Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

Secure Group Key Management Scheme for Dynamic Vehicular Cloud Computing

Nayana Hegde
Department of ECE, HKBK College of Engineering Bangalore-560045
Email: nayana.srikanth@gmail.com
Sunilkumar S. Manvi
School of Computing and Information Technology, Reva University,Bangalore-560064
ssmanvi@reva.edu.in

ABSTRACT

Vehicular cloud facilitates a dynamic set of vehicle users to form a cloud and share the resources and services to make safe journey. A public encryption key which is shared among the users, so that anyone participating in the cloud can send a message securely and efficiently to the vehicular cloud. Users can join or leave the group efficiently without triggering a completely new key agreement protocol, which will greatly benefit the users in the vehicular cloud. We define a generic construction of dynamic asymmetric group key agreement by combining a traditional authenticated group key agreement, public key encryption and signature. We evaluate the performance of the scheme, in comparison with existing scheme.

Keywords -**vehicular cloud, key management, encryption, security**

Date of Submission: June 18, 2021 Date of Acceptance: Aug 13, 2021

1 INTRODUCTION

Vehicular ad hoc networks (VANETs) is a category of Adhoc network, which facilitates vehicle to vehicle (V2V) and Vehicle to Infrastructure (V2I) communication to exchange data between moving vehicles [1]. In order to utilize differently VANET applications, the end-users should have the necessary software and hardware in their vehicles. In traditional VANETs, on-board units (OBUs) and roadside units (RSUs) can perform limited operations. As a result, it is not sufficient for various operations in the emerging world. In spite of several advantages of VANETS, we should look beyond their scope of operations. As a solution to limitations of VANETs, various resources can be utilized in the form of a cloud by other vehicles. This will reduce the need for installing more powerful computing devices for OBUs. The vehicular cloud computing (VCC) is a technology, which permits vehicles to procure unutilized resources of a vehicle like storage, internet connectivity and computing power by sharing or renting between vehicle users [2].

In VCC, the resources are dynamically assigned, reassigned or de-allocated as per the user requirement and resource availability. The most important advantage of the VCC is that vehicles need not buy the required computational resources and can share resources according to their usage. Some of the important examples of vehicular cloud are Ford -equipped with cloud features called Ford SYNC, Toyota- Microsoft Azure cloud platform and General Motors-OnStar track maintenance [3]. Some of the promising applications of the vehicular cloud are distributed data storage, urban traffic management, efficient alerts systems, safety applications, smart parking space management etc.

There are two modes in VCC, zero-infrastructure and infrastructure-based. The first mode comprises of the high mobility vehicle nodes, which leads to the short time of network communication and the loss of allocated resources. Infrastructure based system includes entities like base station and Internet for resources and data backup. This paper is mainly focused on the zero-infrastructure autonomous VCC. Due to the issues such as shared physical medium, lack of central management, highly dynamic topology, vehicular cloud networks are much more vulnerable to security attacks. Hence, it is necessary to find solutions for security. A group key agreement protocol allows a set of users, communicating over an open network. Due to the high mobility of vehicular nodes in the zero-infrastructure scenario, we design a secure group key management scheme, in which vehicles self-organize to groups to ensure the better communication stability.

1.1 Problem Statement

In this paper, we describe a generic construction of dynamic asymmetric group key agreement by combining a conventional group key agreement, a public key encryption and a multi-signature.

1.2 Contribution

The contributions of this work are specified as follows.

- In our proposed work, the broker is considered as main node for key management and is accountable for the formation, maintenance and dissolving of the cloud.RSU is involved only for selection or change of the broker and hence we have reduced communication overhead.
- ECDSA scheme is used for key pair generation at each vehicle OBU using the security parameters

Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

shared by the CA after successful registration.One way re-keying procedure is used to update when users joining or leaving the group.

- We conduct a comprehensive performance comparison between the proposed scheme and the existing schemes and show that the computation overhead of our scheme is significantly smaller than those of the existing schemes.

1.3 Organization

The remainder of this paper is organized as follows. In Section 2, we describe the related works of key management for VCC in details. A generic construction of distributed group key management scheme is described in Section 3. Performance comparison with previous works is given in Section 4. Section 5 concludes the paper.

2 RELATED WORK

In this section we summarize some of the related works in the field of key management in VANET and cloud computing.

