A Secure Vehicular Traffic Sensing Based Road Surface Condition Monitoring System Using Fog Computing

Gaddipathi Bharathi[1], Chinta Komali[2]
[1]Associate Professor, Dept of MCA
[2]Dept of MCA
[1, 2] St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

Abstract- *In the recent past, great attention has been directed towards road surface condition monitoring. As a matter of reality, this activity is of essential importance in transportation infrastructure management. In response, multiple solutions are projected that make use of mobile sensing, a lot of specifically modern applications and architectures that are employed in each crowd sensing and vehicle-based sensing. This has allowed for machine-controlled management similarly as analysis of road surface quality. These innovations have so inspired and showed the importance of cloud to supply reliable transportation services to purchasers. nevertheless, these initiatives haven't been while not challenges that vary from quality support, location awareness, low latency similarly as geo-distribution. As a result, a replacement term has been coined for this novel paradigm, called, fog computing. during this paper, we have a tendency to propose a privacy-preserving protocol for enhancing security in transport crowd sensing based mostly paved surface condition observance system victimisation fog computing. At the onset, the paper proposes a certificate-less combination signcryption theme (CLASC) that's extremely economical. On the idea of the projected theme, a knowledge} transmission protocol for observance paved surface conditions is meant with security aspects like information confidentiality, mutual believability, integrity, privacy similarly as obscurity. In analyzing the system, the flexibility of the projected protocol to attain the set objectives and exercise higher potency with regard to process and communication talents compared to existing systems is additionally considered.*

Keywords- Fog computing, Road surface condition monitoring System, Security, Certificate less aggregate signcryption.

I. INTRODUCTION

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 [1]. Notable as well is the fact that surface condition of roads are amongst the major reasons that vehicles get damaged and age faster. In Ontario (Canada), winter weather is known to bring along with it snow, sleet, ice, and freezing rain, among others, all of which when acting alongside poor road surface conditions create situations that are potentially dangerous to motorists, vehicles, people and property [30]. As a result, this is an area where 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.

Municipalities worldwide spend millions of dollars on maintenance and repair of road surfaces [2]. Traditionally, the municipalities engage patrol crews that perform physical examination of road surface conditions with the aim of identifying slippery spots and potholes, etc. Nonetheless, 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 [3]. As a matter of fact, advances in sensing technologies such as smart phones and other personal smart devices has allowed the use of sensors in gathering useful information from the environment [1], [2], [3]. This makes it one of the most important innovations for the future.

The technological strides made in mobile communication for instance smart phones, smart watches, and other personal gadgets (through their inbuilt sensors) has aided in gathering information regarding the environment around us. For example, everyone has a mobile device and gathering data from the user is one of the key elements of future smart cities. As a matter of fact, emphasis is placed on contemporary applications/architectures for both crowd sensing and vehicle based sensing alongside advances in cloud computing allow

for data collection, analysis, storage, processing and transmission in an efficient manner.

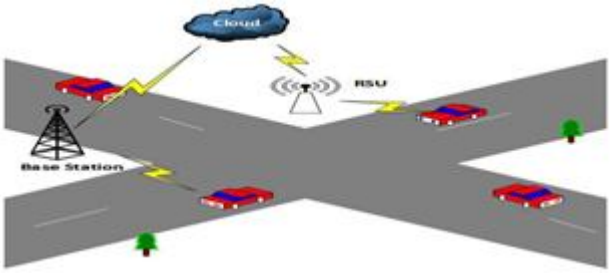
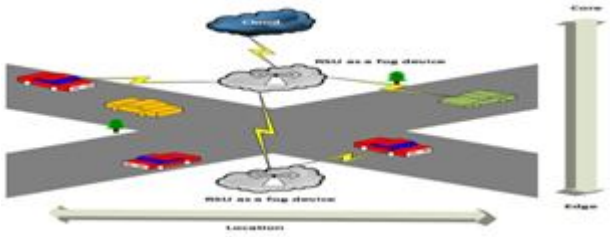


