International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Confederate Process Key Agreement Scheme For Cloud Assisted Vehicular Internet Of Things

[1] Sivannarayana Nerella, [2] G.Sateesh
[1,2]M.Tech & Asst.Professor,
[1]Tirumala Engineering College,[2]Guntur Engineering College,
[1] *nerella.siva@gmail.com*, [2] *sateesh4u.325@gmail.com*

Abstract: In a series of recent papers have promoted the vision of vehicular clouds (VCs) nontrivial extension, along several dimensions, of conventional 6 cloud computing. In addition, the previous functions of the Intelligent Transportation System (ITS) such as traffic accident prevention and providing traffic volume information have been combined with cloud computing. Security and privacy is important in Internet of Vehicles (IoV) where access to electronic control units, applications and data in connected cars should only be authorized to legitimate users, sensors or vehicles. This framework is designed to overcome the challenges including high computation costs, low flexibility in key management, and low compatibility in deploying new security algorithms in IoT, especially when adopting advanced cryptographic primitives. They are connecting with customers through internet. VC concept is an important society impact that needs security and privacy issues that should be corrected. Furthermore, we present taxonomy for vehicular cloud where distinctive attention has been dedicated to the substantial applications, inter cloud communication systems, cloud formations, and broad aspects of seclusion and safety issues. We propose a novel middleware architecture to solve the above issues, and discuss the generic concept of using fog computing along with cloud in order to achieve a higher security level. We discuss these concepts in detail, and explain how our proposal is effective to cope with some of the most relevant IoT security challenges.

Index Terms: Ressource-Constrained Devices, privacy, security, vehicular cloud, Security, Edge Computing, Authentication, Access Control, Security requirements,

1. INTRODUCTION

Internet of Things (IoT) is the new era of technology which envisions making human lives smarter. The concept has attracted wide applications and services in variety of domains including health-care, homes, industry, transportation, power grids [1]. The smart home needs to protect the identity of each controller to conceal sensitive behaviors of each individual, and the smart grid will need to conceal electricity consumption against analysis in appliance usage each IoT application, there are generically challenging issues in guaranteeing security in IoT [2]. Cloud computing is the framework which permit the client to utilize the assets on the premise of pay-peruse [3]. The assets might incorporate programming similar to, application programming, working framework and equipment like capacity, processor and so forth [4]. This makes it feasible for improving new progressive applications plus services for enhancing security, handling traffic and also reducing pollution [5]. Our proposed solution includes data confidentiality, authentication and access control mechanisms using the fog computing approach. Our middleware not only pre-process data locally, but also acts as smart gateway to enhance the utilization of network and cloud resources [6], In addition, VCC-SSF includes a new active payment service that meets user requirements through the Payment as well as Accident Management Services to actively provide traffic accident prevention and accident response and management [7].

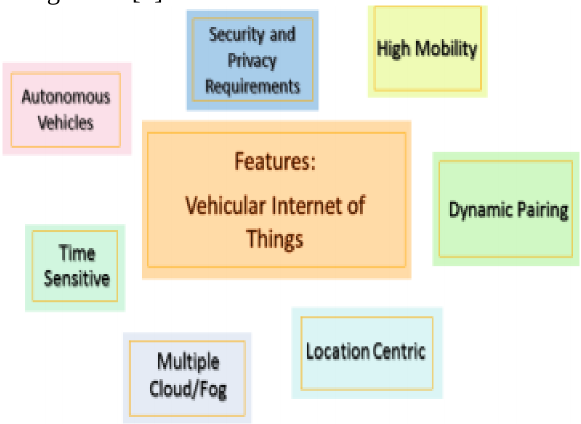

Figure `1: IoV Distinguishing Characteristics

2. RELATED WORKS

While previous ITSs established an overall communication infrastructure to provide traffic information as well as communication between vehicles between vehicles and the infrastructure ITS now has the goal of providing various services to drivers pedestrians based on a communication infrastructure [8]. The bottom layer of ACO architecture comprises physical smart devices like sensors, RFIDs, beacons, and ECUs, which are responsible for data sensing and accumulation, and for sending data to upper layers [9]. The computational infeasibility of resource constrained IoT devices for advanced cryptographic algorithms with high computation complexity the inflexibility in supporting new security functions due to independent design of each communication standard and the layered architecture of networking [10]. The internet cloud is created by cloud provider where the services are processed and maintained by him where as in vehicular cloud the cloud is created on the fly by using the resources of the vehicle, this can be done by making the vehicles to interact with each other [11]. VANET is identified as a subsection of Mobile Ad Hoc Networks is statically desirable for considering VANETs as an idiosyncratic research field, specifically in the light of security implementation [12]. Indeed, many other papers in the literature point out their sever security weaknesses. Furthermore the authors identify IoT security requirements and analyze the existing IoT middleware solutions in the literature [13].

