ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

PROTECTING PRIVACY IN LOCATION-BASED VEHICULAR SERVICES USING VPROOF

S.SWATHIGA
PG Student
Department of CSE
Rajas Engineering College
Vadakkangulam
ss1341993@gmail.com

P.SIVASAMY
ASSISTANT PROFESSOR
Department of CSE
Rajas Engineering College
Vadakkangulam

Abstract—Computing technologies, such as sensing and wireless communication, have enabled intelligent transportation systems (ITS), with which people can achieve safer and more efficient everyday transportation. ITS system for services such as real-time traffic control and roads maintenance. However, before accepting data about a location reported by a vehicle, ITS operators need to verify if the vehicle visited the location at the time indicated in the reported data. Failing to do so will allow malicious users to launch an attack to the ITS system. To verify whether a vehicle's location claims match its actual historical locations, ITS operators need a location proof scheme featuring the following properties. The location proof should be lightweight. The location proof needs to well preserve users' location privacy. To detect malicious users, each vehicle is secured with some cryptographic keys. Each vehicle will sign each piece of data with its secret key before uploading to the ITS system. Vproof, which is a lightweight and privacy preserving location proof solution. Vproof is the first location proof solution designed for vehicular environments and the first that does not rely on PKI to achieve the functionalities of location proofs. An efficient algorithm that can reliably determine if two series of packet RSS are similar given potential packet losses and inaccurate RSS measurements.

I. INTRODUCTION

1.1 AREA OVERVIEW

1.1.1 Network security

Network security consists of the policies adopted to prevent and monitor authorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Communication between two hosts using a network may be encrypted to maintain privacy. Network security is mainly used by using the username and password. Networks can be private, such as within a company, and others which might be open to public access.so it is easy and safe to handle.

1.1.2 Network security concepts

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e., the password, this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle')

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware.

Communication between two hosts using a network may be encrypted to maintain privacy. Honeypots, essentially decoy network-accessible resources. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot.

A honeypot can also direct an attacker's attention away from legitimate servers. A honey pot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet contains one or more honeypots.

1.1.3 Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

1.1.4 Key generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

1.1.5 Encryption

The Advanced Encryption Standard (AES), also known as (its original name), is a specification for the encryption of electronic data. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware

1.1.6 Types of attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Two Types of attacks are

- Passive attack.
- Active attack.

Passive attack

This attack is mostly performed by sending modification changes to the file or any other data.

- Network.
- Wiretapping.
- Port scanner.
- Idle scan.

Active attack

This attack doesn't send the report of malicious attack.

- Denial-of-service attack.
- DNS spoofing.
- Man in the middle.
- Phishing.

II.LITERATURE SURVEY

2.1VR-Defender: Selfdefense against vehicular rogue APs for drive-thru Internet,"Hao Han, FengyuanXu, Chiu C"

Vehicular rogue APs are set up in moving vehicles to mimic legitimate roadside APs so as to lure users into associating with them. Due to the mobility, a vehicular rogue AP is able to maintain a long connection with users, which gives the adversary more time to launch various attacks and steal users' sensitive data. A practical user-side detection scheme is proposed to prevent users from connecting to vehicular rogue APs without the help of a network administrator. In solution, each AP broadcasts its GPS location; thus, a vehicular rogue AP has to forge its location to evade detection.

A lie detector algorithm based on information collected and exchanged by clients is then used to validate whether the reported location is fake, aiming to detect the rogue AP. Implemented the prototype and evaluated it on commercial off-the-shelf devices. Observed that our scheme can achieve more than 90% accuracy in real-world experiments. The drive-thru Internet has been of special interestin the wireless communication research community forseveral years.

Rouge APs in vehicular networks can be broadly classified into two categories: stationary and mobile. In the first category, a stationary rogue AP is set up at a fixed place, such as in a building facing a busy road. It is relatively easy for authorities to detect such a rogue AP. Since a vehicular rogue AP can follow traffic on a road, such an AP is able to maintain a long connection, which gives the adversary more time to launch various attacks. Therefore, this type of rogue APs is more dangerous.