Fig. 1.Cloud based architecture

Cloud based architecture as shown in Fig.1 is used by various applications, such as smart city application [33], consists of mobile sensors that could be embedded in either a vehicle or some smart devices/roadside units and linked to cloud servers. Mobile sensors are used to collect data when the vehicle encounters anomalies while on the road as displayed in Fig.2 (a), for example, hitting a pothole. The data is then transferred to a centralized cloud system from where it is processed. The cloud based facility acts as an efficient means through which the integrated system remains up to date while maintaining privacy and security. It is assumed that the applications are deployed such that the vehicles and smart devices can potentially lead to crowd sensing. The roadside units (RSUs) as well as base stations help in relaying data to the cloud for processing and to provide recommendations for any applications, the approaching cars require real-time data processing in order to be able to offer instant recommendations with regard to the road surface conditions. Nonetheless, solutions that are cloud based and used in dealing with crowd sensing as well as vehicular based sensing data presents a number of issues such as transmission of extensive real-time data to the centralized cloud servers that are prone to time delays and elevated costs of bandwidth. Position awareness, large node, extensive geo-distribution, increased mobility, real-time applications processes, hetero-genetic/interoperability, as well as federation [5]. On the contrary though, unlike the globally centralized cloud based systems, once the included mobile sensors detect and generate data, the data is transmitted to the closest RSU, i.e., a fog device [4]. The RSU then does real-time computation in addition to taking local decisions as shown in Fig.2 (b). The results along with recommendations can also be transmitted to other approaching vehicles heading towards the affected region. This system thus achieves low latency as well as reduction in bandwidth costs. We can thus envision a system for measuring road surface conditions with the use of fog computing which allows applications to operate as reasonably as possible to the sensed, actionable and massive information collected via sensors. Nonetheless, security and privacy issues need to be ad-dressed before its implementation in the Vehicular Ad hoc Networks (VANETs). It is not just message confidentiality that need to be addressed but also the authenticity and integrity of the message. Furthermore, it is important to protect user-related data, including user ID and position, among others. A majority of previously reported literature have paid attention to the transmission of data in VANETs [6], [7], [8], [9], [10]. Nevertheless, the security challenges, particularly with respect to ways through which authenticity and confidentiality can be ensured with regard to the road event reported are still to be explored.



- Detected results at Fog Node (RSU)

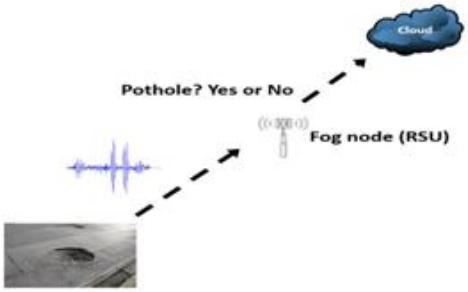
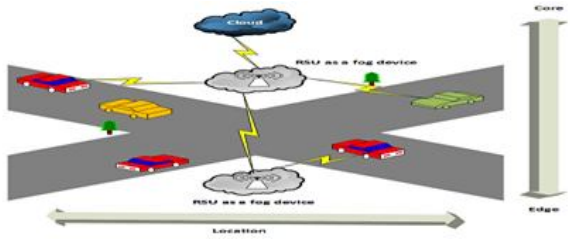


Fig. 2. An example of Detected results

Recently, a computer paradigm is emerging, also referred to as fog or edge computing [5]. This is a computing model that stretches cloud computing and related services to the network edge. This offers interesting features by using fog based architecture as represented in Fig.3 including lowatency In reality, as a result of privacy sensitivity of road event information as well as unauthentic interconnection of mobile sensors and the corresponding road infrastructure, inclusive of the RSUs such transmissions experience major challenges. A number of issues that need to be addressed in design of the security protocol includes a guarantee that the road event is not accessed at the time of transmission by unauthenti-cated users as well as consideration for its scalability. It is supposed that the generated data remain encrypted and hence the system should not only be able to just verify but also to simultaneously decrypt the data based on low computational and communication costs. Additionally, the protocol should attain mutual authentication among sensors, RSU gadgets as well as the cloud servers. Further, the protocol should be lightweight as a result of constraints in energy use and storage.

Also, the protocol needs to retain its robustness when there is a threat; for instance, a case where the authentication keys remain exposed.