Authors in [4] survey authentication schemes for VANET. They classified authentication schemes as: message verification methods, signature verification and cryptography based solutions. The work given in [5] presents a protocol that is efficient in conditional privacy preservation. Authors in [6] propose a dual authentication based security management scheme for VANET. Approaches in [7] [8] [9] [10] explains an implementation of SHA-1 and ECDSA for secure communication in VANET. The results show that the algorithm don't increase any delay in time for message transmission. Authors in [11] [12] have analyzed ECC based security schemes for cloud based applications. Authors have compared the results for secured and non-secured communication [13]. Approach in [14] introduced two schemes: one with name Aydos-Savas-Koc's wireless authentication protocol (ASK-WAP) and another with name user authentication protocol. The proposed scheme verifies various concerns in the area of wireless communication security. Work in [15] [16] presented a mechanism for information security. The designed mechanism meets requirements of security like: confidentiality, authentication, non-repudiation, conditional anonymity, and conditional intractability. Authors have used RSUs for distributing the key pairs in [17][18][30]. The scheme presented by authors, mainly banks upon the trusted platform module. Scheme uses both symmetric as well as asymmetric key cryptography.

Work in [19] [28] proposed light-weight protocols achieving maximal security. A dynamic key sharing protocol for public key infrastructure based VANETs is proposed in [20][21][26]. Approach given in [22] [23] [24][27][29], recommend key management scheme which is owned by group leader centrally. Work in [25] described a scheme comprising of techniques such as pseudo identity, bloom filter and binary search.

With reference to recent research work in key management area, for VCC and VANET, some of the research gaps are identified which are presented as follows. 1) Computational complexity will be more in cases of binary search and bloom filter algorithms employed for key distribution. 2) Overload on RSU for every message communication. 3) Rekeying complexity when user joins or leaves the group. Based on these observations, we propose an ECDSA based security scheme for VCC.

3 PROPOSED WORK

To address the security and privacy issues of vehicular cloud computing, this paper proposes a secure and efficient distributed group key management scheme for VCC. The suggested system protects user's identity, correctness of the data and confidentiality of the data. The proposed scheme consists of six processes. They are: 1) Off-line registration and VCC formation. 2) Key generation 3) Key distribution 3) User joining 5) User leaving 6) Broker leaving.

3.1 Off-line Registration and VCC formation

Registration process is necessary for each vehicle user to get certified as a legal user andgain access to the VCC network. **1)** The vehicle user first approaches the certificate authority (CA) office directly to make offline registration and provide the essential information like name, address, phone number; email id etc. to the CA. 2) After completing the registration process, the CA initializes the system parameters. 3) It provides the Vi to the registered vehicle, which is unique for every user and the CA also maintains the list of all the vehicles and their respective Vi in a secure database. 4) The CA provides the Vi to the user through a tamper proof device which also contains system parameters. 5) In this process both user and vehicle OBU are registered**.**

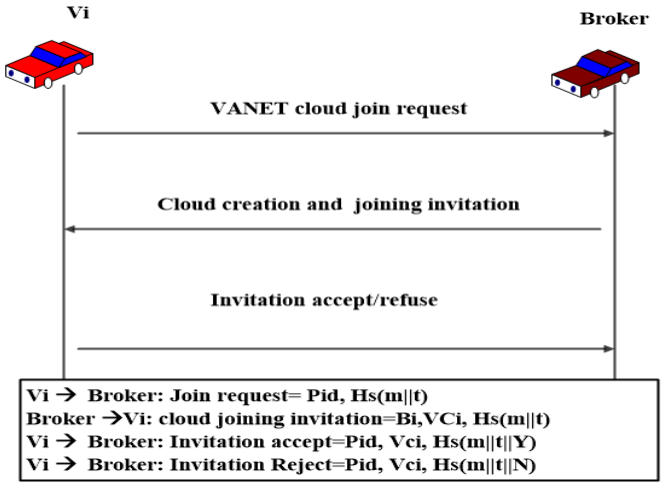

Fig 1. Vehicular cloud formation

Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

Vehicle cloud can be formed by pooling resources of static vehicles, moving vehicles or with the help of fixed infrastructure. We consider these pooled resources as virtualized resources and are managed by the broker. The broker is the main component in vehicular cloud. The broker manages three important tasks. First task is cloud formation, second task is resource management and the third task is request management. Pooling resources and handling the requests are managed by broker. Since the pooling of resources leads to formation of computer cluster, this is similar to infrastructure based cloud computing. VCC formation can also be done with help of existing static infrastructure. Examples are, vehicles in city traffic congestion, pooling or sharing their resources. The information is also exchanged with road side infrastructure and other vehicles. The vehicular cloud formation is illustrated in figure 1. Broker invites the vehicular users to participate in cloud. Interested users join and share their resources. The vehicles share their pseudo id to hide the original identity from other users.

