Intelligent Transport System Using Cloud Computing & PSY Key Generationfor V2V Communication

Pradeep Kumar, Salma Itagi, C Nagarathna, S S Ashwini and N N Srinidhi

February 26, 2023

Intelligent Transport System using Cloud Computing & PSY Key Generationfor V2V Communication

[1]Pradeep Kumar K., [1]Salma Itagi, [2]Nagarathna C., [2]Ashwini S S.,
[3]Srinidhi N N.,
[1]IEEE member - 98464920
[1,2]Assistant Professor, CSE Dept, Sai Vidya Institute of Technology, Bangalore, KA, Ind.
3Assistant Professor, Department of Computer science and engineering,
Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education,
Manipal, India.

Abstract

Internet of Things (IoT) connects many sensors to internet so that it will provides services and applications for smart cities. Vehicles connected to internet can communicate, sense, analyse and also make decision on their own. Vehicular Cloud (VC) is new idea proposedto enhance the vehicular services through mobile cloud computing and networking. This proposed paper highlights an Intelligent Transportation System (ITS) which provides creative applications and service related to traffic management and also to access the information for various users. A model is developed taking picture of vehicles in detail, time of availability of vehicle in a given region. A new paradigm to collect the data for tracking the intelligent system. The simulation results are shown regarding involvement of vehicles in low percentage in dynamic VCN which provides data for intelligent system.

Keywords: Vehicular cloud, Intelligent Transportation System (ITS), Dynamic Vehicular, Mobile Cloud Computing.

I. INTRODUCTION

The fast growth of wireless communication technologies [1],[2], and vehicles provides a solution to all issues related to traffic, vehicles to vehicles communication can be achieved by vehicular networks. Vehicular Adhoc Networks features will enable ITS. These Intelligent system confinement new application and services which will help drivers by combining sensors, mobile devices, vehiclesinto global network.

Vehicular Cloud Computing (VCC) [3],[6] technology where user can access the services at any point of time and space. To serve an online travel system with vehicular cloud, data collection is most important which is achieved by data pull-based model is used. Vehicles are considered as nodes to cloud and vehicular cloud is developed independently by traffic on the road, this cloud will work independently. Vehicles will detect of the traffic congestion and access the flow of traffic in city using ITS. The aim of vehicular cloud is to provide a solution for traffic incidents which is unpredictable, where according to dynamic behaviour can be adapted with vehicular cloud.

Figure 1: An overview of V2V Communication (courtesy:https://www.extremetech.com/extreme/176093-v2v-what-are-vehicle-to-vehicle-communications-and-how-does-it-work)

As number of vehicles increases pseudonym management has become one of major challenge in vehicular clouds, which enables disadvantage of centralized pseudonyms including two aspects:

1. A backhaul delay and heavy workload on central cloud which results in low utilization of pseudonyms.
2. Network control is done by Software-Defined Pseudonym System (SDPS) in a systematic approach.

II. RELATED WORK

Existing work from various authors has suggest for V2V communication: 3-layer Vehicular Fog Computing system based on one M2M to manage resources which are distributed for efficient usage, manage information flows and task on vehicle fog nodes and will send feedback result to users and to connect and monitor heterogeneous data. One M2M has tree-based architecture with five nodes infrastructure node, middle nodes, application nodes dedicated nodes and device node [4].

To protect sensed data by using alpha-geometric techniques- Preserving privacy and sensory data with a framework consists three entities and three layers. A sliding window technique is adopted to recover the sensory data, identity-based signature scheme is adopted for authentication and to preserve the sensory data cryptosystem technique was adapted [5].Vehicular resources in an existing Vehicular Adhoc Network are underutilized, based on public key cryptosystem which allows vehicles to form a Vehicular cloud securely. Architecture consisting trusted authority entity to generate a master key and parameters, to manage vehicular cloud a centre cloud manager entity was used to send and receive the messages.

To connect the vehicles and cloud many communication technologies are used. For instance, in [8], the authors have developed a three-tier cloud architecture which is a hybrid cloud consists of central cloud, vehicular network and roadside cloud. To allocate a resource a game theoretical model is used. Artificial transportation structures are installed to version and describe the real transportation system. Second, destiny evolutions and control plans are designed by computational experiments. Lastly, the real and syntheticstructures are executed in an interactive parallel mode. The authors in [9] focused on artificial intelligent transportation system, to control plans and evolutions computation experiments were conducted. To collect the data three-layer model were developed: terminal layer to detect the radio and video sensors, the sink layer to collect the traffic information and gateway layer to process these data's.