In order to successfully address the aforementioned is-sues, certificateless public key cryptography (CLPKC) [16] is used in pursuing the security objectives. CLPKC avoids often experienced key escrow problem that is associated with identity-based public key cryptography, commonly abbreviated as IDBC. As the user's private keys in CLPKC are not only offered by the Key Generator Center (KGC) but a combination of KGC's and the user's partial private keys. Nonetheless, the KGC lacks information of the user's full private key. Further-more, CLPKC successfully evades the certificates management with regard to certificate-based public key cryptography like revoking, distributing and storing data. In order to achieve efficiency in terms of computational cost and communication overhead, we adopt signcryption technique to accomplish both encryption and signature in one logical step.

In order to adjust current work by adopting signcryp-tion technique, certificateless schemes of signcryption (CLSC) are used in capturing communication with respect to both confidentiality and unforgeability. The first scheme of CLSC was proposed by Barbosa and Farshim [11] using a formal security analysis as evident in random oracle model. The CLSC protocol is premised on the process of aggregation that lowers the volume of exchanged information, signature verification as well as massive data unsigncryption thus attaining scal-ability, and lower computational and communication costs. These can be achieved with a single step and is of particular importance to low communication network bandwidths as well as computationally restricted environments. Eslami et al. and Lu et al. proposed certificateless aggregate signcryption scheme (CLASC) [12], [13]. However, these schemes are realized using many pairing operations that may lead to high computational cost and time consumption if there is an increase in the number of mobile sensors. Motivated by the above mentioned issues, our contributions are twofold:

We propose a new efficient certificateless aggregate signcryption scheme CLASC with a significant im-provement over pairings required by existing aggre-gate signatures verifications and unsigncryption. Our CLASC scheme has the lowest computational cost compared to the existing schemes [12], [13].

Based on our proposed CLASC scheme, we design a privacy-preserving protocol, for enhancing security in data transmission of vehicular crowdsensing based road surface condition monitoring system using fog computing. The proposed protocol achieves data confidentiality, integrity, mutual authentication, privacy and anonymity through utilizing proposed CLASC scheme.

II. RELATED WORK

This section begins by providing an overview of fog networking architecture and then investigating some of the existing systems for road surface condition monitoring before presenting a privacy-preserving protocol that uses certificate-less aggregate signcryption scheme.

FOG NETWORKING ARCHITECTURE

Fog networking is a new architecture that provides stor-age, communications, control, configuration, asurement and management between terminal devices and the Inter-net with significant features, including location awareness, geographic distribution and low response latency [4], [5]. In the fog networking, a huge number of decentralized mobile devices can self-organize to communicate and potentially collaborate with each other via a fog node located at the edge of the Internet. There are several dimensions in fog architecture in term of the current standard practice [35]. At or near the end-user, essential amount of storage is carried out rather than storing in large-scale data centers. Moreover, instead of all routed through the backbone network, fog performs a substantial amount of communi-cation at or near the end-user. Furthermore, a fundamental amount of management, including network measurement, control and configuration, at or near the end-user is carried out. Each node in the fog networking must be able to act as a router for its neighbors and be flexible to node mobility. As a special instantiation of mobile ad-hoc networks (MANETs), crowd sensing vehicular networks (CSVN) is applying the principles of MANETs that could be the basis for future fog networks [34]. Without requiring fixed and costly infrastructures to be available beforehand, MANETs will enable the formation of densely populated networks. More precisely, data collected by sensors are sent to devices like network edge, routers, access point for processing, not sent to cloud server thus fog computing paradigm reduces the traffic due to low bandwidth. Also, Fog computing improves the quality of service and

minimizes latency. Therefore, Fog computing plays an important role by reducing the traffic of data to the cloud and not delaying the computation and communication due to placing near to the data sources.

