IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 68-70
International Conference on Management Practices, Innovations & Research 2019

A Survey on Secure Access Model for Vehicular Cloud Computing

[1]Tejashree Sahare, [2]Prof. Jayant Adhikari
[1]M.Tech Student, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.
[2]Assistant Professor, Department of Computer Science & Engineering, Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, Maharashtra, India.

Abstract —*Cloud computing becomes he topic now a days.Vehicular cloud computing is a novel technical paradigm with enormous security solution. The vehicular cloud pattern aims to enhance computing infrastructure & elaborating security framework with potentially revolutionizing and myriad challenges. The ultimate suggestion of this paper is to address several securities challenges, the problem of unauthorized users accessing and stealing data & privacy issues and to provide unique evolving approach for directional security scheme. Although security issues have created awareness in cloud users, but still is a critical concern in cloud computing, so to overcome this exacerbate challenges in cloud, we propose a reasonable efficient & new directional security scheme that approaches to infrastructures security, authentication and confidentiality, reliability, scalability, cloud vulnerabilities, establishing trustworthy in vehicular cloud and privacy threats. We propose a secure and revocable access control scheme for vehicular cloud computing in this paper, in which the requester can decrypt the ciphertext with only a small amount of computation.*

Keywords*– Access Control, Cloud Computing, CP-ABE, VANETs.*

I. Introduction

Recently numerous study present on cloud, it offers various services to end user. Cloud computing has begun to emerge as a hotspot in both industry and academia; It represents a new business model and computing paradigm, which enables on-demand provisioning of computational and storage resources. In an effort to help their vehicles compete in the market-place, car and truck manufacturers are offering increasingly more potent onboard devices, including powerful computers, a large array of sensors, radar devices, cameras, and wireless transceivers. However, in the vehicular cloud computing, there is still the problem of unauthorized users accessing and stealing data. In fact, security ranked first as the greatest challenge issue of vehicular cloud. As Vehicular networking involves the storage, compute and analysis of massive vehicular data. Vehicular cloud computing, as a special cloud computing platform, seamlessly combines VANETs and conventional cloud computing. Our work more specific to the different security issues and the associated challenges that has emanated in the vehicular cloud computing.

In the traditional ciphertext-policy attribute-based encryption (CP-ABE) scheme, a trusted central authority is employed to manage attributes and distribute keys. Based on multi-authority CP-ABE (MA-CP-ABE), we propose a secure and revocable access control scheme for vehicular cloud computing in this paper, in which the requester can decrypt the ciphertext with only a small amount of computation. We show our MA-CP-ABE scheme can prevent static corruption of authorities in the standard model under the decisional q-parallel Bilinear Diffie-Hellman Exponent (BDHE) assumption. Theoretical analysis and experimental simulation results show that our scheme has lower communication cost and lower computational complexity than other schemes. Hence the main contribution of this paper is to provide the appropriate security framework.

II. Literature Review

In paper [1] authors explain VANET architecture and design principles. VANET has been a core networking technology to provide safety and comfort to drivers in vehicular environments. Emerging applications and services, however, require major changes to its underlying computing and networking models, which demand new network planning for VANET. Their article especially examines how VANET evolves with two emerging paradigms: vehicular cloud computing and information-centric networking. VCC brings the mobile cloud model to vehicular networks and thus changes the way of network service provisioning, whereas ICN changes the notion of data routing and dissemination. Authors envision a new vehicular networking system, vehicular cloud networking, on top of them. Their research scrutinizes its architecture and operations, and discusses its design principles.

In paper [2] authors propose the VANET-Cloud according to them with to the increasing number of traffic accidents and dissatisfaction of road users in vehicular networks, the major focus of current solutions provided by intelligent transportation systems is on improving road safety and ensuring passenger comfort. Cloud computing technologies have the potential to improve road safety and traveling experience in providing flexible solutions (i.e., alternative routes, synchronization of traffic lights, etc.) needed by various road safety actors such as police, and disaster and emergency services. In order to improve traffic safety and provide computational services to road users, a new cloud computing model called VANET-Cloud applied to vehicular ad hoc networks is proposed. Various transportation services provided by VANET-Cloud are reviewed, and some future research directions are highlighted, including security and privacy, data aggregation, energy efficiency, interoperability, and resource management.

