	10:01	Mylapore	ElangoNagar(CollectorNagar)->Mylapore	249	63	drunken
21	V7810	0321456987	10:01	T.Nagar	Agaramthen->T.Nagar	364	64	not drunk
22	V9639	1236547890	10:01	Thiruvallur	AmbatturO.T.->Thiruvallur	138	76	drunken
23	V2389	7896541230	10:02	Ennore	Kelambakkam->Ennore	206	85	drunken
24	V7810	0321456987	10:02	KundrathurMuruganTemple	GuindyEstate->KundrathurMuruganTemple	200	62	not drunk
25	V9639	1236547890	10:02	EastTambaram	Thiruvallur->EastTambaram	245	84	drunken
26	V9502	1236547890	10:25	Thiruporur	Thiruvottiyur->Thiruporur	99	96	not drunk
27	V7703	1236547890	10:32	Kotturpuram	Thiruvanmiyur->Kotturpuram	85	107	drunken
28	V6975	1236547890	10:36	Mylapore	Porur->Mylapore	110	114	not drunk
29	V7434	0321456987	10:37	Mamallapuram	Vellavedu->Mamallapuram	97	91	not drunk
30	V8321	6547893210	10:37	Thiruvotriyur	ForeshoreEstate->Thiruvotriyur	115	81	drunken
31	V7434	0321456987	10:38	Ennore	Iyyapanthangal->Ennore	101	83	not drunk
32	V8321	6547893210	10:38	Egmore	Iyyapanthangal->Egmore	93	116	drunken
33	V7434	0321456987	10:38	Thiruporur	Kotturpuram->Thiruporur	98	109	not drunk
34	V8321	6547893210	10:38	KoyambeduMarket	ForeshoreEstate->KoyambeduMarket	86	73	drunken
35	V6688	7896541230	10:38	Iyyapanthangal	Ennore->Iyyapanthangal	102	93	not drunk
36	V7434	0321456987	10:38	Ennore	Iyyapanthangal->Ennore	106	106	not drunk
37	V6975	1236547890	10:39	Thirunamiyur	T.Nagar->Thirunamiyur	94	85	not drunk
38	V8321	6547893210	10:39	Iyyapanthangal	Ennore->Iyyapanthangal	92	72	drunken

Fig.3: Vehicle data set

Fig 3 shows the data set of the vehicles. This data set contains the sensed information such as Jerk Level, Speed and Safety between the source and destination. These information are useful for the mobile users who requests the safe route. Fig 4 shows the best and safe route between source and destination and additionally it displays the Public Transport for the requested route.

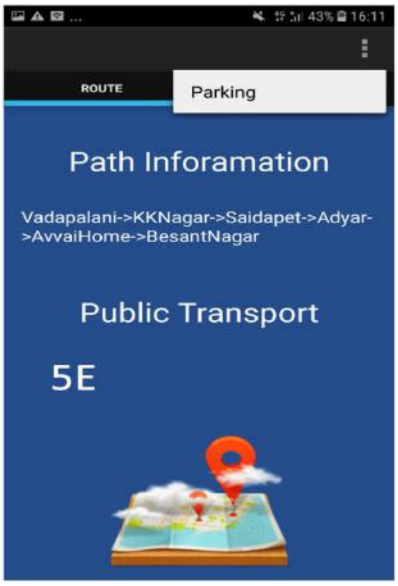


Fig.4: Dipslaying Best Route

Fig 4 displays the best route in map. It points the best intermediate route between source and destination. As it points the places, it will be very comfortable for the mobile users to travel easily and safely.

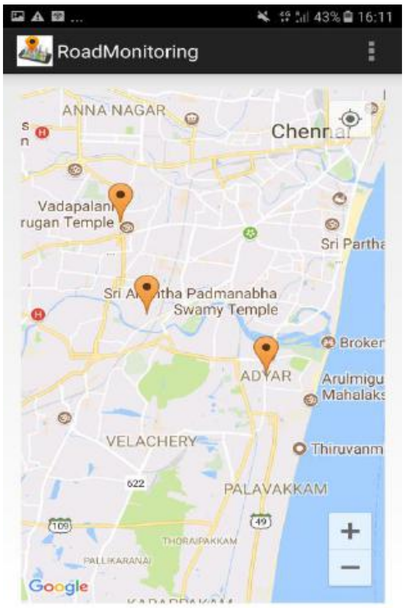


Fig.5: Route in map

Fig 5 displays the additional information to the mobile users such as the number of restaurants, petrol bunks, hospitals.