Road surface condition monitoring system

Modern devices especially mobile devices have made sens-ing capabilities possible through the use of multiple powerful embedded sensors including accelerometers, gyroscopes and GPS systems, among others. We thus evaluate multiple sce-narios/applications where mobile sensors are used in detection and reporting road surface conditions. Eriksson et al. proposed Pothole Patrol (P2) [2], a mobile sensing app used in detection and reporting of road surface condition. In this system, they used a taxi cabinet in which multiple accelerometer sensors were placed and used in the collection of multiple predefined patterns associated with road surface anomalies via manual labelling. In the experiment, Eriksson et al. equipped taxis with an embedded Linux computer system and were able to detect more than 90% of potholes. In a similar system used in traffic sensing and communication, Mohan et al. [14] proposed the use of mobile devices hooked up to integrated sensors to the exterior. Further, Mednis et al. [15] improved on the Pothole Patrol (P2) system using a customized embedded gadget and extended the approach using vehicular sensor net-works operated using wireless sensor networks with the help of smartphones hardware platform for sensing road surface conditions [3]. The framework used involved synchronization and linkage of the data collection system with a database server for storage. A majority of such applications use cloud based architecture. However, in this paper, the system proposed is a privacy-preserving protocol that uses fog architecture.

Certificateless Aggregate signcryption scheme

The proposed protocol is based on privacy preservation us-ing an aggregate scheme of signcryption that is certificate-less. Hence the focus of this work will be on existing certificateless aggregate signcryption scheme (CLASC) literature. Certificate-less public key cryptography was first proposed by Al-Ryiami and Paterson [16] as a way of overcoming the challenges asso-ciated with key escrow as applied in cryptography approaches that are identity-based and hence maintain certificate freeness. There are several schemes proposed in encryption [17], [18], digital signature [19], [20], and signcryption [11], [21], [22], [23], certificateless cryptography. Since we are using certifi-cateless aggregate signcryption, we evaluate multiple aggregate signcryption as used in identity based aggregate schemes of signcryption [24], [25]. Certificateless aggregate signcryption scheme (CLASC) is emphasized [13] as an appropriate secure model as has been proven in its use in the random oracle model [26]. Further, Eslami and Pakniat [12] argued in favour of certificateless aggregate signcryption scheme as a secure system. Nonetheless, the scheme as currently constituted re-quires significant improvements over pairing maps that can potentially lead to a promising low computational scheme in addition to lowering time consumption. We propose a new and efficient certificateless aggregate signcryption (CLASC) scheme by building on the random oracle model.

III. PROPOSED WORK

This section describes our system model, attack model and design goals.

A. System model

Motivated by the various applications found in current liter-ature, we consider that the road surface condition monitoring system comprises of a control center (CC), mobile sensors, e.g., vehicles and smart devices, roadside units (RSUs) as a fog device, and cloud servers, as shown in Fig. 4.

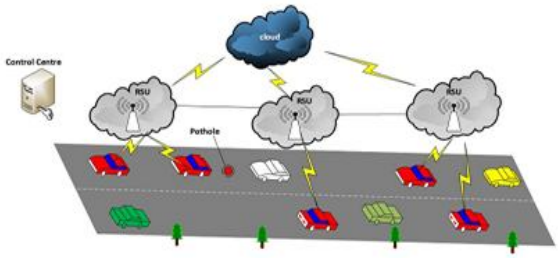


Fig. 4. System model

Control center (CC) is a trustable entity in charge of the entire system and responsible for initializing the system. In the proposed scheme, CC works as the key generation center. CC only generates partial private key for the registers to avoid the key escrow problem and is blocked to access the sensors and RSUs sensi-tive data. It is assumed that the CC is powered with sufficient computation and storage capabilities.

Mobile sensors, which may be embedded to vehicles and smart devices, generate a bunch of data, such as time, location and the actions signals, during road events, i.e., pothole or accidents.

Roadside unit (RSU) is considered as an efficient computational and storage device that can extend the cloud services to the edge. RSUs have the ability to react and make decisions close to the end users. All the real time data sensed

by the mobile sensors are sent to the RSU for immediate processing. Once processed, the RSUs can send for example an alert regarding road hazards at a specific location.

Cloud servers are the data centers of the system. The system data such as historic information are stored in the cloud to be utilized later. The advantage of a fog device is that instead of sending all the data generated by the sensors to the cloud for processing (which can lead to high bandwidth cost and high latency), RSUs do the computation at the edge and only send the results to the cloud and the connected devices.