Vehicular cloud possible applications and implementation cases have been proposed recently. In [10], the authors proposed a framework which connects graph job and service providers through vehicle-to-vehicle communication. This model was developed to address the issues of low traffic and rush hours. They advocate a unique randomized graph task allocation mechanism which is low complexity, hierarchical tree and subgraph isomorphism extraction. The assessment of the overall performance of each the choicest and the proposed randomized set of rules with greedy-primarily based totally baseline strategies is carried out via vast simulations.

To achieve the security and efficient communication the author in [12], had proposed a framework for VCC which was based on Elliptic Curve Cryptography (ECC) and connected to Radio Frequency Identification (RFID) for secure communication using oracle model.Replay attack and man-in-middle attack was solved using simulation tool “AVISPA” and evaluated the performance and compared the results with related schemes.

III. THE PROPOSED MODEL

Apseudonym management approaches in detail is proposed here. The fundamental goal of the model is to offer higher connectivity and consequently higher offerings for driving force convenience. Author hascomply with the pull-primarily based model where in a fascinated vehicle which can send a question on call to a far-off region in the city, and acquire a respond via Internet of Vehicles (IoV) inside affordable delay. Collaboration of vehicles in IoV will cooperate in presenting a significant reaction via way of means of sensing and processing facts with the useful resource of low complexity VC. The model uses SaaS for travel convenience services and IaaS fornetwork services from cloud computing [14].

Sequence Diagram-1

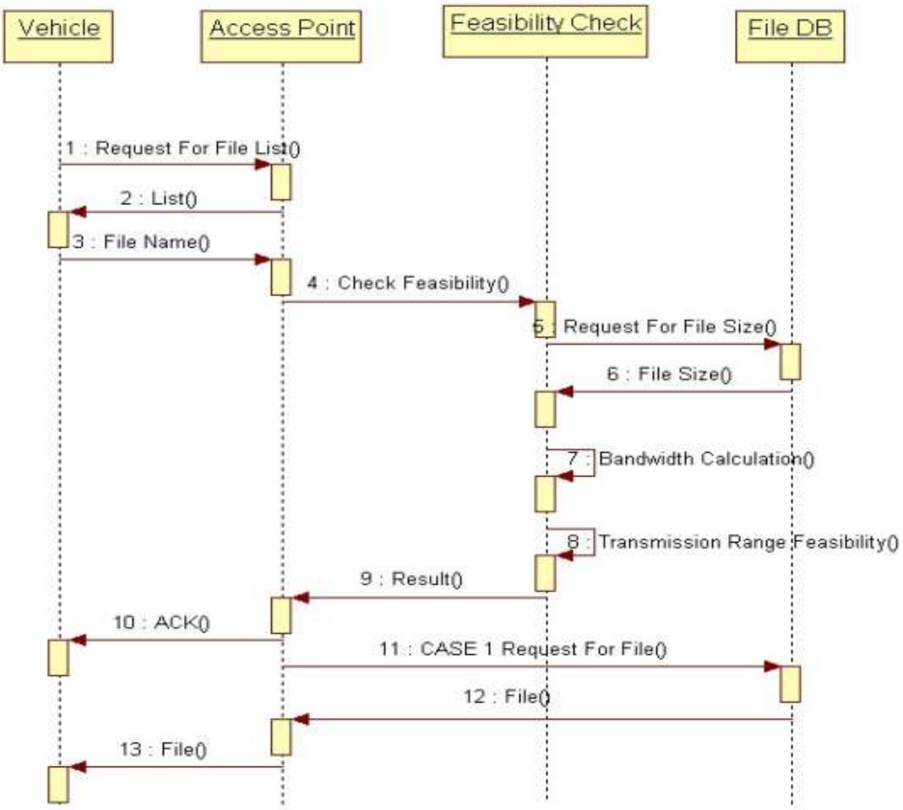

Figure2: Feasibility Check sequence diagram

Step 1: The Authentication Key (AuK) is assigned by cloud to RSU. All the vehicles must register RSU which is reachable, the RSU transmits vehicles vehicle information for key generation to cloud.

