A CERTIFICATE LESS AGGREGATE SIGNCTYPTION FOR ROAD EXTERIOR CONDITION SUPERVISING SYSTEM

Ms. Salamma Ilari[1]
3rd Year Student ,
Department of Computer Science,
SV U CM & CS, Tirupati.

Prof. S. Rama Krishna[2],
Professor,
Department of Computer Science,
SV U CM & CS,, Tirupati.

Abstract: In the recent past, great attention has been directed towards road surface condition monitoring. 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, 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. 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, the paper proposes a certificate less aggregate signcryption scheme (CLASC) that is highly efficient. 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.

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

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 smartphones 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 smartphones, smartwatches, 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 crowdsensing and vehicle based sensing alongside advances in cloud computing allow for data collection, analysis, storage, processing and transmission in an efficient manner.

Cloud based architecture is used by various applications, such as smart city application, 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. For example, hitting a pothole. The data is then transferred to a centralized cloud system from where it is processed. 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 unauthenticated 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.

Disadvantages:

1. 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.

2. Unauthentic interconnection of mobile sensors and the corresponding road infrastructure.

METHODOLOGY

In order to adjust current work by adopting signcryption technique, certificate less schemes of signcryption (CLSC) are used in capturing communication with respect to both confidentiality and unforgeability. The first scheme of CLSC was proposed by 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 scalability, 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. Proposed certificate less aggregate signcryption scheme (CLASC) . 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.

Advantages:

1. CLASC scheme has the lowest computational cost compared to the existing schemes.

2. A new efficient certificate less aggregate signcryption scheme CLASC with a significant improvement over pairings required by existing aggregate signatures verifications and unsigncryption.

3. For enhancing security in data transmission of vehicular crowd sensing based road surface condition monitoring system using fog computing.

Certificate less Aggregate signcryption scheme

The proposed protocol is based on privacy preservation using 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. Certificateless public key cryptography was first proposed as a way of overcoming the challenges associated with key escrow as applied in cryptography approaches that are identity-based and hence maintain certificate freeness. There are several schemes proposed in encryption digital signature and signcryption certificateless cryptography. Since we are using certificateless aggregate signcryption, we evaluate multiple aggregate signcryption as used in identity based aggregate schemes of signcryption. Certificateless aggregate signcryption scheme (CLASC) is emphasized an appropriate secure model as has been proven in its use in the random oracle model.Further,argued in favor of certificateless aggregate signcryption scheme as a secure system.

Control center

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 sensitive data. It is assumed that the CC is powered with sufficient computation and storage capabilities.

Framework of certificateless aggregate signcryption

first define the participants involved in a framework of a certificateless aggregate signcryption scheme. They are composed of four parties which are: a key generator center KGC, an aggregating set IDi of n users with an identity IDign i=1, a receiver with an identity IDR and an aggregate signcryption generator.

PROPOSED CLASC

We propose a solid CLASC scheme based on the schemes. 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.

Conclusion:

In this paper, we propose a new efficient certificate less aggregate signcryption (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.

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. Balakrishnan, ”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] I. 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 RSUAided 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.

Authors Profile

ILARI SALAMMA, received Bachelor of Computer Science degree from Sri Venkateswara University, Tirupathi in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2016-2019. Research interest in the field of Computer Science in the area of Cloud computing , Cloud Computing and Software Engineering.

Prof Dr S. Ramakrishna, working as a Professor in Dept of Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati, (AP)-India. Received M.Sc, M.Phil, M.Tech (IT) and Doctorate in Computer Science from S.V University, Tirupati, having 27 years experience in teaching field. Additional Assignments Working as Dean of Examinations for S.V University, Worked as Additional Convener for S.V University RESET Examinations, Worked as Coordinator for M.Sc Computer Science, Worked as BoS Chairman in Computer Science. Research Papers Published in National & International Journals :99, Total Number of Conferences participated :33, Total number of Books Published:7, Total number of Training Programs Attended : 3, Total number of Orientation & Refresher Courses Attended : 4.Number of research degrees awarded under my guidance :- M.Phil: 20,Ph.D:20.