In paper [3] authors discuss the Vehicular cloud networks: Challenges, architectures, and future directions. Vehicular Cloud Computing is a promising solution to exploit the underutilized vehicular resources and to meet the requirements of VANET applications and services. Although modern vehicles have important capacities of computation and storage, there is an increasing need for resources, in particular, for safety applications which require the cooperation between vehicles. The vehicular cloud offers to users the opportunity to rent resources on-demand or to share them freely to run their applications or to carry out some tasks. Even though this paradigm is feasible, its implementation still faces problems. Many researchers have focused on thearchitectural design in order to overcome different challenges and consequently meet user requirements to provide him/her with reliable services. In their work, they survey the vehicular cloud paradigm. They also focus on its features and architectures. Authors first present a brief overview of the motivation of vehicular cloud. Then, they explore challenges related to its design. Furthermore, Authors highlight the features of existing vehicular cloud architectures: we provide a taxonomy of vehicular cloud followed by our classification criteria. Finally, authors discuss issues that can be considered as open research directions.

In paper [4] authors considers another necessity of ABE without sourced decryption that is termed as verifiability of transformations. Informally, it ensures that a customer can capably check if the change is done effectively or not. Their system demonstrate that the new plan is both secure and unquestionable, without relying upon arbitrary predictions.

In their work, they propose a different view for ABE that, all things considered, wipes out the overhead for clients. However, their construction does not consider overhead computation at the attribute authority involved in the key-issuing process.

Here, an ABE system is proposed by Green et al. [5] with outsourced decryption that to a great extent takes out the overhead of decryption for clients. In ABE system, a client keep up an untrusted server, say a CSP, with a change key that allows the cloud to decipher any ABE ciphertext fulfilled by that clients properties and it simply think of some computational overhead for the customers to recoup the plaintext from the changed ciphertext. Security of an ABE framework with redistributed decoding guarantees that an enemy (Including a malignant cloud) won't have the ability to analyze anything related to the encrypted message; in any case, it does not give any assurance of definiteness of the transformation performed by the cloud.

In this paper [6], the authors proposed a cryptosystem that provides fine-grained access control to encoded information that they called Key Policy ABE(KP-ABE). In their cryptosystem, ciphertext are classified with different characteristics and secrete keys are set with access structures that limits which ciphertext a user is capable to interpret. They have applied their construction in forensic analysis and broadcast encryption. However, their systems fail to hide the attributes that does the encryption. Hence the issue of attribute hiding is left open.

Author Yu et al. [7] consider the issue of user revocation which involves re-encrypting the data that is obtainable to the customer leaving the system and updating the private keys of users remaining in the system. They have proposed a scheme that enables the owner of the data to outsource the task of re encryption and private key updates to a third party without revealing the content and the user information. They have very well attained the finely grained and scalable access in cloud computing. However, the complexity in user revocation elaborate with the expansion in number of users which makes the system complex. In addition, their scheme does not support user accountability.

The notion of ABE was proposed in this paper [8] as fuzzy version of Identity Based Encryption (IBE). In Fuzzy IBE, Sahai et al. consider identity as a practical characteristics set. A Fuzzy IBE scheme considers a private key for an identity, to interpret a ciphertext combined with a personality, if and just if the identities w and w are near one another judged by some metric. A Fuzzy IBE approach can be joined with secure encryption utilizing biometric contributions as personalities; the rupture obstruction characteristics of a Fuzzy IBE course of action has accurately what considers if its utilization of a biometric characters. Moreover, they demonstrate that Fuzzy- IBE can be utilized for different kind of use that they term ABE. Here they exhibit two head ways of IBE Fuzzy orchestrates. Their progressions can be seen as an IBE under two or three attributes that make a (delicate) character of a message. Their IBE arrangements are couple oversight patient and private against plot attacks. Besides, the key advancement does not use arbitrary prophets. Creator exhibit the privacy of their arrangements under the Selective-ID security display.