3. SYSTEM ARCHITECTURE

The common security requirements of confidentiality, integrity, availability, and non-repudiation, the ReS IoT gives rise to additional security issues regarding the computation of security functions (SFs) on SAs for IoT devices [14]. The Security Layer is the layer providing functions such as authentication encryption, access control, and privacy protection. Furthermore it authenticates stationary and driving vehicles and encrypts personal identification and sensitive information [15]. The fog node receive computation requests and sensed data from various IoT devices and can be implemented in different devices such as edge servers, smart routers, base stations and gateway devices [16]. In addition, it enhance road security by sensing, collecting, and forwarding traffic data from and to vehicles and RSUs to perform suitable action in unwanted traffic circumstances like accidents or blocking [17].

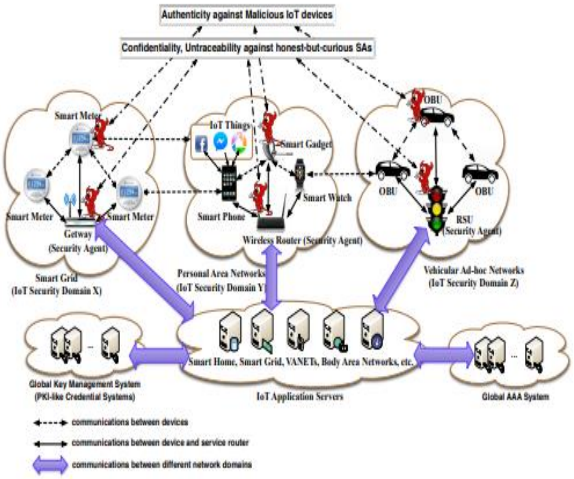
Authenticity against Malicious IoT devices
Confidentiality, Untraceability against honest-but-curious SAs
Smart Meter
Smart Meter
Smart Meter
Getway
(Security Agent)
Smart Grid
(IoT Security Domain X)
IoT Things
Smart Gadget
Smart Phone
Smart Watch
Wireless Router (Security Agent)
Personal Area Networks
(IoT Security Domain Y)
OBU
OBU
OBU
RSU
(Security Agent)
Vehicular Ad-hoc Networks
(IoT Security Domain Z)
Smart Home, Smart Grid, VANETs, Body Area Networks, etc.
Global Key Management System
(PKI-like Credential Systems)
IoT Application Servers
Global AAA System
communications between devices
communications between device and service router
communications between different network domains

Fig. 2.Ssystem Architecture Model of IoT Reconfigurable Security

4. PROPOSED SYSTEM

The network service providers and the vehicle drivers have access to trust. There will be a large number of government agents the Department of Motor Vehicles (DMV) and the Bureau of Motor Vehicles (BMV) is trusted organizations [18]. Only authenticated users can use the Payment Service, and the registered private information, payment information, and payment list are protected by encryption. The proposed Accident Management Service uses VCC. It has two modes: before and after an accident. Before an accident occurrence, it utilizes a human body detection sensor inside the vehicle to monitor the health status and driving capability of the driver [19]. Duplicate Address recognition plans have three important aims: (a) enhancing the accurateness of identifying address conflicts, (b) enhancing the detection victory ratio, plus(c) deducting the taken time for finding these conflicts [20].

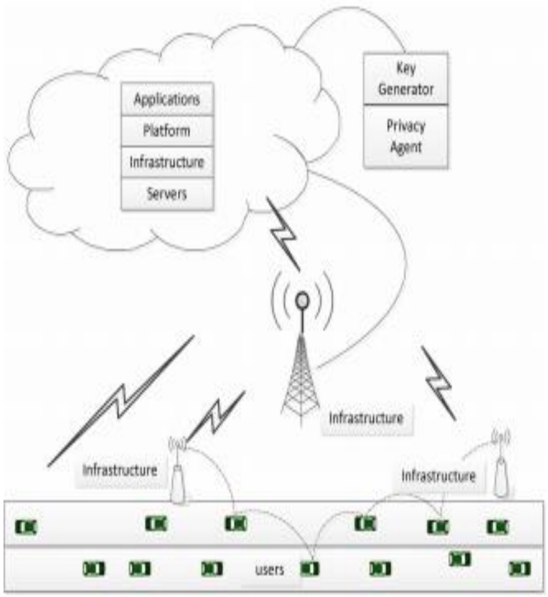

Fig. 3. Vehicles often communicate through multichip routing

5. IOT CONSTRAINED DEVICES SECURITY CHALLENGES

The security is challenges and necessitates new essential changes to the existing security solutions. Indeed most of the available security approaches are designed for regular internet and are geared toward protecting data centers, enterprise networks and consumer electronics [21].