Parameter Initialization

CA generates some initial system parameters. This process must only be performed once for the entire system. However, CA may periodically update the system master key to enhance the security performance. The detailed processes are as follows. CA selects a cyclic additive group G_1 and a cyclic multiplicative group G_2 that have bilinear map properties [2]. CA selects a random number $r \in Z$ and calculates its public key $CA_{pb}=r.P$. All system parameters (G_1, G_2, a, b, e, q, P, H, h, F_q, CA_{pb}) and public key of CA are securely provided in (tamper proof device) TPD to user. All the security details provided by CA are saved into the memory of OBU of the vehicle through TPD [1].

3.2. Key generation

This process takes place at the OBU of a registered vehicle or RSU. The security parameters (G_1, G_2, e, q, P, H, h, F_q) are provided by the CA for every registered vehicle and RSU. The public key is a randomly selected point V_{pb} in the group P generated by G_1. The corresponding private key is V_{pr}= logP. V_{pb}. The vehicle Vi generating the key pair must have the assurance that the domain parameters are valid. The association between domain parameters and a public key must be verifiable by all entities who may subsequently use Vi 's public key. The problem of computing a private key V_{pr} from a public key V_{pb} is the elliptic curve discrete logarithm problem. The numbers V_{pr} produced must be "random" in the sense that the likelihood of any particular value being chosen must be small enough to prevent an adversary from gaining an advantage by optimizing a search based on such probability. The validity of the public key is verified using the following steps: 1) Verify that $V_{pb} \neq \infty$.
2) Verify that V_{pb} is properly represented by the elements of F_q in the interval $[0,q-1]$ if F_q is a prime field and bit strings of length m bits if F_q is a binary field of order 2^m.
3) Verify that V_{pb} satisfies the elliptic curve equation defined by a and b. 4) Verify that $nV_{pb} = \infty$.

3.3 Key sharing

The public key is securely shared between VCC members with the help of RSU and the broker. The broker generates a session key (S_k), where $S_k \in Z$ and multi casts its value in encrypted form to all the users and RSU. Using this session key, all the users of VCC encrypt their public key and send it to the broker. Broker prepares the list of public key with the valid digital certificate and broadcasts it to all the members of the clod. Vehicle Vi, sends its public key V_{pb} with timestamp T_0 to broker. The broker receives the public key of all group members and checks the timestamp. The broker creates an acknowledgement with a timestamp Tsand encrypts using session key S_k , and sends to each group member of vehicular cloud. Broker creates a list of all public key and sends to all member of the group with a timestamp T_{s+1}. The users can share the data among cloud users. Messages are decrypted using the public key of the user. The validity of the key pair and certificates is authorized by RSU. If a member joins/leaves the group, list will be updated along with the session key. If the broker leaves the VCC, new broker is selected by RSU and process repeats.

3.4 Member joining VCC

Suppose that a set of vehicles, V_1,V_2,V_n have participated in formation of VCC and session key, Sk is shared by the broker among them as described. The detailed process of a new vehicle Va joining the group is described as follows. The vehicle Va selects a random number ri, generates key pair at OBU. Then the new vehicle sends request to RSU with its unique id Vi, Pseudo Id Pidand T_0. The Pseudo Id Pid is calculated using relation: XOR(Vi‖T0). The hash value of the message created is: Hs(m‖t), where m is the message for requesting joining VCC and t is the current timestamp. Once RSU verifies the details, send these details to the broker. The broker will share the session key with the new user and updates the list of public key again for all users. This is illustrated in figure 2.