Step 2: RSU receives the request which encrypted with digital signature. Verification of request is done by RSU and RSU adds its signature and forwards to central manager.

Step 3: The central manager checks the pseudonym request and bandwidth ratio of the vehicles and acknowledge it and pseudonyms is encrypted and transmited them to RSU.

When a vehicle comes in scope of RSU, authentication is not required as the vehicles has been in communicated. The RSU retransmits the verification messages to other RSU. The RSU which receives the request verifies the authentication in table and sends the results to RSU. AuK key will send to vehicles which are authenticated on same RSU. RSU which are nearby by to vehicles can obtain AuK as there are authenticated by different RSU

Sequence Diagram-2

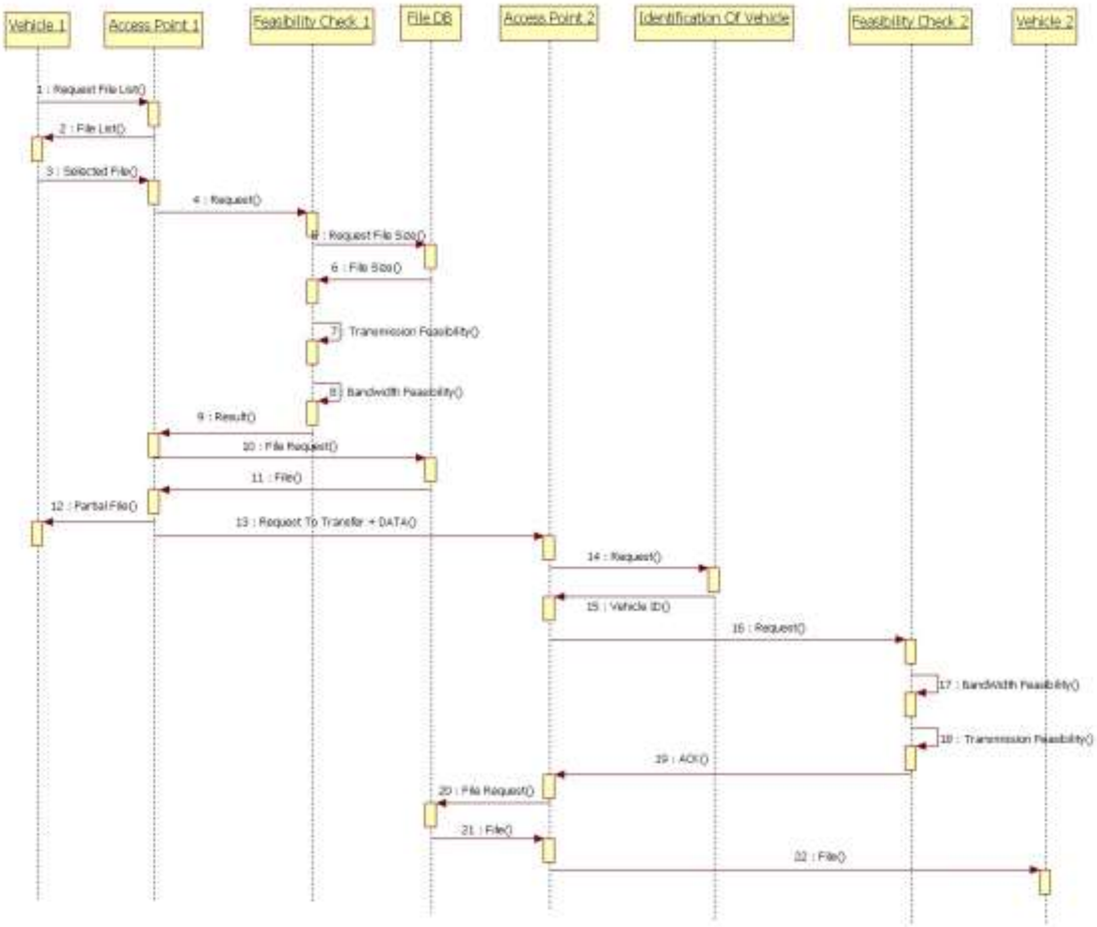

Figure3: Identification of Vehicle Sequence diagram

Sequence Diagram-Case 2B

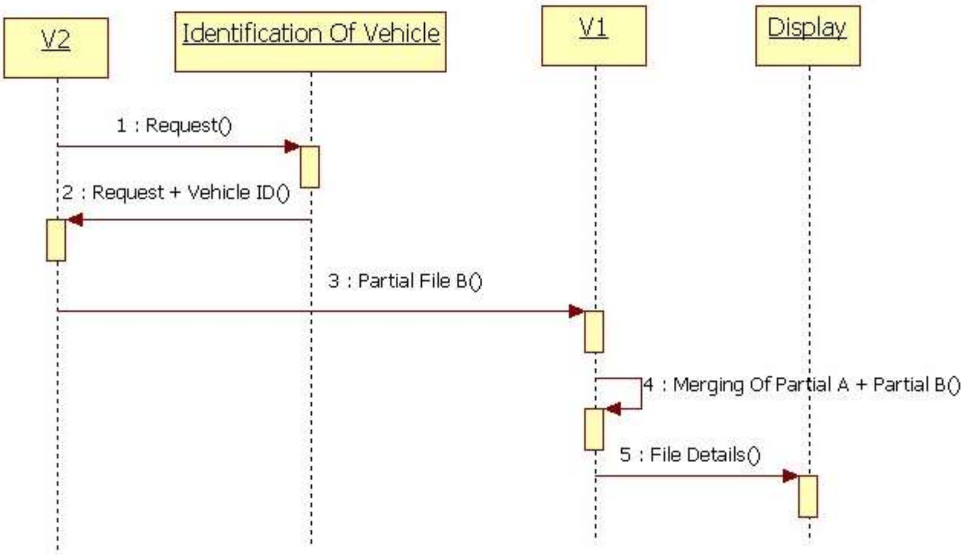
V2
Identification Of Vehicle
V1
Display
1 : Request()
2 : Request + Vehicle ID()
3 : Partial File B()
4 : Merging Of Partial A + Partial B()
5 : File Details()

Figure 4: Sharing the PKey&Authenication

Step1: Vehicle identifies another vehicle.
Step2: Identified vehicle 2 will requests the pseudonym key.
Step3 &4: vehicle 1 & vehicle2 will share the key and merges the same with the cloud.
Step 5: details of the file which the vehicle 1 is accessing will be shared and it will be ready for transmission.