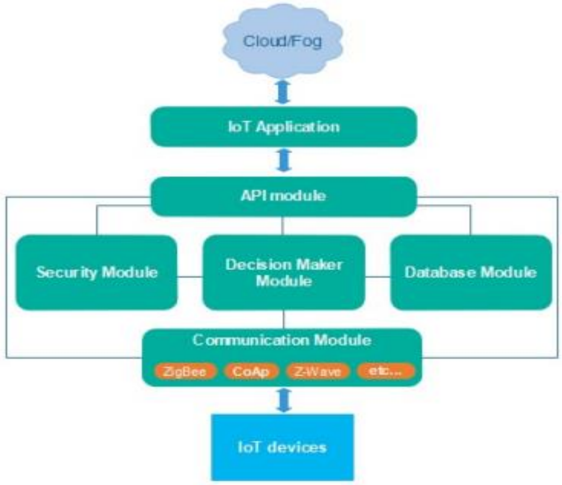

Figure 4: Proposed security architecture

5.1 Many Iot Devices Are Constrained And Difficult To Update

IoT devices can be geographically distributed; updating devices might turn out to be demanding and hard to manage. Usually brute force solutions are the main techniques used as incident response to solve security issues, and systems are required in a lot of cases to be offline in order to replace the compromised files and have the system cleaned up.

2. *Security Firewalls For Iot Devices Is Unpractical And Infeasible*

Many IoT devices such as sensors, wearable devices, vehicles, drones are placed in unprotected vulnerable physical environments. Consequently, accessing them through wired or wireless local network is a very feasible task [22]. Accessing the internal vehicle network by eavesdropping and false data injection is easily done through physically attaching low-cost and readily available tools such as dongles on the vehicle. Thus using firewalled castles is technically not possible, as placing a firewall on every single microcomputer can prove to be unmanageable, complex and costly.

3. *Public Key Infrastructures Iot Environments*

The verifier then validates cryptographically these claims. Unfortunately a large number of resource-constrained devices are not able to implement remote attestations algorithms and protocols because of their intensive processing requirements. Moreover remote attestation methods are geared toward allowing an individual device to attest for its own trustworthiness.

6. CLOUD ASSISTED VEHICULAR INTERNET OF THINGS

The vision of smart city and intelligent transportation encompasses connected cars and vehicular IoT as an important component. The eventual goal of IoV is the integration of vehicles, infrastructure, smart things, homes or ultimately anything to promote efficient transportation, accidental safety, fuel efficiency etc. and for pleasant travel experience to the driver [23]. A connected car has several ECUs and sensors on it, and hence is referred as a clustered object whereas a single ECU in a car generally performs one function and is an individual object. Such characterization is necessary as it drives our access control framework and models [26].

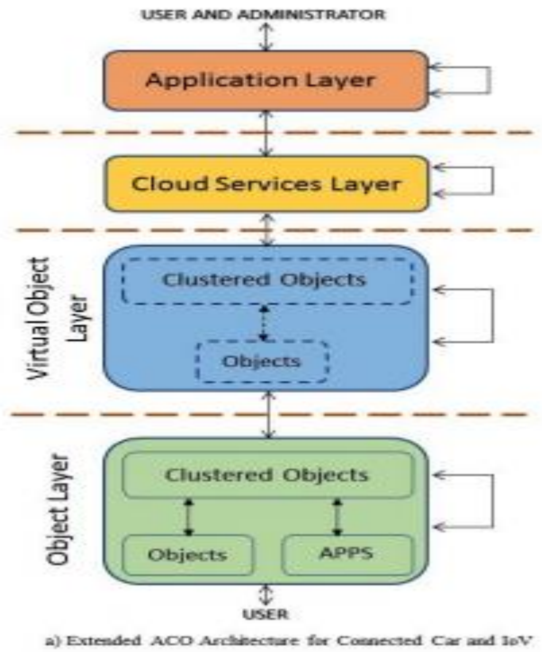

Figure 5: Extended ACO Architecture

A. Authorization Framework For Internet Of Vehicles

The dynamic and distributed nature of vehicular IoT brings in challenges to secure the ecosystem. Broad attack surface and numerous external interfaces along with the intrinsic characteristics of IoV makes it hard to ensure security and privacy of the components and data inside. Access controls are important to restrict unauthorized access to data, sensors, applications, infrastructure and other resources in connected cars and IoV [24].