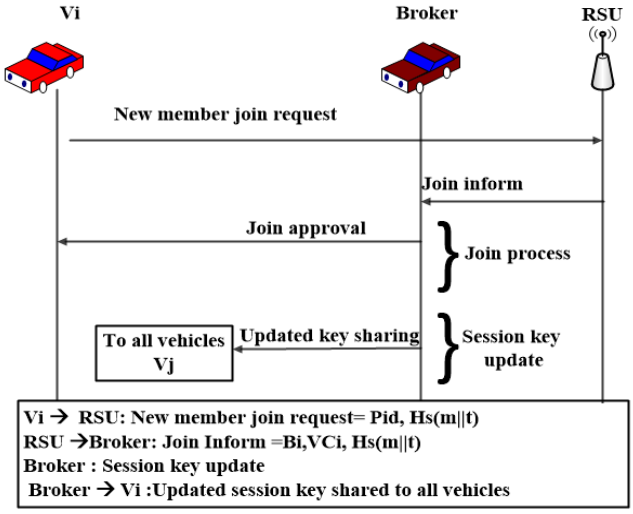

Fig. 2 New group member joining the VCC

Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

3.5 Member leaving VCC

Suppose that V_1,V_2,Vn have a session key as described above. Let Vn be a vehicle leaving the VCC. The broker should update the session key for the remaining n-1 vehicles. The detailed process of the group key updating is described as follows. The vehicle Vn send message to the broker for leaving the group. The broker deletes the old session key. Deletes the public key details from the list and calculates new list with n-1 users. The broker sends message to Vn vehicle to delete session key shared and list of public key of other users. Vn deletes the keys details and send acknowledgement to the broker. The broker calculates new session key, new list and broadcasts to the users. Also send a message to RSU. The process is illustrated in figure 3.

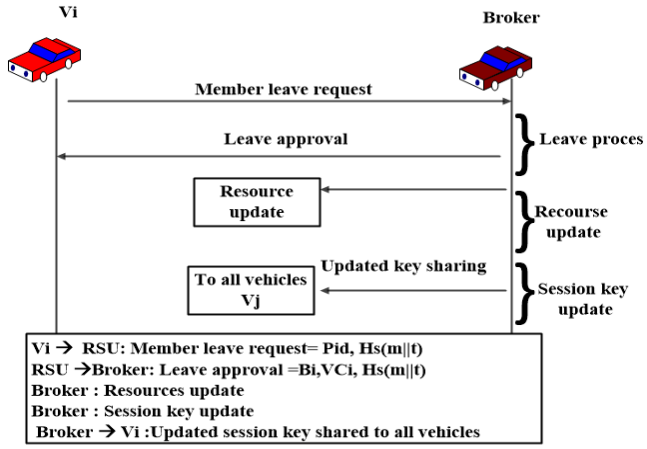

Fig. 3 Present group member leaving

3.6 Broker leaving the VCC

Broker is the main resource and request controller in the VCC. If the broker wants to leave the cloud group, then he should first send message to RSU. The RSU sends message to the broker to delete session key shared and list of public key of other users. The broker deletes the keys details and send acknowledgement to the RSU. The RSU will select new broker and the list of vehicles for the VCCi will be updated. The new broker will compute new session key for the remaining (n-1) vehicles.

4 RESULTS AND DISCUSSION

In this section we evaluate performance with respect to the results that are obtained from simulation. The proposed method has been implemented using JAVAprogramming language. For implementing key generation scheme suitable for VCC,the CA generated 1000 Vi values randomly. For the programs we have used BigInteger class for large integers.The proposed solution was tested on a Windows 10 computer with an Intel Core i5 processor, 2GB of RAM, and a 500GB hard drive.

We have compared our scheme results obtained from the simulation with that of existing schemes results. We are comparing the results of the proposed scheme with work proposed in DSKM [23] (Design of Secure Key Management), CGKM [27] (Centralized Group Key Management) and KAAC [24] (Key Aggregate Authentication Cryptosystem).

We discuss the efficiency of our scheme with related schemes in vehicular network. Performance parameters we considered are key generation time, computational cost and re-keying communication overhead. The graph in figure 4 shows the compassion of different schemes for the key generation time. It is observed from the graph proposed scheme has very less time requirement and KAAP scheme is having more time for key generation. The scheme has additional calculation for addressing the key leakage problem and is more secure for cloud environment. The scheme in CGKM is mainly dependent on the group leader for the key generation. Group leader takes care of the group key and is the attributes of each user is required for the generation of the key so CGKM requiresindividual key pair which is more secure and time efficient due to ECC technology.