Advantages

- It is relatively easy for authorities to detect such a rogue AP.

Disadvantages

- Aps adversary can launch various attacks to steal the user's secrets. The time left for detection is restricted.

2.2 CARAVAN: Providing Location Privacy for VANET. K.SampigethayaLepingHuangy, MingyanLia, Radha

In vehicular ad hoc networks (VANET), it is possibleto locate and track a vehicle based on its transmissions, duringcommunication with other vehicles or the road-side infrastructure.This type of tracking leads to threats on the location privacyof the vehicle's user. The problem of providing location privacy in VANET by allowing vehicles to prevent tracking of their broadcast communications. First, identify the unique characteristics of VANET that must be considered when designing suitable location privacy solutions.

Based on these observations, A location privacy scheme called Caravan is proposed, and evaluate the privacy enhancement achieved under some existing standard constraints of VANET applications, and in the presence of a global adversary.Vehicular ad hoc networks (VANET) enable vehicles to communicate among themselves (V2V communications) and with road-side infrastructure (V2I communications). The communication unit of the access points is called Road Side Units (RSU).Such networks present various functionalities in terms of vehicular safety, traffic congestion reduction, and location based service (LBS) applications. Recognizing the potential of VANET, The unique requirements of maintaining liability of vehicles involved in accidents, and ensuring the safety rendered by the communication between vehicles, challenge the network connectivity, privacy, certain security aspects. theproblem of allowing any vehicle to be able to achieve unlinkability between two or more of its locations in presence of tracking by an adversary.

Advantages

- VANET, it is possible to locate and track a vehicle based on its transmissions, during communication with other vehicles.

Disadvantages

- The location tracking information about a user can be misused by an adversary.

2.3 Enhancing the security of local danger warnings in VANETs—A simulative analysis of voting schemes

Vehicular ad-hoc networksdoes not only facilitate novel telematics applications, butalso poses strong requirements on security. Especially theadoption of active safety applications may raise new threats to road safety if security issues are not properly handled, thus thwarting their initial purpose. A special active safety application is considered that enables cooperative foresighted driving through the exchange of local danger warnings, which are based on individual observations and refer to the current road condition.From a security point of view, the decision whether or not such an applicationshould rely on a reported hazard, is a crucial issue, which cannot be completely protected by conventional security measures. An additional security mechanism is proposed is information centric evaluation of the plausibility of received hazard messages. It is reasonablemeans to increase the stability and security of a cooperative local danger warning service.VANETs - Vehicular Ad hoc Networks - are a subset of the class of mobile, self-organizing and decentralized networks, called mobile ad hoc networks (MANETs), that consist of cars acting as mobile routers. A couple of research projects have addressed technologies and applications dedicated to VANET. The lightweight plausibility checks on application level of nodes that can be expected in most traffic scenarios and complements conventional security measures.

Advantages

- The major stimuli for VANETs are the desire to further increase road safety and traffic efficiency by using communication.

Disadvantages

- Plausibility of received hazard messages, so it cannot be completely protected by conventional security measures.

2.4 AMOEBA: Robust Location Privacy Scheme for VANET Krishna Sampigethaya, Mingyan Li, Leping Huang, RadhaPoovendran.

Communication messages in vehicular ad hoc networks (VANET) can be used to locate and track vehicles. While tracking can be beneficial for vehicle navigation, it can also lead to threats on location privacy of vehicle user. Addresses the problem of mitigating unauthorized tracking of vehicles based on their broadcast communications, to enhance the user location privacy in VANET.Compared to other mobile networks, VANET exhibits unique characteristics in terms of vehicular mobility constraints.Additional security mechanism based on an information centric evaluation of the plausibility of received hazard messages. We developed four decision methods, which are based on voting schemes, and evaluated them by simulation using two attacks trying to manipulate the decision process by distributing false information. Application requirements such as a safety message broadcast period, and vehicular network connectivity. Based on the observed characteristics. A scheme called AMOEBA, that provides location privacy by utilizing the group navigation of vehicles. By simulating vehicular mobility in freeways and streets, the performance of the proposed scheme is evaluated under VANET application constraints and two passive adversary models. It make use of vehicular groups for anonymous access to location based service applications in VANET, for user privacy protection.