B. Attack model

In this study, we assume that the connection between RSUs and cloud is secure. We focus our attention to the threat to data generated by the sensors which is then forwarded to the RSUs. Road event reports devoid of content oriented privacy may result in eavesdroppers disclosing the road event report of the source and make the receiver get false road event reports. Malicious attackers may modify or fabricate the data for their own purposes. particularly, the adversary can control the whole communication channel and monitor all the data pass through the channel. The adversary can also tamper the message, drop some packets and even replace the original message. Furthermore, the adversary can also capture and compromise a small number of RSUs and mobile sensors. All the data transmitted to/through compromised RSUs and mobile sensors can be intercepted and analyzed by the adversary. Moreover, we also take into account the scenario where some RSUs become malicious and can transmit forged reports to vehicles to make them react in a certain way. At the same time, a vehicle or a drive could become malicious by generating false reports for his own benefits, for example, gaining credits for contributing to a crowd sensing task. Ultimately, the third trust party that is the CC in this application scenario may disclose users authentication keys and fabricate the road event reports.

Design goals

In this paper, we aim to achieve the following security
and performance objectives based on the system model and potential threats.

1) Security objectives

Data confidentiality and integrity. All accepted messages should be delivered unaltered, and the origin of the messages should be protected i.e.,from revealing private and sensitive information.

Mutual authentication. The mobile sensors and the RSU should authenticate each other in order to guarantee that the data from the source and once received is unaltered.

Anonymity. The identities of mobile sensors should be hidden from a normal message receiver during the authentication process to protect the sender's private information.

Key escrow resilience. The key generation center doesn't have the users full private keys. Therefore, we ensure that the adversary cannot get user's full private keys if KGC is compromised.

2) Performance objectives

Low communication overhead and fast verification. The security scheme should be efficient in terms of communication overhead and acceptable processing latency. A large number of report signatures should be first verified and then unsigncrpted in a short interval.

Robustness. The data generated via mobile sensors should not be accessed in case part of the private keys is infiltrated.

Light weight. Mobile sensors and devices have constraints such as limited power and storage.

Therefore the proposed scheme should have low computational cost

PROPOSED CLASC

In this section, we propose an efficient CLASC scheme that serves as the design basis for our privacy-preserving protocol.

We propose a solid CLASC scheme based on the schemes of Eslami et al. [12] and Lu et al. [13]. They utilize the bilinear map that is an efficient way of pairing. However, their schemes may suffer from high computational complexity because of the number of pairing operations for signcryption, aggregate,aggregate verification and aggregate unsigncryption. Therefore, we address this problem by reducing pairing operations that provide low computational and communication cost. The proposed CLASC scheme is composed by the following six algorithms.

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

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

- Chooses a cyclic multiplicative group GT of the same order q and a bilinear map ^ e : G G ! GT
- Randomly selects a master private key s 2 Z ——————————q and compute the master public key Ppub = sP .
- Selects four secure hash functions H1 :f0; 1g ——————————!Z ——————————q, H2 :f0; 1g——————————! f0; 1gn here n is the bit-length of
plaintexts, H3: f0; 1g —————————— ! G and H4: Z——————————q ! G.
- Publishes the system parameter params =(G; GT; ^ e; P; q; Ppub; H1; H2; H3; H4) and the master
private key s will be kept secure by the KGC.
Key-Generation: This algorithm is interactively performed by the user ID I and KGC as follows:
- The user ID i randomly chooses x i 2 Z——————————q as the secret value and computes a partial public key Y ib = x i P .
- The user sends its identity and partial public key(IDi; Yib) to the KGC.
- The KGC then randomly selects y i 2 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 (Yib; Yia).
- The KGC computes the partial private key Di = yi + s —————————— Qi where Qi = H1(IDi) ,and Di issent securely to the user ID i
- The user ID I judges the validity of the partial private key by checking Di P = Y ia + PpubH1(ID i).Notably, these procedures finish three different algorithms which are, set-secret-value, partialprivate-key-extract and set-public-key of the proposed scheme. These algorithms generate public key (Yib; Yia) that is kept in the public tree by the KGC,and the full private key (xi ; Di) is kept secret by the user.