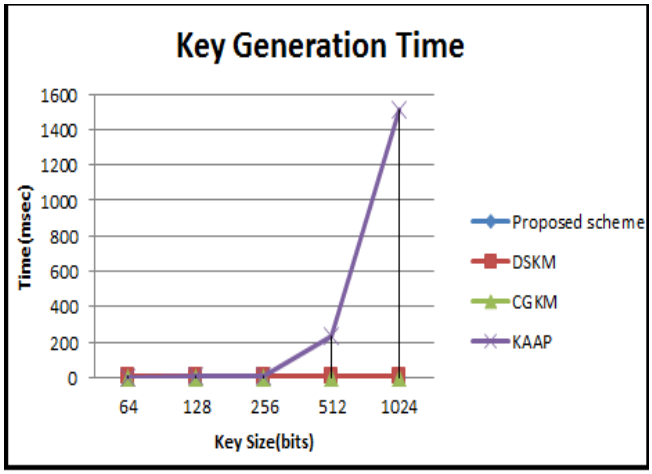

Fig. 4 Comparison of key generation time

DSKM scheme uses XOR operation and hash function and thus is secure as well as light on computation of keys. Computational cost of each work is compared in figure 5. The graph shows the comparison of the total computational cost of the schemes for security and VANET and cloud computing systems. We can observe from the graph that the computational cost of scheme DSKM is more compared to other schemes. This is due to complex authentication procedure involved in smart devices and fog computing and the additional privacy preserving mechanism involved. CGKM scheme linearly increases the computational cost with increase in the number of nodes or vehicles. This is because centralized computational managed by the single group leader.KAAP scheme has a feature of extracting the key details from the ciphertext which is more costly in computation compared to the proposed scheme. The re-keying process in VCC imposes a communication overhead on the key management scheme. We have considered a cloud formed with 10 users and have calculated the number messages received by the user in cloud when a new vehicle user joins or existing user leaves the cloud.

Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

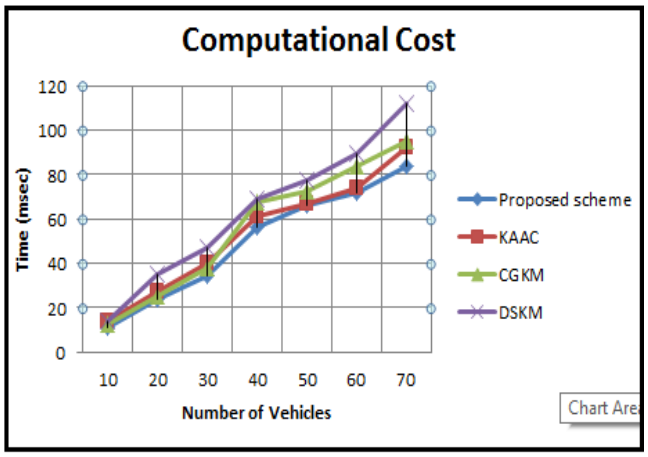

Fig. 5 Comparison of Computational cost

The simulation results are compared and the same is illustrated in figure 6. Proposed scheme got least number of messages and communication cost is less compared to other scheme. The proposed scheme achieves minimized message communication because of the broker responsible for the group management. Thus overload on the RSU is reduced.