ARCHITECTURE OF SDPN

SDN is used to separate control and data plane so that data forwarding can be abstracted from applications and data is logically centralized. OpenFlow protocol is used for resource scheduling and to control the network in centralized, programmable and systematic manner.

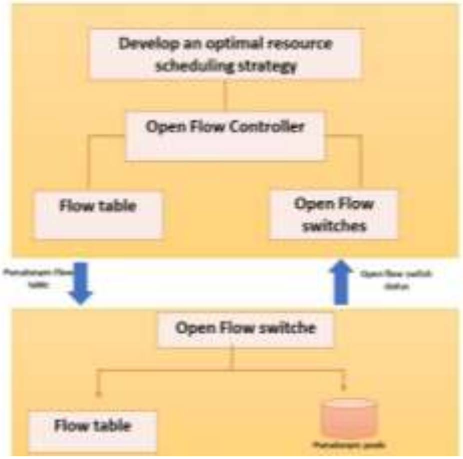

Figure5: Architecture of Software Defined pseudo-Network

Figure describes the architecture of Software Defined Pseudo Network (SDPN) in vehicular clouds. The vehicular clouds proposed has three-layer clouds: local, central and vehicular clouds. The registration in the central cloud consists of registration authority, data centre, and an OpenFlow controller. The authority is in charge of registration controls all entities' digital certificates, such as automobiles, Pseudonym pools, Road Side Units (RSU).

A local cloud is formed by RSUs which are adjacent and a faraway data centre, pseudonym pool with an OpenFlow switch. Vehicles with insufficient pseudonyms submit their location to be kept private. Table of pseudonym-flow Information shows the status of OpenFlow switches and create a resource scheduling plan. Local pseudonym pools generate pseudonyms in the SDPS and moved to other pseudonym pools in various local clouds as needed.When some pseudonyms are provided to a vehicle, the local clouds' signatures will be linked to the pseudonyms to signify the management.