PROPOSED PRIVACY-PRESERVING PROTOCOL

In this section, we present the details of our privacy-preserving protocol. In this application scenario, mobile sensors are considered as a fog device, which aggregates the data, aggregates verification and then aggregates unsigncryption. Our certificateless aggregate signcryption scheme is introduced in the protocol to fulfill the design objectives. The proposed protocol consists of four steps: system initialization, data formulation and sending, SRER aggregated verification, and data receiving.

A. System initialization

The mobile sensors and RSUs register to the CC to generate their full private keys and public keys. Moreover, it determines the format of road event report that is generated by the mobile sensors. Furthermore, routing is also established in this part. Given the security parameter k, the CC first generates the bilinear parameters (G;G_T ;e;^ P; q) by running Gen(k). Then, the CC selects a random s 2 Z_q as its master secret key and computes its master public key P_{pub} = sP . Additionally, the CC chooses four secure hash functions: H_1 :f0; 1g Z_q , H_2 :f0; 1g ! f0; $1g^n$ here n is the bit-length of plaintexts, H_3: f0; 1g ! G and H_4: Z_q ! G. After that, the system parameters params will be published, which include

(G; G_T ; e;^ P; q; P_{pub}; H_1; H_2; H_3; H_4).

A significant task of the setup procedure is to determine the format of secure road event report $SRER_{ij}$. For a road event RE_i , the mobile sensors Sen_jwill generate the data where $Data_i$ = (T ime_{ij}; $Location_i$; $Signals_i$) and the $SRER_{ij}$ will securely forward to the RSU in the format $SRER_{ij}$ = (Q_j; Signcrypt($Data_i$)) where,T ime_{ij} - denotes the time when the vehicle j makes the claim on this emergency event i.

$Location_i$ - denotes the place where the road event takes place.

Q_j - denotes the pseudo identity of the mobile sensor that generates the claim.

$Data_i$ - denotes a report generated by a mobile sensor about road event.

$Signcrypt_ij$ - denotes the signcryption generated by the sensor Sen_j on the road event RE_i that sends to RSU.

Mobile sensors and RSUs can join the system by performing the following Steps:

A mobile sensor Sen_j can randomly choose x_j 2 Z_q as its secret value and compute its partial public key $Sen_{jb} = x_jP$. To keep the identity privacy, the Sen_j can also randomly choose Q_j as its pseudo identity.

Sen_j sends its identity and partial public key (Sen_j; Sen_{jb}) to the CC for registration.

The CC randomly selects y_j 2 Z_q and compute an-other partial public key for the mobile sensor $Sen_{ja} = y_jP$.

The CC then computes the partial private key $D_j = y_j + s\ Q_j$,where $Q_j = H_1(Sen_j)$, for the register Sen_j with partial public key Sen_{jb}.

D_j is sent to the Sen_j via a secure channel. The full public key (Sen_{jb}; Sen_{ja}) is kept in the public tree by the CC.mobile sensor Sen_j receives the partial private key D_j and concatenates with its secret value x_j to form

its full private key (D_j; x_j) The user Sen_j judges the validity of the partial private key by checking $D_jP = Sen_{ja} + P_{pub}H_1(Sen_j)$.

B. Data formulation and sending

This part is performed by the source with a mobile sensor Q_j. A road event RE_i is sensed by one or multiple mobile sensors and then $Data_i$, which include (T ime_{ij}; $Location_i$; $Signals_i$), is discovered. After that, Q_j with encrypted $Data_i$ as a $SRER_{ij}$ sends to the RSU as fog device receiver. Then, Q_j utilizes the certificateless signcryption algorithm on $Data_i$ as follows:

- Sen_j randomly selects $r \in Z_q^*$ and compute $T_j = rP$,
- Compute $Z_b = rPK_{rb}$,
- Compute $Z_a = r(PK_{ra} + P_{pub}Q_j)$,
- Compute $h_a = H_2(ID_R||Pk_{ra}||PK_{rb}||\Delta||T_j||Z_b||Z_a)$,
- Compute $K_j = h_a \oplus Data_i$ and compute,
- $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_j||K_j||Q_j||Sen_{ja}||Sen_{jb})$
- Compute $h_c = H_4(\Delta)$,
- Compute $\alpha_j = D_j h_c + rh_b + x_j h_c$.