Advantages

- In vehicular groups for anonymous access to location based service applications in VANET, for user privacy protection

Disadvantages

- These protocols has some vulnerable for attacks

2.5 Enhancing Wireless Location Privacy Using Silent Period

"Leping Huang, KantaMatsuura , Hiroshi Yamane, and Kaoru Sezaki"

The Advance of ISM-band radio-based tracking systems (for example, wireless LAN-based tracking system) extends the application of location-based services (LBS), but it also threatens to allow the movement of users to be tracked whenever they are transmitting frames. However, new correlation attacks, which utilize the correlation between the old and new addresses of the same node, can defeat current protection methods.To combat such attacks, the concept of a silent period is proposed. A silent period is defined as a transition period between the use of new and old pseudonyms.Through analysis, the silent period should contain a constant period and a variable period. Silent period protocol is the first step for us to realize random address in wireless location privacy protection. The performance of silent period through simulation. Simulation results show that silent period proposal significantly reduces the duration of time a node can be tracked continuously. Finally, we denote that there are still many open research problems before random address can be implemented to protect wireless location privacy. Silent period protocol is the first step for us to realize random address in wireless location privacy protection. There are various approaches for estimating the location of a mobile nodes. Such high precision tracking system may harm user's location privacy in the future. To protect user from potential threat, there are several research results in Bluetooth and Wireless LAN respectively.A silent period is defined as a transition period between the use of new and old pseudonyms, when a node is not allowed to disclose either the old or the new address. In Bluetooth, there is a need to prevent location tracking using Bluetooth MAC address, channel access code (CAC),device access code (DAC).

Advantages

- Risks are solved by accurately.

Disadvantages

- It won't consider user density and address life time.

2.6VPriv: Protecting Privacy in Location-Based Vehicular Services.

Ralua Ada Popa and HariBalakrishnan

A variety of location-based vehicular services are currently being woven into the national transportation infrastructure in many countries. These include usage- or congestion-based road pricing, traffic law enforcement, traffic monitoring, "pay-as you-go" insurance, and vehicle safety systems. Although such applications promise clear benefits, there are significant potential violations of the location privacy of drivers under standard implementations (GPS monitoring of cars).Develop and evaluate VPriv, a system that can be used by several such applications without violating the location privacy of drivers. The starting point is the observation that in many applications, some centralized server needs to compute a function of a user's path—a list of time-position tuples. VPriv provides two components. The first practical protocol to compute path functions for various kinds of tolling, speed and delay estimation a system that can be used by several such applications without violating the location privacy of drivers.VPriv is resistant to a range of possible attacks.The first practical protocol to compute path functions for various kinds of tolling, speed and delay estimation, and insurance calculations in a way that does not reveal anything more than the result of the function to the server, and an out-of-band enforcement mechanism using random spot checks that allows the server and application to handle misbehaving users. The second component of VPriv addresses a significant concern: making VPriv robust to physical attacks.

Advantages

- VPriv, a system that can be used by several such applications without violating the location privacy of drivers. VPriv is resistant to a range of possible attacks.

Disadvantages

- It can serve the car but it is not a trusted one for vehicle owner.