https://dx.doi.org/10.22161/ijaems.4.3.12 ISSN: 2454-1311

Fig.6: Additional Information

IV. CONCLUSION

We propose a new efficient CLASC scheme . We then designed a privacy preserving vehicular crowd sensing Road Surface Condition monitoring system using fog computing based on the proposed CLASC scheme. In addition, the proposed privacy-preserving protocol meets the security requirements such as data confidentiality and integrity, mutual authentication, anonymity, and key escrow resilience. Extensive comparisons of computational cost and communication overhead show that the proposed scheme can achieve much better efficiency than the existing schemes.

V. REFERENCES

[1] M. Scott. Efficient Implementation of Crytographic Pairings. Accessed on Feb. 18, 2017. [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf
[2] Winter Driving—Be Prepared, Be Safe, Ontario Ministry Transp.,Toronto, ON, Canada, Feb. 2017. [Online]. Available: http://www.mto.gov.on.ca/english/ontario-511/pdfs/winter-safe-driving.pdf
[3] J. Kar, “Provably secure identity-based aggregate signcryption schemein random oracles,” Int. J. Netw. Security, vol. 17, no. 5, pp. 580–587,Sep. 2015
[4] L. M. Vaquero and L. Rodero-Merino, “Finding your way in thefog: Towards a comprehensive definition of fog computing,” ACMSIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 27–32, 2014
[5] Z. Eslami and N. Pakniat, “Certificateless aggregate signcryption:Security model and a concrete construction secure in the random oraclemodel,” J. Comput. Inf. Sci., vol. 26, no. 3, pp. 276–286, 2014.
[6] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, “An efficient certificateless encryption for secure data sharing in public clouds,” IEEE Trans.Knowl. Data Eng., vol. 26, no. 9, pp. 2107–2119, Sep. 2014.
[7] I. Stojmenovic, “Fog computing: A cloud to the ground supportfor smart things and machine-to-machine networks,” in Proc. Aust.Telecommun. Netw. Appl. Conf. (ATNAC), Southbank, VIC, Australia,2014, pp. 117–122.
[8] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, “Combiningcloud and sensors in a smart city environment,” EURASIP J. WirelessCommun. Netw., vol. 2012, p. 247, Dec. 2012.
[9] M. Perttunen et al., “Distributed road surface condition monitoring usingmobile phones,” in Ubiquitous Intelligence and Computing. Heidelberg,Germany: Springer, 2011, pp. 64–78.
[10] G. Strazdins, A. Mednis, G. Kanonirs, R. Zviedris, and L. Selavo,“Towards vehicular sensor networks with android smartphones for roadsurface monitoring,” in Proc. 2nd Int. Workshop Netw. CooperatingObjects (CONET) Electron. CPS Week, Chicago, IL, USA, 2011,pp. 1–4.
[11] W. Xie and Z. Zhang, “Efficient and provably secure certificateless signcryption from bilinear maps,” in Proc. IEEE Int. Conf.Wireless Commun. Netw. Inf. Security (WCNIS), Beijing, China, 2010,pp. 558–562.
[12] F. Li, M. Shirase, and T. Takagi, “Certificateless hybrid signcryption,”in Proc. 5th Inf. Security Pract. Experience Conf. (ISPEC), vol. 5451.Xi’an, China, 2009, pp. 112–123.
[13] C. Wu and Z. Chen, “A new efficient certificateless signcryption scheme,” in Proc. Int. Symp. Inf. Sci. Eng. (ISISE), vol. 1. Shanghai,China, 2008, pp. 661–664.
[14] A. W. Dent, “A survey of certificateless encryption schemes and security models,” Int. J. Inf. Security, vol. 7, no. 5, pp. 349–377, 2008.
[15] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, “Certificateless signature:A new security model and an improved generic construction,” Design Codes Cryptography, vol. 42, no. 2, pp. 109–126, 2007.