

# Smart Vehicle Insurance Verification System

**T.Sivakumar<sup>1</sup>, L.Kalicharan<sup>2</sup>, R.S.Selvanithila<sup>3</sup>, M.Surekha<sup>4</sup>**

Department of Computer Science and Engineering, Dr. Mahalingam College of Engineering and Technology,  
Pollachi, Coimbatore, India<sup>1,2,3,4</sup>

**Abstract:** Vehicle Insurance is issued by the Road Transport Offices (RTOs) and the Vehicle Registration Certificate (RC) are used by the citizens to drive vehicles across the country. Vehicle Insurance is mandatory while driving. The driver should keep the vehicle insurance while driving. The major constraint is to carry the insurance paid certificate while driving otherwise the driver has to pay penalty for not having the insurance certificate as per the driving laws. In this paper, we propose a online security protocol to verify the insurance certificate and further to authenticate the vehicle's insurance to the traffic police. Also, security services to the personal details present in the insurance certificate are provided during the transmission of data via the Internet. The proposed protocol is simple and easy to implement in real time.

**Keywords:** Digital India, Vehicle Insurance, Online Insurance Verification, Security Protocol, Authentication Service

## I. INTRODUCTION

Disclosing Personal identity information poses substantial trust challenges, both for the people who disclose the information and for those who receive it. Development of Internet technology leads to initiate several online services including e-governance, e-commerce. It is mandatory for the driver to keep the insurance paid certificate while driving. However, it is a big challenge for the driver to bring the insurance certificate during travel. In this paper, an authentication protocol is proposed to authenticate the vehicle with insurance to the traffic police. The desirable security services to the personal details of the insurance certificate are addressed. This protocol helps the drivers by avoiding need of bringing the insurance certificate during travel.

The purpose of the protocol is to verify the vehicle insurance by using vehicle number. The advantages are (a) no need of hardcopy of the insurance certificate (b)only traffic police has smart phone with internet access (c)Application to be installed on the traffic police handled smart phone or other device. The rest of the paper is organized as follows: Chapter 2 presents a brief overview of the existing Protocols and methods. Chapter 3 describes the proposed authentication protocol. Chapter 4 presents the experimental results of the proposed protocol. Chapter 5 describes the conclusion of the paper.

## II. LITERATURE SURVEY

Insurance Number can be combination of numbers and alphabet, which is the unique number. But there must be no information on the insurance unprotected, which enables an application to identify the card holder. There is a need for digital signature signing server due to the fact that the integrity of digital assets is under constant risk of being maliciously or intentionally modified [8]. Authentication can be accomplished in many ways. Authentication protocols are capable of simply authenticating the connecting party or authenticating the connecting party as well as authenticating itself to the connecting party. Digital signature mechanisms can be incorporated in insurance for signature verification [8]. Document is used to create additional public and private sector identity documents like driver's license, bank account passbook, and passport [9].

### 2.1 Vehicle Insurance

Insurance in India are issued by Insurance agencies. For obtaining an Insurance, the owner of the vehicle must have driver insurance, with the minimum age is 18. One must be 18 years or older to drive any other type of vehicle. A police officer or any other official authorized by the government can ask for Insurance documents for verification purpose [5]. While driving, drivers must carry the driving insurance. They should have an additional Badge if they are driving a taxi or any other public transport vehicle [6].

### 2.2 Kerberos Protocol

Kerberos is a widely used authentication protocol. The two main components are (a) ticket, which is used for user authentication and securing data, and (b) an authenticator, used for verification. The major issue with Kerberos is its scalability [3, 14].

### **2.3 Secure Online Authentication**

A digital identity represents a set of unique, distinguishing digital characteristics or claims that could establish the identity of the subject, that is, ensures that the subject is who or what it claims to be [2]. The circulation of electronic official documents is an important part of electronic government activity. It is authenticated by the traditional stamp or manual signature. In [16], digital signature technology and RSA algorithm were applied to provide digital signature on electronic official documents to solve the security problem in the circulation of electronic official documents. The impact of identity theft and fraud as a result of vulnerabilities in online security is staggering. The biggest challenge to organizations, both public and private, is the high cost to implement and manage authentication. Personal privacy and the protection of personally identifiable information become even more critical as nearly everything about a user becomes accessible online [1].