Cheung et al. [9] have proposed yet one another type of ABE scheme known as ciphertext policy attribute based encryption (CP-ABE). Where every private key is set with properties, and each ciphertext is named with an access strategy. Decryption is done if and just if the client property set achieve the ciphertext access structure. This can get fine-grained access control on shared information in various useful settings. Here, Author can take just CP-ABE in record designs in which get to structures are AND gates on positive and negative qualities. Their important arrangement has been shown to be picked plaintext assault (CPA) secure underneath the decisional bilinear Diffie-Hellman presumption however the usage of autonomous occasions of CP-ABE encryption, and furthermore the security of this proposition stays as an open issue.

III. Proposed Methdology

The figure 1 shows proposed system architecture.

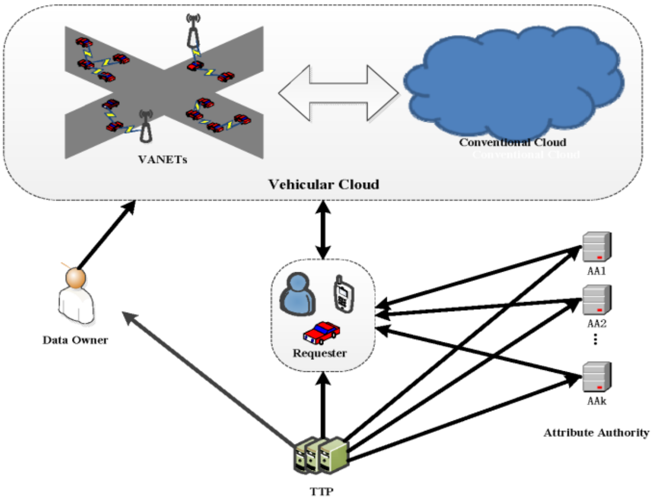

Fig 1. System Architecture

IV. Conclusion

Here we utilized vehicular cloud pattern to improve computing infrastructure and security by locating numerous security challenges. User which is not authorized access, steal data and privacy. We proposed efficient & new directional security scheme to overcome security and privacy challenges in cloud computing, and that scheme approaches to infrastructures security, authentication and confidentiality, reliability, scalability, cloud vulnerabilities, establishing trustworthy in vehicular cloud and privacy threats. Also here we proposea secure and revocable access control scheme for vehicular cloud computing.

References

[1]. E. Lee, E.K. Lee, M. Gerla, et al. Vehicular cloud networking: architecture and design principles[J]. IEEE Communications Magazine, 2014, 52(2): 148- 155.

[2]. S. Bitam, A. Mellouk, S. Zeadally, VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks[J]. IEEE Wireless Communications, 2015, 22(1): 96-102.

[3]. T. Mekki, I.Jabri, A. Rachedi, et al., Vehicular cloud networks: Challenges, architectures, and future directions, In Vehicular Communications, 2017, 9: 268-280.

[4]. J. Lai, R. Deng, C. Guan, and J. Weng, Attribute-based Encryption with Verifiable Outsourced Decryption, Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354,Aug. 2013.

[5]. M. Green, S. Hohenberger, and B.Waters, Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Secur. (SEC). Berkeley, CA,USA: USENIX Association,2011, p. 34.

[6]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data, in 2006, Proc. 13th ACM Conf. Comput. Commun. Security, pp. 89-98.

[7]. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, Fine-Grained Data Access Control in Cloud Computing, in Proc. IEEE 29th INFOCOM, 2010, pp.534-542

[8]. A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, in Proc. Adv. Cryptol.- EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer- Verlag.

[9]. L. Cheung and C. Newport, Provably Secure Ciphertext Policy ABE, in Proc. 14thACM Conf. CCS, 2007, pp. 456- 465.

[10]. S. Ruj, A. Nayak and I. Stojmenovic, DACC: Distributed access control in clouds. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, 2011: 91- 98.