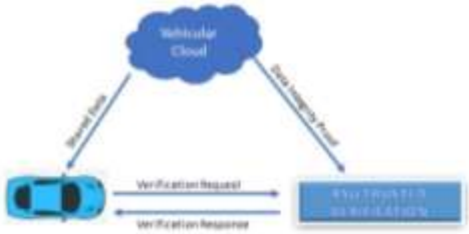

Figure6: Formation of Network using cloud, RSU & OBU

OpenFlow controller identifies the pseudonym resource allocation among pseudonym pools. Control plane obtains global information,requests from vehicles and pseudonym pools. Resource allocation strategy is done by control panel.

Table1: Operation used in the model & consumed energy for V2V Communication

Operation		**Consumed Energy**
Hashing operations	**SHA-1**	**076 µJ/byte**
	HMAC	**1.16 µJ/byte**
	MD5	**0.302 µJ/byte**
Symmetric-key encryption and decryption operation	**AES**	**1.21 µJ/byte**
	IDEA	**1.47 µJ/byte**
	DES	**2.08 mJ/byte**
Pairing operation		**25.5 mJ/byte**
Transmitting/receiving one bit		**0.72/0.81 µJ**

The pseudonym pools in cloud are indicated by V={P1,P2, … Pm}and represented by undirected graph G(V,E) where 'E' represents the transmission links which are undirected set of edges.Weights of edges is determined by c=l*d, where c represents transmission loss(c) per unit(l) which are connected between pseudonym pools, d is distance between pools.

SOLUTUIONS FOR PSEUDONYM KEY (PKey)GENERATION:

PKey is implemented in distributed manner to use fictitious identities and certificates. In the proposed framework usage of MD5 message digest hashing technique.

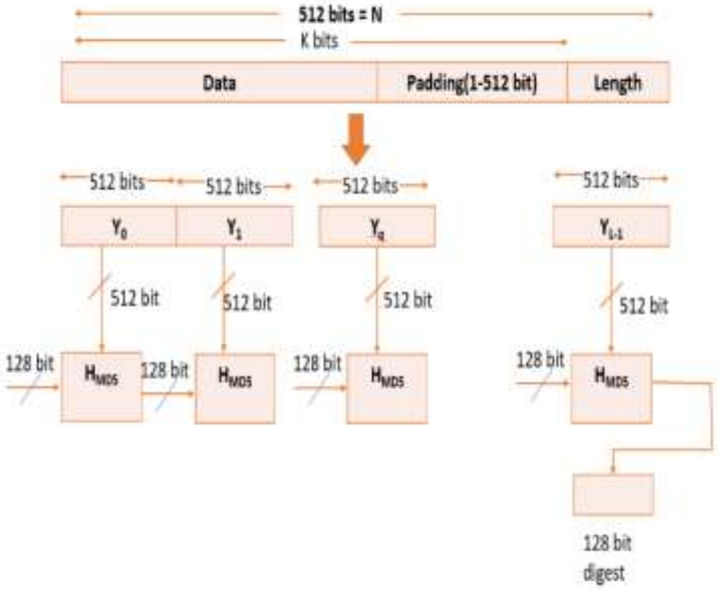

Figure7: MD5 algorithm

A hash algorithm MD5 (Message Digest Method 5) is used which will generate a 128-bit digest from a string of any length. The digest is of 32-bit hexadecimal number.

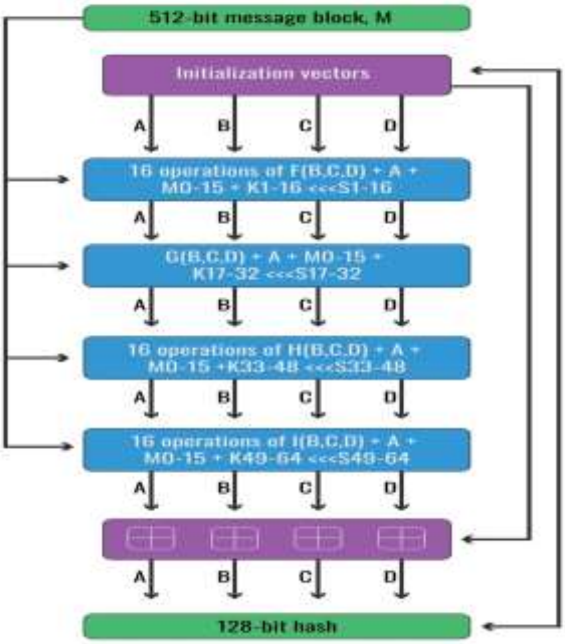
512-bit message block, M
Initialization vectors
A
B
C
D
16 operations of F(B,C,D) + A + M0-15 + K1-16 <<<S1-16
G(B,C,D) + A + M0-15 + K17-32 <<<S17-32
16 operations of H(B,C,D) + A + M0-15 +K33-48 <<<S33-48
16 operations of I(B,C,D) + A + M0-15 + K49-64 <<<S49-64
128-bit hash