There is a need for digital signature signing server due to the fact that the integrity of digital assets is under risk of being maliciously or intentionally modified. Hence to provide integrity services there can be used a common server for signing that can also be included in the identity management system [4]. Online identity theft being common reason for most of the cybercrime crimes that are happening today and hence there is a need for an efficient online identity system that provide unique identities to overcome online threats. Such systems have many issues such as speed, volume, security, and accuracy [7]. Government has introduced the number plate in vehicles number plate consist of a 8-digit unique number which the Unique Identification number for vehicles issuing for all vehicles of India. It is a random number generated, devoid of any classification based on caste, creed, religion and geography.

Digital documents are easy to generate, modify and manage. The easy modifiable property of digital document makes it more vulnerable to forgery. So the challenge is to produce digital documents that are highly resistant to forgery and reliably confirms the real owner of the document. Because of limited server and network capacities for streaming applications, multimedia proxies are commonly used to cache multimedia objects such that, by accessing nearby proxies, clients can enjoy a smaller start-up latency and receive a better quality-of-service (QoS) guarantee [10]. Online identity theft being common reason for most of the cybercrime crimes that are happening today there is a need for an efficient online identity system that provide unique identities to overcome online threats. Such systems have many issues such as speed, volume, security, and accuracy [8]. The Indian government is initiated the project UIDAI (Unique Identification Authority of India) to provide a unique identification number to each and every citizen of India [15].

Public key cryptosystem offer confidentiality, integrity, authentication, and digital signature services. Both encryption and verification of signature is accomplished with the public key. Public keys are often published to public directories on the Internet so that they can be easily retrieved. This simplifies key-management efforts. The integrity of a public key is usually assured by completion of a certification process carried out by a certification authority (CA). Public key cryptosystems are typically used to provide digital signature service [3, 6, 14].

The issue of Online Authentication and identity are studied extensively. From survey it is observed that there is potential scope to develop new authentication protocols for specific application. This paper deals with the verification of insurance with the help of Vehicle Number in online. The major security challenge is vehicle to communicate the insurance information securely. Thus, it is necessary to offer the security services like authentication, confidentiality, and integrity.

## **III. THE PROPOSED SMART VEHICLE INSURANCE VERIFICATION SYSTEM**

In this section, the working principle of the proposed protocol is presented with sequence diagram. The protocol is primarily developed to authenticate vehicle insurance to the traffic police and to securely share the insurance details between the servers and the traffic police.

### **A. Communication Sequence between the Entities**

The communication sequence between the entities during the verification phase is discussed as follows:

1. Traffic police asks for vehicle insurance during travel for verification.
2. The drivers vehicle number is given to the Traffic police.
3. If the driver drives within district, then the insurance details corresponding to the vehicle number are fetched from the DSP and send to the traffic police for verification.
4. If the driver drives outside of his/her district, then the request is forwarded to the SSP. The details corresponding to the vehicle number are fetched from the database available SSP and send to DSP. A copy the received data is stored at DSP and sends to the traffic police for verification.