It is worth pointing out that using only pseudo identities in vehicular networks to preserve driver privacy is insufficient [31].This is because due to the nature and characteristics of vehicular networks, vehicle mobility can be predicted. As a result, even the vehicle's pseudo identities change, the reported locations in the future traffic information from a vehicle can be used to link pseudo identities and even worse a real-world identity could be discovered. In order to address the problem, several mechanisms have been proposed in the past. For example, using silent period [31], creating mix-zones [32]. In our proposed scheme, we can adopt the mix-zone technique. For instance, when all the vehicles approaching an intersection where there is an RSU deployed, they coordinate with each other and change their pseudo identities at the same time. Also, their public and private keys are updated accordingly with the involvement of CC through the RSU. CC will update the public tree with the vehicles new public keys as well.

C. SRER aggregated verification

Notably, this application scenario is based on Vehicles to Infrastructure communication (V2I) which means mobile sensors can directly communicate with the RSUs. Once a road event RE_i is sensed by one or multiple mobile sensors, they then generate a road event report $SRER_{ij}$ that includes accurate information such as time, location and the type of event. We utilize this system on the highway, that massive of objects can pass through. Therefore, a bunch of data will be generated by the various mobile sensors and sent to the closest RSU. If the RSU receives each ciphertext separately to verify the signature and then usingcrypt it, this process will have a long time that may lead to long delay. We exploit an advantage of fog devices, which are efficient in computational cost and bandwidth. Therefore, our protocol provides the aggregation property that the RSUs can aggregate all the ciphertexts generated by the multiple mobile sensors.This process provides a sufficient amount of efficiency over sending each ciphertext separately. Whenever receiving a SRER, the aggregator will perform the SRER aggregation and SRER batch verification operations as follows.

SRER aggregation: Aggregate SRER is used to aggre-gate multiple SRERs into a single SRER. For a road event RE_i , given n SRERs $SRER_{ij}$ = (Q_j; Signcrypt($Data_i$)) by mobile sensors Sen_1; ::::Sen_n, we can obtain

$SRER_{agg}$=Q_1:::Q_n; Signcrypt$(Data_i)^i{}_1$... Signcrypt$(Data_i)^n{}_i$). This algorithm is performed by an aggregate signcryption generator on the receiver as follows:

This algorithm takes a collection of individual ci-phertexts C_j = (T_j; K_j; $_j)^n{}_{j=1}$ generated by mobile sensors with $(Q_j)^n{}_{j=1}$ to a receiver with identity ID_R under the same state information , which is consid-ered as a secret value to insure the aggregation phase.

SRER batch verification: This step performs signature batch verification for all the ciphertexts simultaneously. Given the signature aggregation sig_{agg}, the report sets $SRER_{ij}$j i n , corresponding public keys (Sen_{ja}; Sen_{jb})j i n for all the mobile sensors and a receiver's identity ID_R, and its corresponding public key (P k_{ra}; P K_{rb}) using the same state information .

In summary, the tuples given are $(SRER_{agg}, (Q_j)_{i=1}^{n}, (Sen_{ja}, , Sen_{jb})_{j=1}^{n}, ID_R, (Pk_{ra}, PK_{rb}), x_R, D_R, \Delta)$. In order to verify the signature, this algorithm computes the following:

- $h_b = H_3(ID_R||Y_{ra}||Y_{rb}||\Delta||T_i||K_i||Q_i||Sen_{ja} ||Sen_{jb})$, for $j = 1, ..., n$
- $h_c = H_4(\Delta)$,

The signature aggregation Sig_{agg} accept if

$$\hat{e}(sig_{agg}, P) = \hat{e}(\sum_{i=1}^{n}(sen_{ja} + P_{pub}Q_j, h_c) \prod_{i=1}^{\infty} \hat{e}(\sum_{i=1}^{n} T_i, h_b)\hat{e}(\sum_{i=1}^{n} sen_{jb}, h_c)$$

If the batch verification holds, the aggregator will accept SRERs in list V as a valid SRERs. Then the aggregated SRER $SRER_{agg}$ in V will be forwarded to complete unsigncryption step. Once a road event report SRER is verified valid, RSU pursues the next unsigncryption step.