III. PROPOSED SYSTEM

3.1 SYSTEM ARCHITECTURE

User will generate the report for safer & efficient Transportation ITS. This is known as Vproof or VPackets. ITS system for services such as real-time traffic control and roads maintenance, It will be broadcasted via the Road Side Unit (RSU). RSUs continuously broadcast packets that are specifically for the location .Vehicle user's who registered their details in ITS system as vproof,vproof is collected by the RSU unit and then sends to ITS operator for checking purpose,whether the data given by the user is original or fake. If it is original it sends the secret key to the user,which is performed by key bit. Each vehicle user who registered for proof will get the key which is generated by 16 bit key by using AES algorithm. After checking the data, ITS operator sends them to the RSS database. Which is send to the database by encrypting format? by using the RSA However, before accepting data about a location reported by a vehicle, ITS operators need to verify if the vehicle visited the location at the time indicated in the reported data. Failing to do so will allow malicious users to launch an attack to the ITS system. To verify whether a vehicle's location claims match its actual historical locations, ITS operators need a location proof scheme featuring the following properties. The location proof should be lightweight. The location proof needs to well preserve users' location privacy. To detect malicious users, each vehicle is secured with some Some cryptographic key. This light weight, fine grained report will be verified by the ITS Operator based on the historical claims to classify the authorized &malicious user.

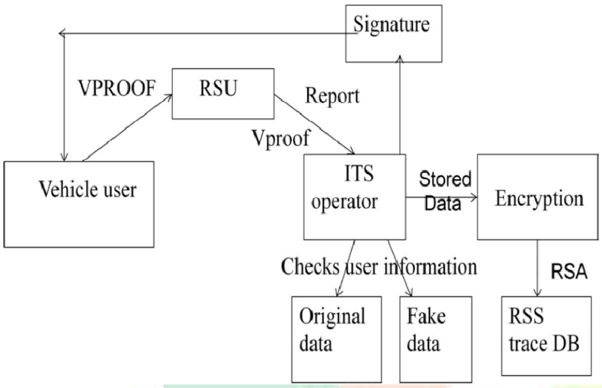


Fig: System architecture

Generating or verifying the VPacket or vproof authentication message. If any unauthorized users trying to steal the users details,it is not possible to do like that,so it is well performed by using AES and RSA algorithms.These algorithms are performed by using 16bit key generation and encryption process.It is the well preserved process for all the vehicle users for their safety and good for ransportation purpose.This vproof is light weight protection privacy preserving and easy to handle. VProofs is used to ensure the user privacy data on the ITS using some cryptographic application.

3.2MODULES

- User registration.
- Vproof report.
- Query parsing execution.
- ITS system.

3.2.1 User registration

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

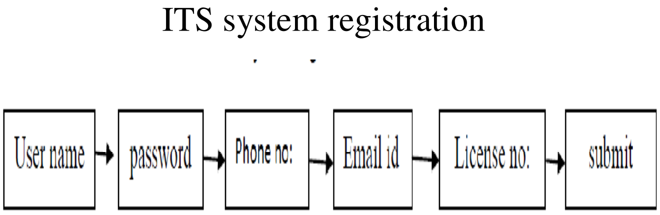


Fig. User registration

3.2.2 Vproof report

VProof, which is a lightweight and privacy preserving location proof solution that verifies if a vehicle's location claims match its historical locations. To the best of our knowledge, VProof is the first location proof solution designed for vehicular environments and the first that does not rely on PKI to achieve the functionalities of location proofs. Design an efficient algorithm that can reliably determine if two series of packet RSS are similar given potential packet losses and inaccurate RSS measurements .It implement a prototype of the VProof system and evaluate the prototype system with extensive experiments performed on real road conditions.

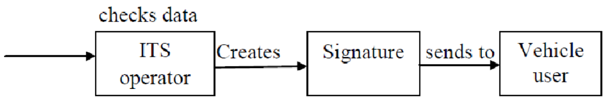


Fig ITS operator

3.2.3 Query parsing and execution

A client defines a database schema and partially populates it. Sensitive attributes are marked using the SENSITIVE keyword which the client layer transparently processes by encrypting the corresponding attributes. A client sends a query request to the host server through a RSU interface. The query is transparently encrypted at the client site using the public key .The host server thus cannot decrypt the query. The host server forwards the encrypted query to the ITS System.The Request Handler decrypts the query and forwards it to the Query Parser. The query is parsed generating a set of plans. Each plan is constructed by rewriting the original client query into a set of sub queries, and, according to their target data set classification, each sub query in the plan is identified as being either public or private. The Query Dispatcher forwards the public queries to the host server and the private queries to the RSS database engine while handling dependencies.