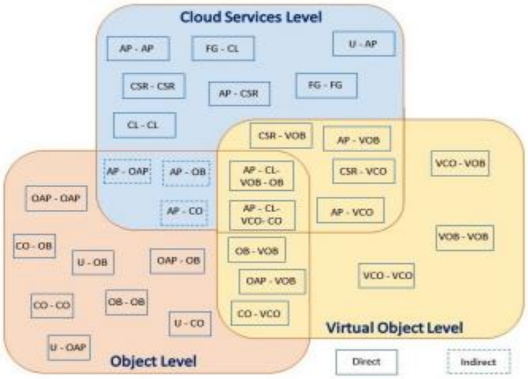

Figure 6: Different Interactions in IoV Ecosystem

B. Authorization Framework

Several interaction scenarios exist in Internet of Vehicles which makes it hard to comprehend different access control decision and enforcement points, together with other security requirements. Based on the extended ACO architecture, we have put together various vehicular IoT communications into three categories: Object Level, Virtual Object Level and Cloud Services Level [25]. Vehicular IoT mainly has two data exchange scenarios: static and dynamic, where static considers interaction due to long lasting relation for example, vehicle and owner or car manufacturer.

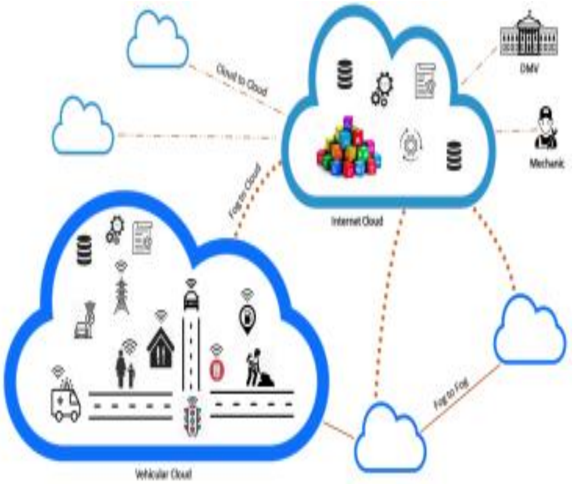

Figure 7: Connected Cars and Internet of Vehicles Ecosystem

7. PERFORMANCE OF RESIOT

This section evaluates the communication and computation costs of two RSFs. The advanced cryptographic algorithms are used such as Bone Boyne Sachem group signatures (BBS GS) and Goyal-Sahai Pandey Waters attribute-based encryption (GSPW ABE) for anonymous authentication and we present the computational time of the bilinear pairing related operations, including multiplication (Mul) exponentiation and pairing in the same bilinear pairing groups on both platforms by Java Pairing based library. We compare the performance of RSFs with the legacy solutions for two security requirements anonymous authentication and ABAC. Here, the legacy solutions mean the ones simply perform SFs (i.e., BBS GS and GSPW ABE) on IoT devices for the aforementioned security requirements.

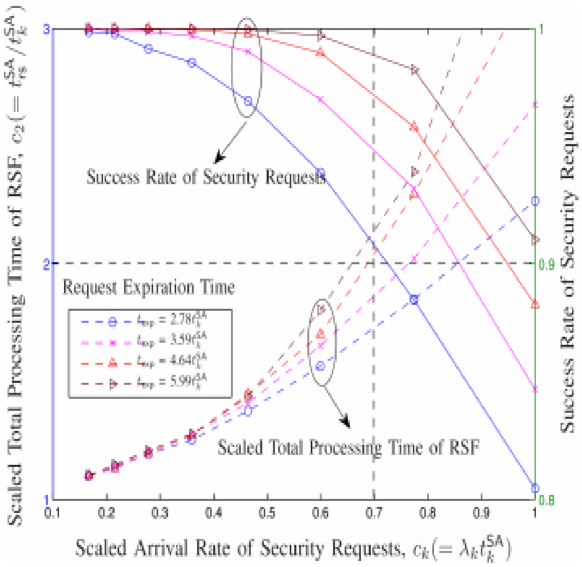

Fig. 8. This evaluates system processing time and success rate of security requests with different arrival rate of security requests and different request expiration time.

