A Secured Data sharing among Vehicles to Keep Track of Road Conditions

Rahul Chatterje[1], Ramya R[2], Venkatesh M[3], Vinod kumar[4], Mrs. Visalini S[5]

Final year B.E Students(UG) , Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore, India[1,2,3,4]

Assistant Professor, Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore, India[5]

ABSTRACT*:* The main objective is to improve the travel efficiency and safety of transportation system and it represents the design of a road side authority, such that it needs to monitor real-time road conditions with the help of a cloud server so that it could make sound responses to emergency cases timely. Vehicles on site are able to report the information to a cloud server engaged by the authority when they detect some bad road conditions, for example some geologic hazard or accidents. The main goal is to provide authorized reporting of the vehicles. A vehicle can collect the real time road condition information and encrypt it with the root authority's public key, its secret key and the token issued by the administrative RU and the cloud server is engaged to perform much of the monitoring work. The entities in RCoM system such as sub-authorities, vehicles and roadside units are recognized with their identities.

KEYWORDS: Data privacy, vehicular ad hoc network, cloud computing, authentication.

I. INTRODUCTION

In real world application scenario, the road side authority may need to monitor real time road conditions so that it could respond quickly in emergency cases. Each vehicle with an embedded on- board unit is able to collect and communicate the current road/traffic information with the help of distributed road side unit. When T(toe) or more road condition reports for the same location are received, where T denotes the threshold in the monitoring system, the root authority considers it as an emergency case and then makes response. Mainly, the vehicles have to be authorized by some roadside unit. To guarantee the privacy against the cloud server, the road condition information should be reported in cipher text format. The cloud server and authority should be able to validate the report source. So in this way, every nearby recipient vehicle would be able to get better awareness of driving environment and change driving plan if needed. However this approach requires root authority to equip with powerful computing and storage resources, which would bring unaffordable costs to RA.

II. LITERATURE REVIEW

Title: Efficient Hierarchical Identity-Based Signature with Batch Verification for Automatic Dependent Surveillance-Broadcast System
Author: Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, and Wei Wu
- They proposed an efficient TLHIBS scheme and show it is provably secure and can meet summarized security requirements.

Title: How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption
Author: JoonsangBaek, EmanHableel, Young-Ji Byon, Duncan S. Wong, Kitae Jang, and Hwasoo Yeo
- The author proposes a modified version which they call a "Staged Identity-Based Encryption (SIBE)" scheme, to address the aforementioned challenges of providing ADS-B with confidentiality