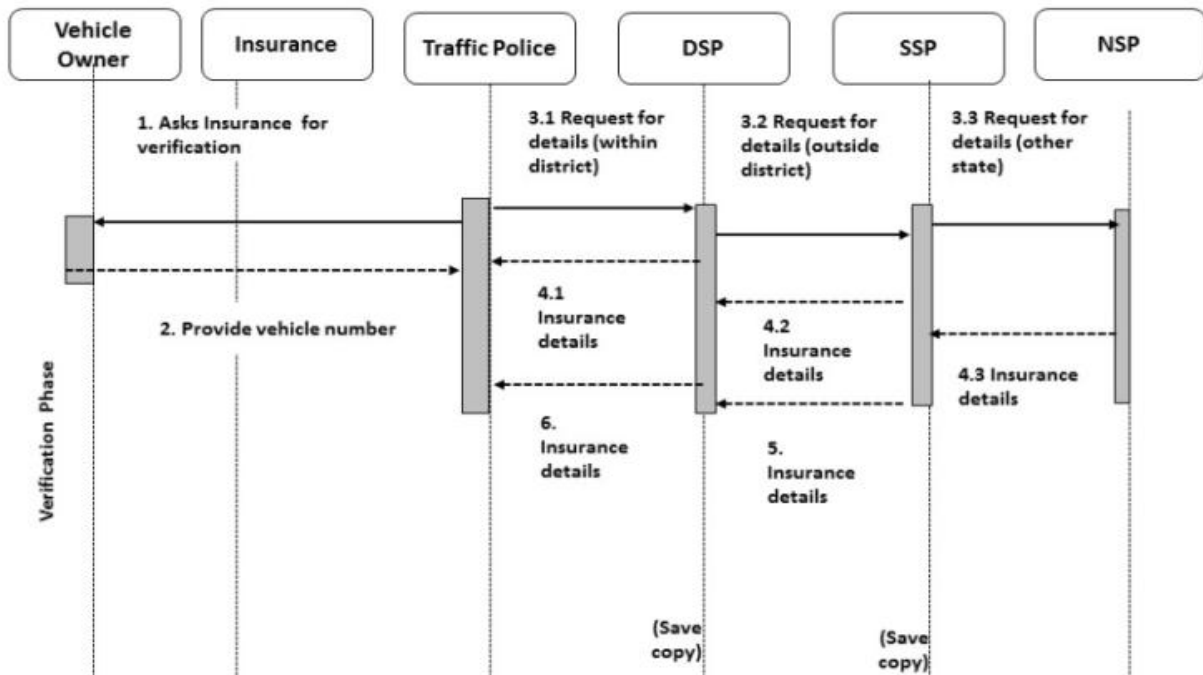


Figure 1. Sequence diagram to depict the communication sequence

5. If driver travels outside state since the details won't be available in the DSP and SSP databases. Then, the request is forwarded to the NSP. The details are retrieved from the centralized database available at NSP and forwarded to SSP. A copy of the insurance details is stored in the SSP and further forwarded to the DSP to keep a copy in the database. From DSP the details are sent to the handheld device available with the traffic police for verification.

**B. Secure Message Exchanges**

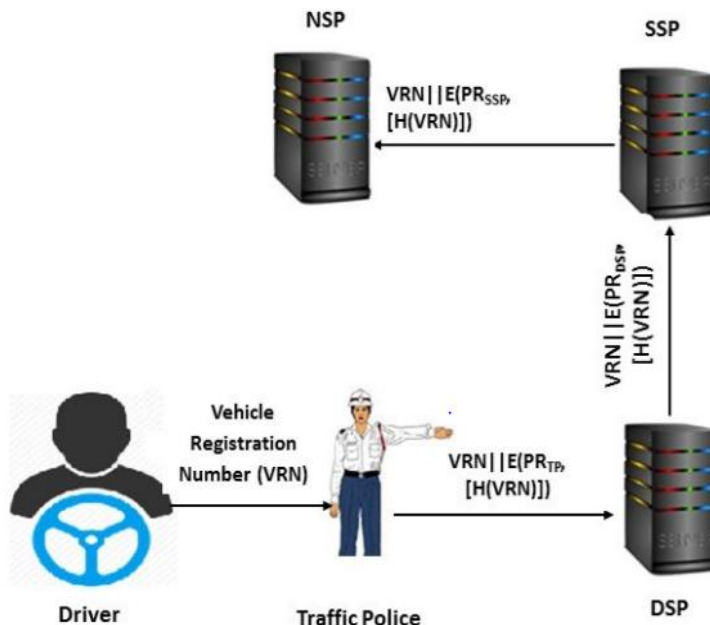


Figure 2. Secure request communication during verification

In this section, the communication sequences between the entities during request and response phases are illustrated. The secure request message exchanges between the entities is illustrated in figure 2. The traffic police request the vehicle number from the driver for verification. Next, the vehicle number is sent to the DSP to get the details corresponding to the vehicle number. If the details are not present in the DSP, then the request is forwarded to the SSP and further to the National Service Provider (NSP), if details are not present in the SSP.