Figure8: 512-bit to 128-bit hash key (HKey)

Algorithm: Pseudonym Key Generation

- *Input: Data file, public key*
- *Output: Hash value of 128-bit, signature*
- *Split the data into blocks of size 512 bits.*
- *Initialize the constant array value T[1]->T[64]*
- *The length of message, expressed in binary as a 64-bit number, is appended to the data.*
- *Between the end of the message and length field, a padding is inserted:*

- *Data+pad+64 = multiple of 512, the block size.*
- *Each block is split into 16 words, each 32 bits.*

- *Initialize the MD Buffer (Buffer 32 bit, buffers[A,B,C,D])*

Denote each sub-block as M[0]->M[15]

- *Process each block (512 bit)*
  - *R1 (B, C, D): (B^C) v (¬B⋀D)*
  - *R2 (B, C, D): (B ^ D) v (C ^ (¬D))*
  - *R3 (B, C, D): (B ⊕ C ⊕D)*
  - *R4 (B, C, D): (C ⊕ (B v (¬D)*
- *Process each round in 16 steps*
  - R_i<- $B +_m((A +_m R_i(B,C,D) +_m$ *Data File* $+_m T[i]]<<< S)$
- *Digital signature of data with private key*
  - *Sig(M) = (k,r) generated*
  - *If sig(m) valid then*
    - ✓ *CA public key encrypts the response*
    - ✓ *VCC contains data file sig(m) signed by owner*
    - ✓ *Transaction details D is sent by VCC to RSU*
  - *Else*
    - *Response is sent as failure to RSU*

The bits of shift registersare mangled together with each of the words of the array in turn.The vehicles which request through the secret key from vehicular cloud for pseudonym. The pseudonym gets initial key from pseudonym pools through vehicular cloud.The authentication of vehicle is done by certificate Authority through Pk_{ca} (public key of CA). The vehicle is verified by vehicular cloud through Pk_{ca}. After successful verification pseudonym certificate from certificate authority. The request is verified and communicate to the vehicle.

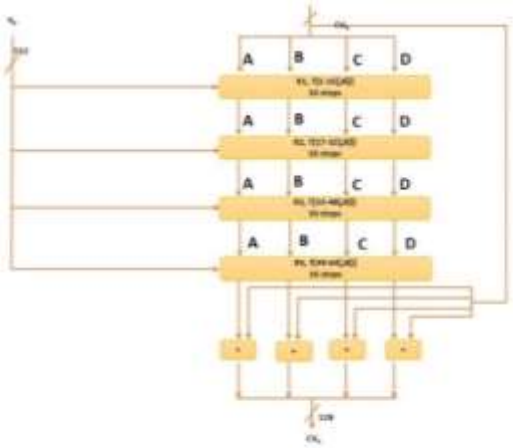

Figure9: MD5 processing 512-bit data

MD5 processing

The figure depicts the compression function that consists of four rounds. each block takes input of 512 bits block as input and 128 bit buffer value ABCD. the ith element of T[i] is 32 bits used to eliminate any regularities in input data. The output of fourth round is added to the input first round (CVq).

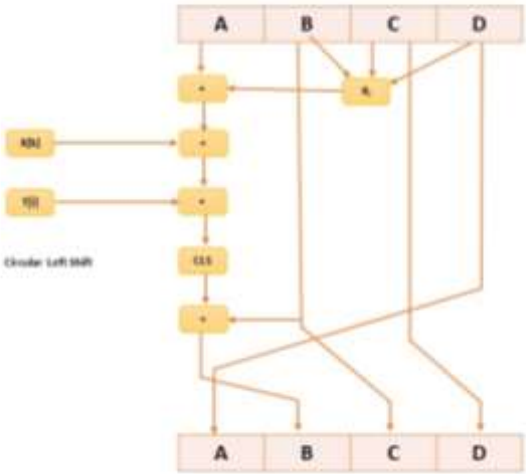

Figure10: MD5 Compression function-Single step

MD5 compression function- single step

The figure depicts compression function, each round consists of a sequence of 16 operating on buffer ABCD. each step is of form:

R_i<- $B +_m((A +_m R_i(B,C,D) +_m \textit{Data File} +_m T[i]]<<< S)$

R_i is primitive function for four rounds. X[k] is kth 32-bit word in current data file. T[i] is ith entry in the matrix of constants T.