SYSTEM ARCHITECTURE

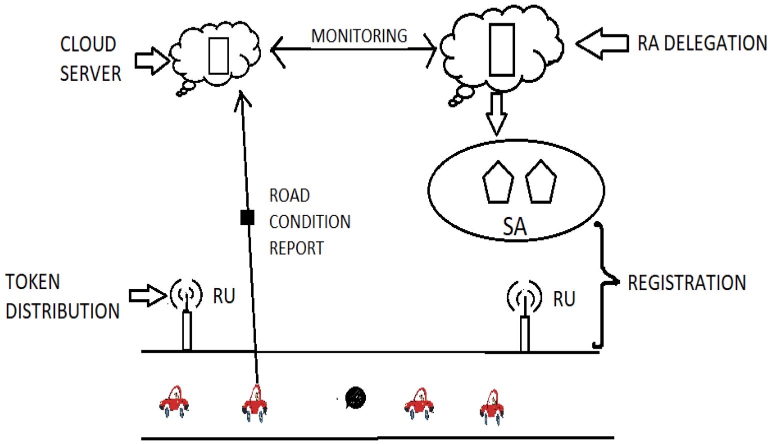


Figure:3.1

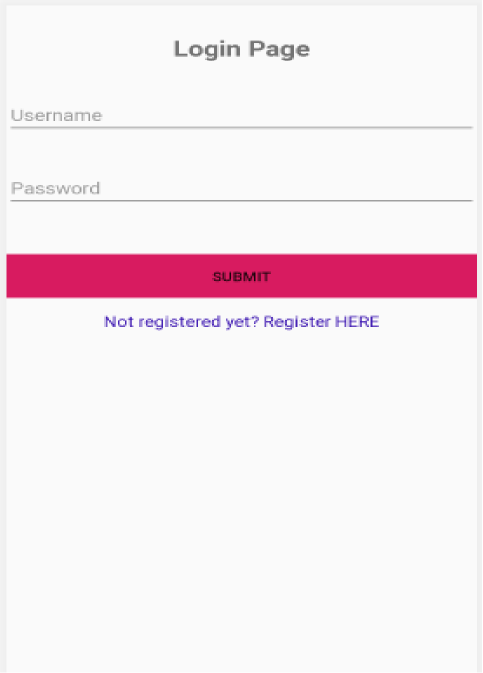
The system architecture consists of five types of entities, that is, a root authority (RA), many sub-authorities (SAs), many roadside units (RUs), a cloud server, and many vehicles. As in VANET, RA, SAs and RUs are the trusted participants. In real-world applications, RA can be the Department of Transportation. The goal of RA is to monitor the real-time road conditions with the help of a cloud server, so that it could make timely response to emergency cases. The cloud server is maintained by some cloud service provider (CSP), which has significant computing and storage resources, and provides on-the-move access to outsourced data (i.e., road condition information) to end users. In RCoM, the cloud server is a curious entity, which is engaged by RA to maintain and process all road information collected by vehicles.

III. MODULE SETS

Setup(1^K)->(par, msk): On input $1^K$where k is a security parameter, the RCoM system setup algorithm, which is run by the root authority RA, generates the public parameter par for the system and a master secret key msk for itself. **SAdlg(par, msk; SAi) ->ssk$_i$:** On input the public parameter par, the master secret key msk and the identity of some sub-authority SA$_i$, the delegation algorithm, which is run by RA, generates a secret key ssk$_i$ for SA$_i$. Sub-authority SA$_i$ should be able to validate ssk$_i$ before accepting it as secret key. **VHreg(par, Sa$_i$, ssk$_i$, V$_j$) ->vsk$_j$:** On input the public parameter par, the identity SA$_i$ and secret key ssk$_i$ of some sub-authority, and the identity of some vehicle V$_j$, the vehicle registration algorithm, which is run by SA$_i$, generates a secret key vsk$_j$ for V$_j$. Vehicle V$_j$ should be able to validate vsk$_j$ before accepting it as secret key. **RUreg(par,SA$_l$,ssk$_l$,RU$_l$) ->rsk$_l$:** On input the public parameter par, the identity SA$_l$ and secret key ssk$_l$ of some sub-authority, and the identity of some roadside unit RUl, the roadside unit registration algorithm, which is run by SA`, generates a secret key rsk$_l$ for RU$_l$. Roadside unit RU$_l$ should be able to validate rsk$_l$ before accepting it as secret key. **TKdis(par, (Sa$_i$,V$_j$,vsk$_j$), (Sa$_l$,RU$_l$,rsk$_l$)) ->T$_l$ / L:** On input the public parameter par, the token distribution protocol, which is jointly run by vehicle V$_j$ and roadside unit RU$_l$ with (SA$_i$,vsk$_j$) and(SA$_l$,rsk$_l$), respectively, outputs an authentication tuple T$_l$ including a token theta($_l$) if both sides are honest, or L otherwise. Here, SA$_i$ and SA$_l$ denote the administrative sub-authorities of V$_j$ and RU$_l$, respectively. **RCrep(par,vsk$_j$,T$_l$,RU$_l$, I) -> (U,W):** On input the public parameter par, the secret key vsk$_j$ of vehicle V$_j$, an authentication tuple T$_l$, a roadside unit identity RU$_l$ and some road condition information I, the road condition report algorithm, which is run by vehicle V$_j$, outputs a ciphertext U and a tuple W. **CLpro(par,U,W) ->{0, 1}:** On input the public parameter par and a pair of (U,W), the cloud processing algorithm, which is run by the cloud server, outputs “1” if the pair (U,W) can be inserted into some group; otherwise it outputs “0”. **RApro(par,msk,U,W) -> (RU$_l$, I):** On input the public parameter par, the master secret key msk and a pair of (U,W), the RA processing algorithm, which is run by the root authority, outputs a decrypted pair of (RU$_l$, I).