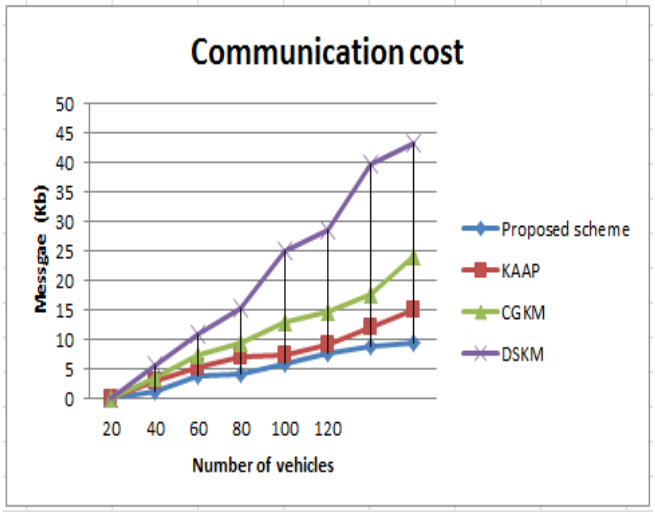

Fig. 6 Comparison of communication cost

5. CONCLUSION

In this paper we presented secure group key management scheme for dynamic vehicular cloud computing. Furthermore we focused on how keys are generated, distributed in VCC model. Extensive simulations are presented to evaluate the performance of the proposed techniques. Our proposed scheme is more efficient performance than the decentralized, distributed key management schemes. Proposed scheme supports dynamic nature of VCC. The security mechanism does not affect communication time. Thus response time for VCC is improved. The future work aims to extend the focus measure the parameters like time during which vehicles will be connected to VCC, maximum storage per customer, maximum storage time available, cost per storage unit and maximum available storage capacity for VCC environment.

REFERENCES

[1] Nayana Hegde, SS Manvi, A novel key management protocol for vehicular cloud security, Telkomnika, 2019, 17, (2), pp. 857-865

[2] Nayana Hegde, SS Manvi, Hash Based Integrity Verification for Vehicular Cloud Environment, IEEE CCEM conference proceedings, 2019, pp. 1-5

[3] Whaiduzzaman, Sookhak, M., Gani, M., RajkumarA survey on vehicular cloud computing, Journal of Network and Computer Application, 2014, 40, (1),pp. 325–344

[4] Manvi, S.S., Tangade, S.: A survey on authentication schemes in vanets for secured communication, Vehicular Communications, 2017, 9, (3), pp. 19–30

[5] Lu, R., Lin, X., Zhu, H., Ho, P.H., Xuemin: Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications, IEEE Conference on CCP Phoenix USA, 2008, pp. 1903–1911

[6] Vijayakumar, P., Azees, M., kannan, A., Deborah, L.J.: Dual authentication and key management techniques for secure data transmission in vehicular adhoc networks, IEEE Transactions on Intelligent Transportation Systems, 2015, 17, (4), pp. 1015 – 1028

[7] Wu, H.T., Horng, G.J., Vehicular cloud network and information security mechanisms, International Conference on Network and Communication Technologies Taiwan, 2016, pp. 196–199

[8] Nacy, S., Oh, T., Leone, J. Implementation of sha-1 and ecdsa for vehicular ad-hoc network using ns-3, Conference on Research in Information Technology Orlando Florida USA, 2013, pp. 83–88

[9] Waziri, V., Adebayo, O., Danladi, H., Isah, A., Magaji, A., Abdullahi, M.B. Network security in cloud computing with elliptic curve cryptography, Network and Communication Technologies, 2013, 2, (2), pp. 43–58

[10] Manvi, S.S., S, K.M., G., A.D. Message authentication in vehicular ad hoc networks: Ecdsa based approach, International Conference on Future Computer and Communication, KualaLumpar, Malaysia, 2009, pp. 16–20

[11] Wang, R.C., Juang, W.S., Lei, C.L.: Provably secure and efficient identification and key agreement protocol with user anonymity, Journal of Computer and System Sciences, 2011, 77, (4), pp. 790â˘A ¸S798

[12] Tripathi, A., Yadav, P.: Enhancing security of cloud computing using elliptic curve cryptography, International Journal of Computer Applications, 2012, 57, (1), pp. 26–30

[13] Durech, J., Frankova, M., Holecko, P., Bubenikova, E.: Modelling of security principles within car-to-car communications in modern cooperative intelligent transportation systems, Information and safety-related systems, 2016, 14, (1), pp. 40–57

[14] Glas, B., Sander, O., Stuckert, V., Muller.Glaser, K.D., Becker, J.: Prime field ecdsa signature processing for reconfigurable embedded systems, International Journal of Reconfigurable Computing, 2011, 2011, (5), pp. 1–12