CONCLUSION AND FUTURE WORK

Authors have used software defined pseudonym system which will manage pseudonyms among the pseudonym pools which are distributed.Hash-based integrity verification scheme is used for vehicular cloud computing which provides identity preserving and remote integrity verification. In future work, we are interested in mitigation of performance degradation caused by noise and further improve in the system utility and query accuracy.The future work will consider with the communication & calculation of vehicle speed & sharing the information from cloud to OBU via RSU.

References

[1] S. Bitam, A. Mellouk, and S. Zeadally. “Vanet-cloud: a generic cloud computingmodel for vehicular ad hoc networks”. *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96–102, February 2015.

[2] Srinidhi, N. N., G. P. Sunitha, E. Nagarjun, J. Shreyas, and SM Dilip Kumar, "Lifetime maximization of IoT network by optimizing routing energy." In *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE),* pp. 1-4. IEEE, 2019.

[3] Azzedine Boukerche, Robson E. De Grande, “Vehicular cloud computing: Architectures, applications, and mobility”. *Computer Networks,* vol. *35,* pp. 171-189, 2018.

[4] WISEBORN M. DANQUAH, D D. TURGAY ALTILAR, “Vehicular Cloud Resource Management, Issues and Challenges: A Survey”, *IEEE Access*, vol. 8, 2020.

[5] KIEU-HA PHUNG, HIEU TRAN, “oneVFC—A Vehicular Fog Computation Platform for Artificial Intelligence in Internet of Vehicles”. *IEEE Access*, Special Section on Collaborative Intelligence for Internet of Vehicles, vol. 9, August 2021.

[6] Qinglei Kong, Rongxing Lu, “Privacy-Preserving Continuous Data Collection for Predictive Maintenance in Vehicular Fog-Cloud”, *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[7] M. Chaqfeh, N. Mohamed, I. Jawhar and Jie Wu, "Vehicular Cloud data collection for Intelligent Transportation Systems," *2016 3rd Smart Cloud Networks & Systems (SCNS)*, pp.1-6, 2016

[8] L. Zhang, X. Meng, K. R. Choo, Y. Zhang and F. Dai, "Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud," in *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 634-647, 2020.

[9] P. Mohanty, L. Kumar, M. Malakar, S. K. Vishwakarma and M. Reza, "Dynamic resource allocation in Vehicular cloud computing systems using game theoretic based algorithm," *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 476-481, 2018.

[10] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong and F. -Y. Wang, "Parallel Transportation Systems: Toward IoT-Enabled Smart Urban Traffic Control and Management," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 10, pp. 4063-4071, Oct. 2020,

[11] M. LiWang, S. Hosseinalipour, Z. Gao, Y. Tang, L. Huang and H. Dai, "Allocation of Computation-Intensive Graph Jobs Over Vehicular Clouds in IoV," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 311-324, 2020.

[12] Hussain, R., Kim, D., Son, J., Lee, J., Kerrache, C.A., Benslimane, A. and Oh, H, "Secure and Privacy-Aware Incentives-Based Witness Service in Social Internet of Vehicles Clouds," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2441-2448, Aug. 2018.

[13]Vinod Kumar, Musheer Ahmad, Dheerendra Mishra, Saru Kumari, Muhammad Khurram Khan, “RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing, Vehicular Communications”, vol. 22, pp. 100213, 2020.

[14] Lee, Euisin, Eun-Kyu Lee, Mario Gerla, and Seong Y. Oh, "Vehicular cloud networking: architecture and design principles." *Communications Magazine, IEEE*, vol. 52, no. 2, pp. 148-155, 2014.

[15] Talal H. Noor, Sherali Zeadally, Abdullah Alfazi, Quan Z. Sheng, “Mobile cloud computing: challenges and future research directions”, *Journal of Network and Computer Applications*, vol. 115, pp. 70-85, 2018.