3.2.4ITS operator

VPackets submit the location proofs to the ITS system for verification. Using the information in the location proofs, specifically the transmission power of each VPacket, the ITS operators can restore the inherent VPacket RSS patterns, which are the RSS patterns if the VPackets were transmitted using full power. The location proofs are deemed as valid only if they can be used to correctly restore the inherent RSS patterns of RSUs. Since the transmission power of each VPacket is onlyknown by the ITS operators, enforce the unforgeability of the location proofs VProof constructs. information regarding the user's identity nor link any cryptographic keys with the user, and thus, there is no way users reporting data to the ITS systems can be traced.

3.3 METHODOLOGY

- **Advanced encryption standard (AES)**
- **RivestShamir Adelman (RSA)**

3.3.1 Advanced encryption standard (AES)

The Advanced Encryption Standard (AES), also known as (its original name), is a specification for the encryption of electronic data. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

3.3.2 High-level description of the algorithm

- **KeyExpansions**—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
- **InitialRound**

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

- **Rounds**

SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

- **Final Round** (no MixColumns)
  1. SubBytes
  2. ShiftRows
  3. AddRoundKey.

3.3.3RivestShamir Adelman (RSA)

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm involves three steps: key generation, encryption and decryption.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits'[2] to make factoring harder. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
5. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$).
   - This is more clearly stated as: solve for d given $d{\cdot}e \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond toe and $\varphi(n)$, respectively.
   - d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \operatorname{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.

Since any common factors of (p-1) and (q-1) are present in the factorisation of p*q-1,[9] it is recommended that (p-1) and (q-1) have only very small common factors, if any besides the necessary 2.

Encryption

User transmits her public key (n, e) to User and keeps the private key d secret. User then wishes to send message M to User.First turns M into an integer m, such that $0 \le m < n$ and $\gcd(m, n) = 1$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done efficiently, even for 500-bit numbers, using Modular exponentiation. User then transmits c to user Note that at least nine values of m will yield a ciphertext c equal to m.

Decryption

user can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}$$ Given m, can recover the original message .

IV. EXPERIMENTAL RESULTS ANDDISCUSSIONS

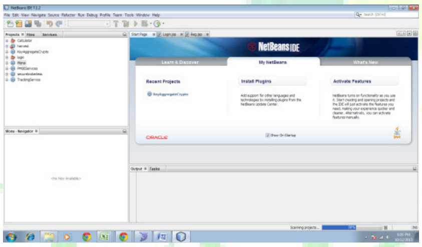
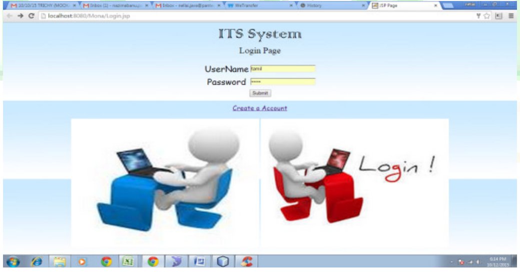