8. CONCLUSION

This paper describes about novelty in Intelligent Transportation System and also highlights the security issues that are caused due to the high mobility of the vehicles. To overcome security problem, the methodology used in VANET. The routing information is saved in both client plus remote storage through considering the cloud features. Accordingly this review paper proffers sufficient characterization of prevailing techniques with its pros and cons. we present a novel security architectural paradigm that harnesses the benefits of IoT, fog, and cloud. Our middleware mediates between the subsystems and the cloud and aims to cope with the highlighted security issues discussed. It provides security requirements and discusses several access control decision and enforcements points necessary in the dynamic ecosystem of IoV. In the future, we would like to implement and analyze it on actual test-beds and real world scenarios to test its feasibility, practicality and performance.

REFERENCES

[1] N. Lu et al., “Connected Vehicles: Solutions and Challenges,” IEEE Internet Things J., vol. 1, no. 4, 2014, pp. 289–99.

[2] 2015. Building Autonomous and Connected Vehicle Systems with the Vortex IoT Data Sharing Platform. Prismtech (2015).

[3] 2016. Convergence Of Secure Vehicular Ad-Hoc Network And Cloud In Internet Of Things. http://mahbubulalam.com/convergence-of-secure-vehicular-ad-hocnetwork-and-cloud-in-iot/ [Online; Accessed: 2018-02-01].

[4] 2017. Connected Car. (2017).

[5] 2017. Securing The Connected Vehicle. Thales E-Security (2017). [

6] 2018. Cloud IoT Core.

[7] 2018. Device Twins. https://docs.microsoft.com/en-us/azure/iot-hub/iot-hubdevguide-device-twins [Online; Accessed: 2018-02-03].

[8] M. Aazam and et al. 2014. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In Proc. of IBCAST. 414–419.

[9] A. Al-Fuqaha and et al. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Comm. Surveys & Tutorials (2015), 2347–2376.

[10] Asma Alshehri and Ravi Sandhu. 2016. Access control models for cloud-enabled internet of things: A proposed architecture and research agenda. In Proc. of CIC. IEEE, 530–538.

[11] Asma Alshehri and Ravi Sandhu. 2017. Access Control Models for Virtual Object Communication in Cloud-Enabled IoT. In Proc. of IRI. IEEE, 16–25.

[12] B. Libert, T. Peters, and M. Yung, “Group signatures with almost-forfree revocation,” in Proc. of Advances in Cryptology -CRYPTO. LNCS, 2012, pp. 517–589.

[13] J. Zhou, Z. Cao, X. Dong, and X. Lin, “Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems,” in IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2398–2406.

[14] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc.of Advances in Cryptology - CRYPTO, August 2004, pp. 41–55.

[15] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in Proc.of Advances in Cryptology - ASIACRYPT, December 2001, pp. 514–532.

[16] Zhang, J. and Xu, Y. Privacy-preserving authentication protocols with efficient verification in VANETs. International Journal of Communication Systems 27 (12) (2014) 3676-3692.

[17] Wang, Y., Zhong, H., Xu, Y. and Cui, J. ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs. International Journal of Network Security 18 (2) (2016) 374-382.

[18] Zhou, J., Dong, X., Cao, Z. and Vasilakos, A.V. Secure and privacy preserving protocol for cloud-

based vehicular DTNs. IEEE Transactions on Information Forensics and Security 10 (6) (2016) 1299-1314.

[19] Rajput, U., Abbas, F. and Oh, H. A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET. IEEE Access 99 (2016) 1-1.

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

[21] Alam, K.M., Saini, M. and El Saddik, A. Toward social internet of vehicles: Concept, architecture, and applications. IEEE Access 3 (2015) 343-357.

[22] Campolo, C., Molinaro, A., Vinel, A. and Zhang, Y. Modeling and enhancing infotainment service access in vehicular networks with dual-radio devices. Vehicular Communications 6 (2016) 7-16.

[23] Cordeschi, N., Amendola, D., Shojafar, M. and Baccarelli, E. Distributed and adaptive resource management in cloud-assisted cognitive radio vehicular networks with hard reliability guarantees. Vehicular Communications 2 (1) (2015) 1-12.

[24] Lee, E., Lee, E.K., Gerla, M. and Oh, S.Y. Vehicular cloud networking: architecture and design principles. IEEE Communications Magazine 52 (2) (2014) 148-155.

[25] Mershad, K. and Artail, H. Finding a STAR in a Vehicular Cloud. IEEE Intelligent transportation systems magazine 5 (2) (2013) 55-68.

[26] Qadir, J., Ahmed, N. and Ahad, N. Building programmable wireless networks: an architectural survey. EURASIP Journal on Wireless Communications and Networking (2014).