D. Data receiving

The RSUs decrypt the SRERs when the signature ver-ification outputs true. The RSU continues to complete the decryption phase as follows:

- $Z_b' = x_r T_j$, $Z_a' = D_r T_j$
- $h_a' = H_2(ID_R||Pk_{ra}||PK_{rb}||\Delta||T_j||Z_b'||Z_a')$,
- $Data_i' = K_j \oplus h_a'$

IV. CONCLUSIONS

In this paper, we tend to propose a new efficient certificateless aggregate signcryption (CLASC) theme. we tend to then designed a privacy-preserving vehicular crowdsensing road surface con-dition monitoring system using fog computing supported the planned CLASC theme. additionally, the planned privacy-preserving protocol meets the safety needs like knowledge confidentiality and integrity, mutual authentication, namelessness and key written agreement resilience. in depth comparisons of procedure value and communication overhead show that the planned theme can do far better potency than the existing schemes.

REFERENCES

[1] M. Perttunen, O. Mazhelis, F. Cong, M. Kauppila, T. Leppanen, J. Kantola, J. Collin, S. Pirttikangas, J. Haverinen, T. Ristaniemi, and J. Riekki, "Distributed road surface condition monitoring using mobile phones," Ubiquitous Intelligence and Computing, Springer, pp. 6478, 2011.

[2] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden and H. Balakrish-nan, "The pothole patrol: Using a mobile sensor network for road surface monitoring," Proc. 6th Int. Conf. Mobile Syst., Appl., Serv., pp. 29-39, 2008.

[3] G. Strazdins, A. Mednis, G. Kanonirs, R. Zviedris, and L. Selavo, "Towards Vehicular Sensor Networks with Android Smartphones for Road Surface Monitoring," 2nd International Workshop on Networks of Cooperating Objects (CONET'11), Electronic Proceedings of CPS Week'11, 2011.

[4] Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," Telecommunication Networks and Applications Conference (ATNAC), Australasian, pp. 117-122, 2014.

[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," proceedings of ACM SIGCOMM, Helsinki, pp. 13-16, 2012.

[6] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39-68, 2007.

[7] T. Little and A. Agarwal, "An information propagation scheme for VANETs," IEEE Intell. Transportation Syst., pp. 155-160, 2005.

[8] C. Li, M. Hwang, and Y. Chung, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Computer Communication, vol. 31, pp. 2803-2814, 2008.

[9] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," 2008 IEEE International Conference on Communications, Beijing, pp. 1451-1457, 2008.

[10] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks," 2008 IEEE International Conference on Communications, Beijing, pp. 1436-1440, 2008.

[11] M. Barbosa and P. Farshim, "Certificateless signcryption," Proceedings of the 2008 ACM symposium on Information, computer and communi-cations security, pp. 369-372, 2008.

[12] Z. Eslami and N. Pakniat, "Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model," Journal of Computer and Information Sciences, vol. 26, no. 3, pp. 276-286, 2014.

[13] H. Lu, Q. Xie, "An efficient certificateless aggregate signcryption scheme from pairings," 2011 International Conference on Electronics, Communications and Control (ICECC), pp. 132-135, 2011.

[14] P. Mohan, V. N. Padmanabhan and R. Ramjee, "Nericell: rich monitor-ing of road and traffic conditions using

mobile smartphones," Proceedings of the 6th ACM conference on Embedded network sensor systems, ser. SenSys '08, pp. 323-336, 2008.

[15] Mednis, A. Elsts and L. Selavo, "Embedded Solution for Road Condition Monitoring Using Vehicular Sensor Networks," Proc. 6th IEEE Int'l Conf, Application of Information and Communication Technologies (AICT'12), pp. 1-5, 2012.

[16] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," Proceedings of the Asiacrypt 2003, LNCS, vol. 2894, pp. 452-473, 2003.

[17] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans, Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-119, 2014.

[18] W. Dent, "A survey of certificateless encryption schemes and security models," International Journal of Information Security, vol. 7, pp. 349-377, 2008.

[19] Hu, D. Wong, Z. Zhang, and X. deng, "Certificateless signature: a new security model and an improved generic construction," Designs, Codes Crypt, Vol. 42, pp. 109-126, 2007.

[20] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signature revisited," Proc. ACISP2007, pp. 308-322, 2007.