Fig. Run page



localhost:8080/Mona/Login.jsp

ITS System

Login Page

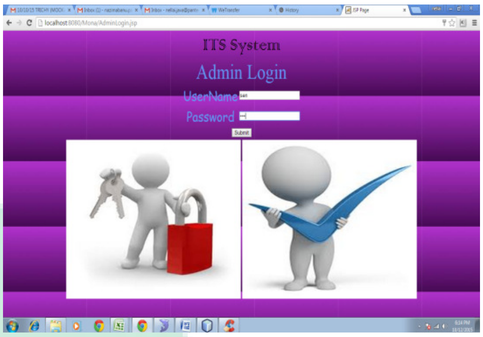
UserName tamil

Password *****

Submit

Create a Account

Fig . Creating account



localhost:8080/Mona/AdminLogin.jsp

ITS System

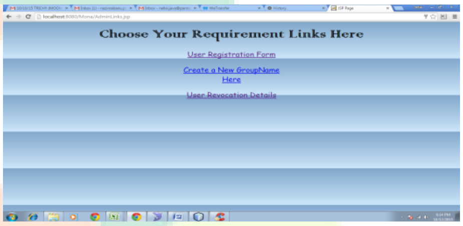
Admin Login

UserName

Password

Submit

Fig. ITS Login page



localhost:8080/Mona/AdminLinks.jsp

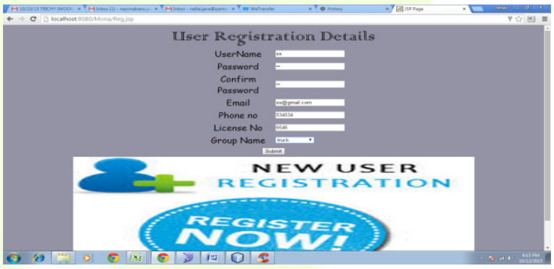
Choose Your Requirement Links Here

User Registration Form

Create a New GroupName Here

User Revocation Details

Fig. Choosing the requirements link



localhost:8080/Mona/Reg.jsp

User Registration Details

UserName ss

Password **

Confirm Password **

Email ss@gmail.com

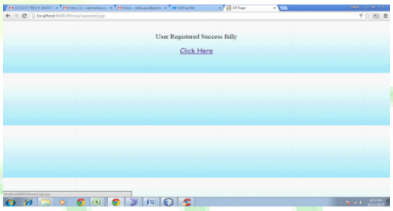
Phone no 534534

License No 6546

Group Name truck

Submit

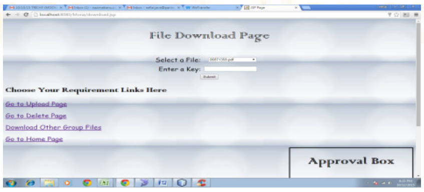
Fig. User registration page



User Registerd Success fully

Click Here

Fig. Registration done



localhost:8080/Mona/download.jsp

File Download Page

Select a File:

Enter a Key:

Submit

Choose Your Requirement Links Here

Go to Upload Page

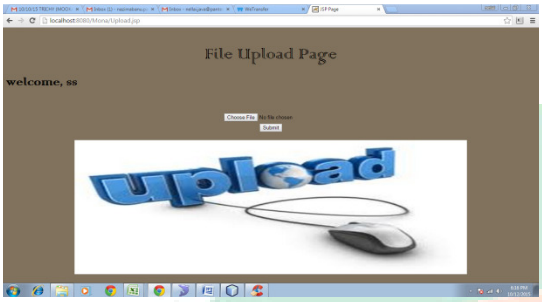
Go to Delete Page

Download Other Group Files

Go to Home Page

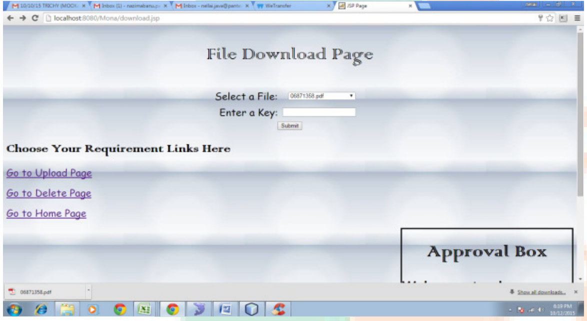
Approval Box

Fig . Approval box


File Upload Page

welcome, ss

Fig. File upload


File Download Page

Select a File: 06871358.pdf

Enter a Key:

Choose Your Requirement Links Here

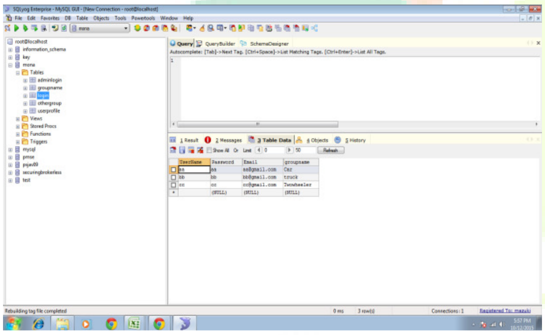
Go to Upload Page

Go to Delete Page

Go to Home Page

Approval Box

Fig. File download page



Autocomplete: [Tab]->Next Tag. [Ctrl+Space]->List Matching Tags. [Ctrl+Enter]->List All Tags.

UserName	Password	Email	groupname
aa	aa	aa@gmail.com	Car
bb	bb	bb@gmail.com	truck
cc	cc	cc@gmail.com	Twowheeler
	(NULL)	(NULL)	(NULL)

Fig. Mysql Database page

V. CONCLUSION

Vehicle Location Proofs to ensure the user privacy data on the ITS using some cryptographic application . VProof is performed by using the ITS system with extensive experiments performed on actual road conditions . It should be verified by the ITS Operator & perform the Location proof verification to avoid the malicious user in the security system. LBD an acceptable location tracking accuracy. A novel method called location-based delivery (LBD), which uses the Global positioning system (GPS) to track the Vehicle's Location base on the latitude and longitude coordinates. Finally, the use of a dynamic threshold reduces the required number of short message transmissions compared with the fixed threshold.

REFERENCES

1. P. Hu, B. Boundy, T. Truett, E. Chang, and S. Gordon, Cross-Cutting Studies nd State-of-the-Practice Reviews: Archive and Use of ITS-Generated Data, 2002.
2. R. A. Popa, H. Balakrishnan, and A. J. Blumberg, "VPriv: Protecting privacy in location-based vehicular services," Aug. 2009, pp. 335–350.
3. C. Manasseh and R. Sengupta, "Middleware for Cooperative Vehicle- Infrastructure Systems," Partners for Advanced Transit and Highways, Richmond, CA, 2008.
4.Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," Mar. 2007,
5. G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proc. VANET, 2007, pp. 19–28.
6. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc, Apr. 2008.
7. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Locationbased trust for mobile user-generated content: Applications, challenges and implementations," in Proc. HotMobile, 2008.
8. S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in Proc. HotMobile, 2009.
9. W. Luo and U. Hengartner, "Proving your location without giving up your privacy," in Proc. HotMobile, 2010.
10. Y. Zhang, C. C. Tan, F. Xu, H. Han, and Q. Li, "Lightweight and Privacy-Preserving Location Proofs for Intelligent Transportation Systems," 2014.
11. K. Sampigethayaet al., "CARAVAN: Providing location privacy for VANET", 2005.
12. J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for location privacy in vehicular networks," Aug. 2007.
13. A.Wasef and X. Shen, "REP: Location privacy for VANETs using random encryption periods," Mobile Netw. Appl., vol. 15, no. 1, Feb. 2010.
14. Y. Zhang, Z. Li, and W. Trappe, "Power-modulated challenge-response schemes for verifying location claims," in Proc. GLOBECOM, 2007.

15. X. Zhenget al., "Characterizing the impact of multi-frequency and multipower on localization accuracy," in Proc. MASS, Nov. 2010.
16.H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, "Defending against
vehicular rogue APs," in Proc. INFOCOM, Apr. 2011.
17. H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, "VR-Defender: Selfdefense against vehicular rogue APs for drive-thru Internet," IEEE Trans.
18. U.S. Department of Transportation, IntelliDrive Data Capture and Management program: Transforming the Federal Role, 2010.