IV. IMPLEMENTATION

Step 1:



Login Page

Username

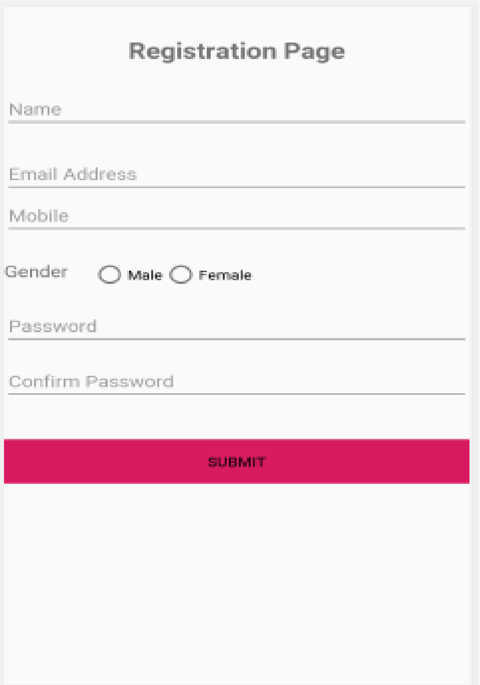
Password

SUBMIT

Not registered yet? Register HERE

Login from app

Step 2:



Registration Page

Name

Email Address

Mobile

Gender ○ Male ○ Female

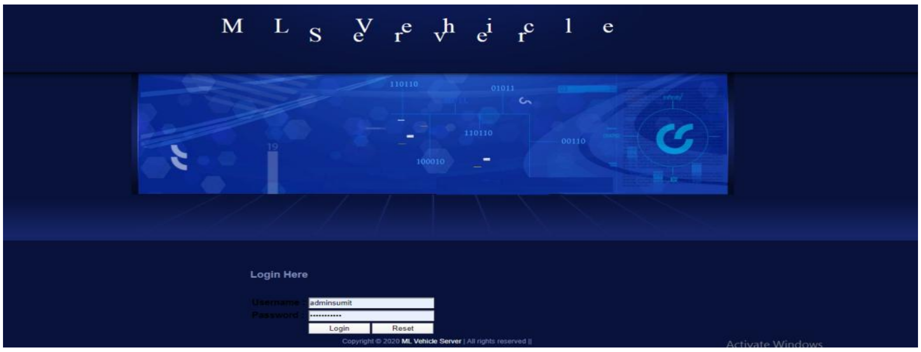
Password

Confirm Password

SUBMIT

Registration

Step 3:



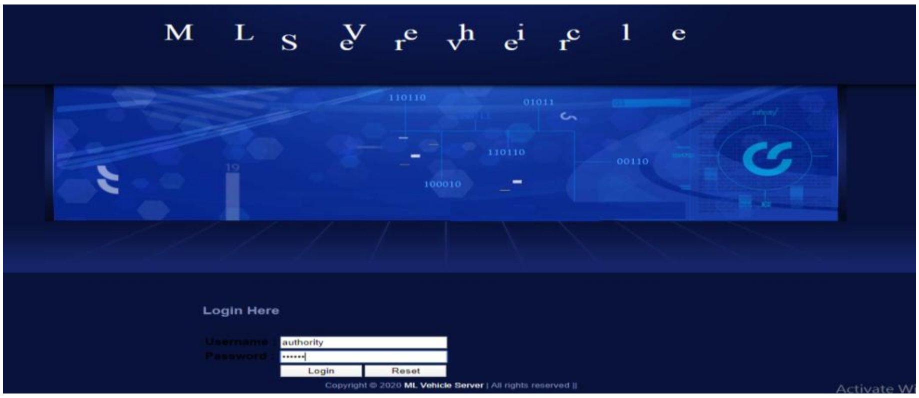
Login Here

Username : adminsumit
Password : ••••••••••••

Copyright © 2020 ML Vehicle Server | All rights reserved ||

User homepage and updating GPS location

Step 4:



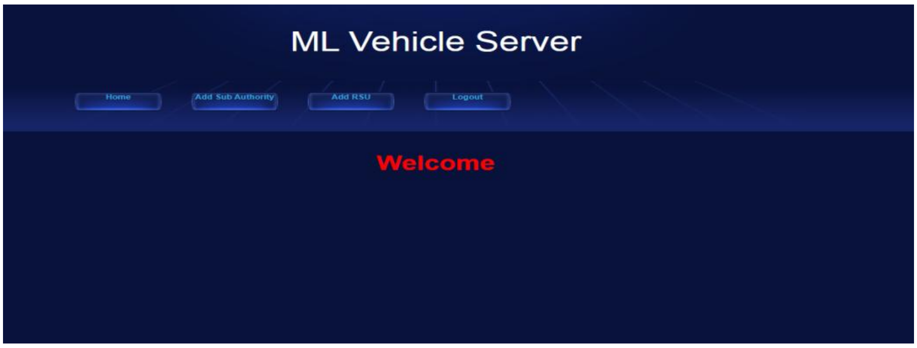
Login Here

Username : authority
Password : •••••••

Copyright © 2020 ML Vehicle Server | All rights reserved ||

GPS tracker

Step 5:

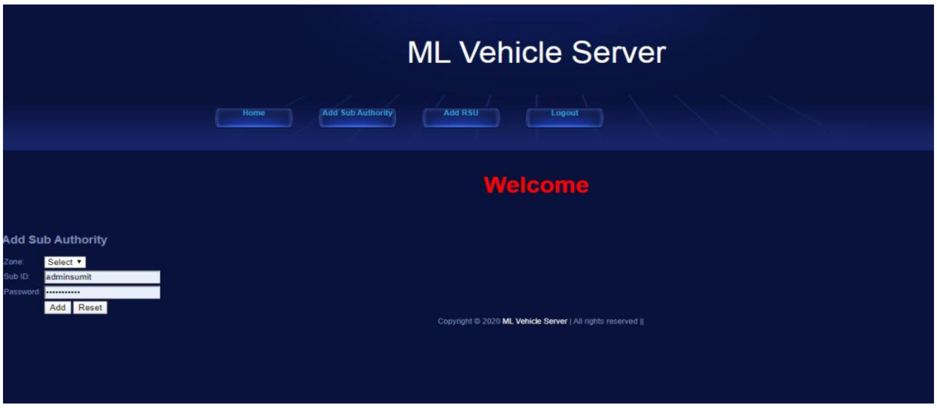


ML Vehicle Server

Welcome

Authority home

Step 6:



ML Vehicle Server

Welcome

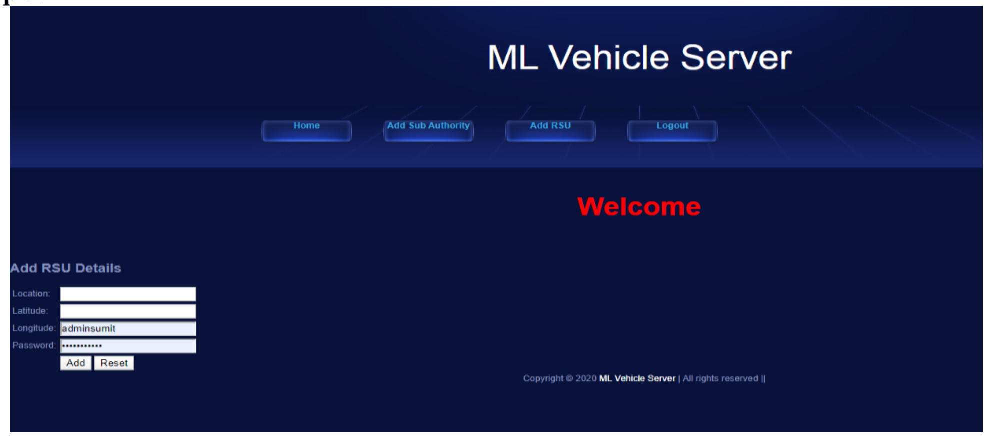
Add Sub Authority

Zone: Select ▾
Sub ID: adminsumit
Password: ••••••••••••

Copyright © 2020 ML Vehicle Server | All rights reserved ||

Add Sub-authority

Step 7:



Add RSU Details

Location:

Latitude:

Longitude: adminsumit

Password: •••••••••••

Add Reset

Copyright © 2020 **ML Vehicle Server** | All rights reserved ||

Add RSU

V. EXPERIMENTAL RESULTS

The performance of the Setup, SAdlg, VHreg and RUreg algorithms are shown in Figure 1. The evaluation shows that the Setup algorithm can be completed in less than 20 msec, which is mainly determined by two exponentiations in G. For a delegation, RA can generate a secret key sski for some sub-authority SAi in roughly 7 msec, whereas SAi is able to validate sski with less than 8 msec. These two procedures are presented by DelGen and DelVrf in the figure. The vehicle registration enjoys the comparable performance of the roadside unit registration, that is, the secret keys vskj and rskl can be generated by sub-authorities in roughly the same time, and the verification at respective sides of vehicle and roadside unit also takes the similar time. Figure 2 plots the performance of the token distribution TKdis protocol, and the RCrep and RApro algorithms. The experiment results are shown in Figure 3, which demonstrate that the performance linearly determined by the number of equivalence classes at the cloud server side. It is easy to see that the average execution time of comparing with a single equivalence class is roughly 4 msec.

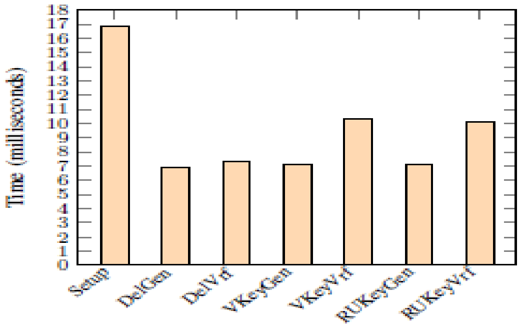


Fig.1. Performance evaluation of the Setup, SAdlg, VHreg and RUreg algorithms.

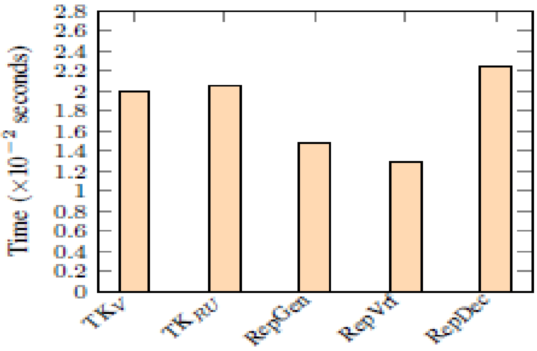


Fig.2 Performance evaluation of the TKdis protocol, and the RCrep and RApro algorithms.

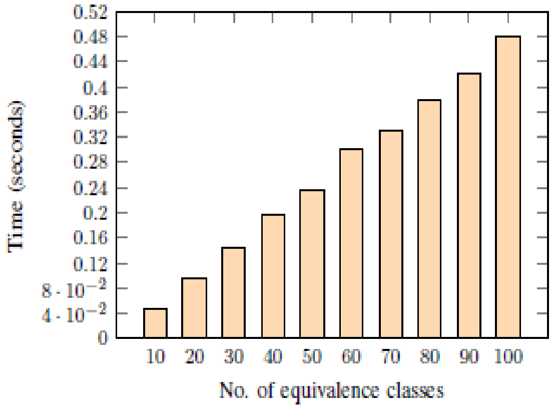


Fig. 3. : Performance evaluation of the CLpro algorithm.

VI. CONCLUSION AND FUTURE WORK

In this article, we considered the problem of a secured data sharing among vehicles to keep track of road condition. There are two levels of authorities such that the root authority delegates sub authorities to perform registration for vehicles and RUs. RA monitors real-time road conditions through a third party intermediary, that is, vehicles report the detected road conditions to the cloud server for verification and processing, in this way, only the valid information sent from legitimate vehicles will be picked out for RA to make response. To protect the privacy against the cloud server, the road condition report should be uploaded in cipher text format, which brings another challenge for the cloud server to distinguish the same road condition for the same place from lots of reports. In response to these functionalities and security and privacy requirements, we presented an efficient scheme and compared it with related techniques. Through extensive theoretical and experimental analyses, we demonstrate that the proposed RCoM scheme is practical in application settings and we can increase the performance of privacy requirements.

REFERENCES

[1] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, “Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,” IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 559–573, Feb 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[3] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, “Probabilistic public key encryption with equality test,” in Topics in Cryptology - CT-RSA 2010: The Cryptographers’ Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings, J. Pieprzyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 119– 131

[4] L. Chen, S. L. Ng, and G.Wang, “Threshold anonymous announcement in vanets,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, March 2011.

[5] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection for the masses,” IEEE Computer, vol. 45, no. 1, pp. 39–45, Jan 2012.