Volume: 13 Issue: 01 Pages: 4821-4826(2021) ISSN: 0975-0290

[15] Tripathy, L., Paul, N.R.: An efficient and secure key management scheme for hierarchical access control based on ecc, International Journal Communication and Network Security, 2011, 1, (2), pp. 50–55
[16] Hao, Y., Cheng, Y., Ren, K., Song, W.: Distributed key management with protection against rsu compromise in group signature based vanets, IEEE Journal on Selected Areas of Communication, 2011, 29, (3), pp. 616–629
[17] Damgard, I., Jakobsen, T.P., Nielsen, J.B., Pagter, J.I.: Secure key management in the cloud, International Conference on Cryptography and Coding Oxford UK, 2013, pp. 135–145
[18] Tripathy, L., Paul, N.R., Salem, A.H., Abdel.Hamid, A., El.Nasr, M.A.: The case for dynamic key distribution for pki-based vanets, International Journal of Computer Networks and Communications, 2014, 6, (1), pp. 61–78
[19] Woodbury, A.D., Bailey, D.V., Paar, C.: Elliptic curve cryptography on smart cards without coprocessors, Conference on Smart Card Research and Advanced Applications Bristol UK, 2000, pp. 71–92
[20] BERTA, I.Z., Mann, Z.A.: Implementing elliptic curve cryptography on pc and smart card, Periodicpolytechnic System Science and Engineering, 2002, 46, (2), pp. 47–73
[21] Kerrache, C.A., Lakas, A., Lagraa, N.: 'Uav-assisted technique for the detection of malicious and selfish nodes in vanets', Vehicular Communications, 2018, 11, (3), pp. 1–11
[22] Lin, J.C., Lai, F., Lee, H.C.: 'Efficient group key management protocol with one-way key derivation', The IEEE Conference on Local Computer Networks, Sydney,Australia, 2005, pp. 336–343
[23] Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V.: 'Design of secure key management and user authentication scheme for fog computing services', Future Generation Computer Systems, 2019, 91, (1), pp. 475–492
[24] Guo, C., Luo, N., Bhuiyan, M.Z.A., jie, Y.: 'Key aggregate authentication cryptosystem for data sharing in dynamic cloud storage', Future Generation Computer Systems, 2018, 84, (1), pp. 190–199
[25] W., C.T., M., Y.S., C., H.L., Victor, L., Jiang, Z.L.: 'Specs: Secure and privacy enhancing communications schemes for vanets', International Conference on Ad Hoc Networks, Niagara Falls, Canada, 2009, pp. 160–175
[26] Das, A., Roy choudhury, D., Bhattacharya, D., Srinivasan, R., Shorey, R., Thomas, T.: 'Authentication schemes for vanets: a survey', International Journal of Vehicle Information and Communication Systems, 2013, 3, (1), pp. 48 – 55
[27] Guo, M.H., Liaw, H.T., andHanChieh.Chao, D.J.D.: 'Centralized group key management mechanism for vanet', Security Commmunication Networks, 2013, 6, (1), pp. 1035–1043
[28] Pshwang Wang, Zecheng Wang , "Research on Privacy Protection Strategies of Mobile Social Network Users ", Int. J. Advanced Networking and Applications, Volume: 12 Issue: 01 Pages: 4528-4531(2020)
[29] Ramesh Kumar, "A Reliable Authentication Protocol for Peer to Peer Based Applications", Int. J. Advanced Networking and Applications, Volume: 12 Issue: 05 Pages: 4714-4718(2021)
[30] Aye PwintPhyu , EiEi Thu, "Short Survey of Data Mining and Web Mining using Cloud Computing" , Int. J. Advanced Networking and Applications, Volume: 12 Issue: 05 Pages: 4725-4731(2021)

AUTHOR'S BIOGRAPHY

Nayana Hegde

Mrs. Nayana Hegde did her Bachelors in Electronics and Communication from Karnataka University, India in year 2001 and Masters in Digital Communication and Networking from VTU, India in 2014. She is pursuing her PhD in Electronics and Communication and Engineering from Reva University Bangalore, India.

Dr. SunilkumarS.Manvi

Dr.SunilkumarManvi received M.E., and Ph.D., from the University of Visweshwariah College of Engineering (UVCE),and Indian Institute of Science (IISc.), Bengaluru, India, respectively. He is currently working as a Professor and Director of School of Computing and IT, REVA University, Bengaluru, India. He has experience of around 29 years in teaching and research.He received **Prof. SatishDhawan Young Engineers State Award** for the year 2015 from KSCST. The award is due to outstanding contribution in research on Engineering Sciences.