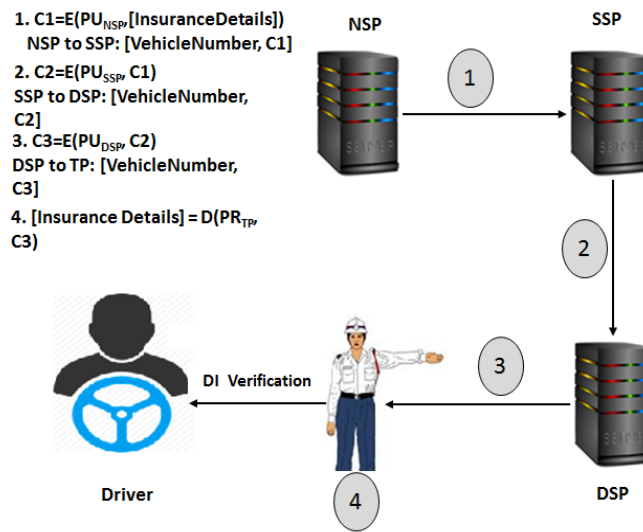


Figure 3. Secure response communication during verification

The response from DSP/SSP/NSP contains the insurance details of the requested vehicle number. If the response is from NSP, the copy of the encrypted details ( $C_1$ ) is stored in the SSP database for future reference without decrypting. From SSP, the  $C_1$  is again re-encrypted to get  $C_2$ . From DSP, the  $C_2$  is re-encrypted to get  $C_3$  and  $C_3$  is forwarded to the handheld device available with Traffic Police. At Traffic Police, the encrypted message received from DSP ( $C_3$ ) is decrypted using a single private key (PR) and the insurance details are displayed for verification. Multi-key RSA algorithm can be utilized to achieve this confidentiality service [10].

**C. Network Topology to Implement the Proposed Protocol in Real Time**

This Client/Proxy/Server architecture has a main server and several proxy servers. These proxy servers in turn have their appropriate clients or a proxy server again. A proxy server is a computer that sits between a client and a server to intercept requests. There are several uses of a proxy server, but the most common is to speed network traffic by caching files that are requested often. By doing so, the proxy server can reply to the request rapidly, only polling the server when required. A proxy server not only speeds up network traffic, but also relieves processing load at the server [7, 10, 11]. Major Internet hubs and Internet Service Providers (ISPs) employ dozens of proxy servers to provide quality of service to the customers. In the proposed protocol, NSP is the main server and both SSP and DSP act as proxy servers. The client is the Traffic Police (TP) with application on the smart phone or laptop. The client/proxy/server architecture to implement the proposed protocol in real time is shown in Figure 4.

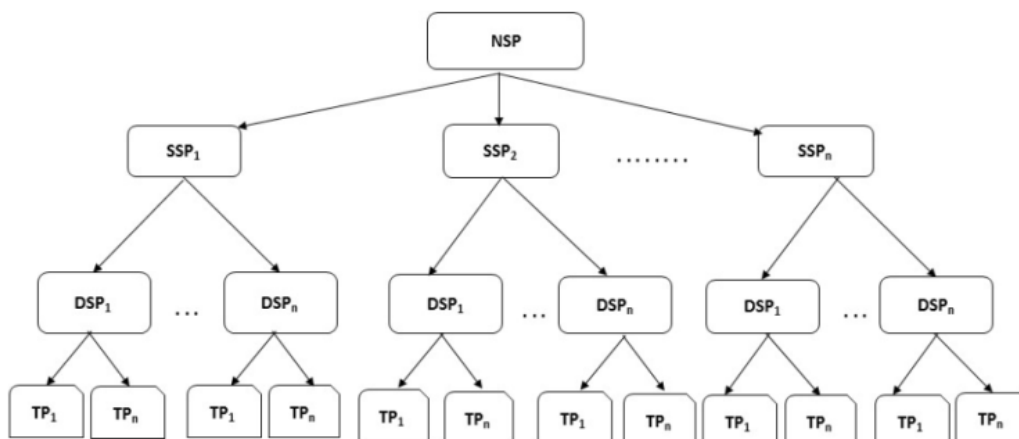


Figure 4. The Proposed Network Topology

It includes the modules such as:

- (a) Traffic Police (TP)
- (b) District Service Provider (DSP)
- (c) State Service Provider (SSP)
- (d) National Service Provider (NSP)
- (e) Data Security Services (DSS)

Insurance details are stored in the database at DSP, SSP, and NSP. Thus, the NSP contains details of the driving insurance nationwide. The National Service Provider (NSP) is the primary server. Insurance detail stored in the servers and proxies are includes vehicle number, owner name, valid from, valid to. When the traffic police enter the vehicle number, the details corresponding to that insurance is first searched in the DSP as the user most travels within the region. If not found in DSP, the search request is forwarded to SSP and then to the NSP, if the search request is from other state. Here, speed is taken care by keeping a copy in the DSP and SSP for the fast retrieval of insurance details. The DSS module is a part of TP, DSP, SSP, and NSP to provide security services such as confidentiality, integrity, authentication, and digital signature during transmission of data between the entities such as TP, DSP, SSP, and NSP. The overload on the main sever can be reduced and the speed of data transmission over network improves greatly. This serves the problem of scalability of the main server. In addition to speed, security services are provided at different levels.

**IV. EXPERIMENTAL RESULTS**

In this section, the experimental result of the proposed vehicle insurance verification protocol is presented.

**A. System Configuration**

The system configuration utilized to experiment the authentication protocol is given in Table 1.

Table 1. System Configuration

<b>Processor</b>	Intel Core i5
<b>Operating System</b>	Microsoft Windows 10
<b>Memory</b>	8 GB RAM
<b>Storage</b>	500 GB
<b>Monitor/Display</b>	14” LCD monitor

**B. Module for administrator**

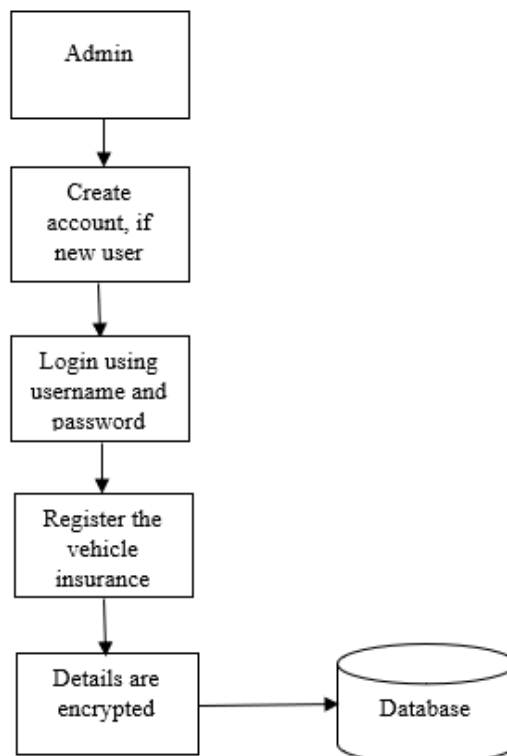


Figure 1: Module for Administrator

Administrator can able to login using username and password. After login, the admin can register the details of vehicle like Vehicle number, Insurance number, Name, Valid date and Issued date of insurance. After clicking register button, the details are stored in the database as shown in Figure 1.

### C. Module for Traffic Police

Traffic Police can able to login using their username and password. New user can create account by giving their user id, name, password and email. Then, police can get the vehicle number. If vehicle number matches with the database then it shows the insurance details. Insurance details are decrypted and then displayed in the user interface as shown in Figure 1.

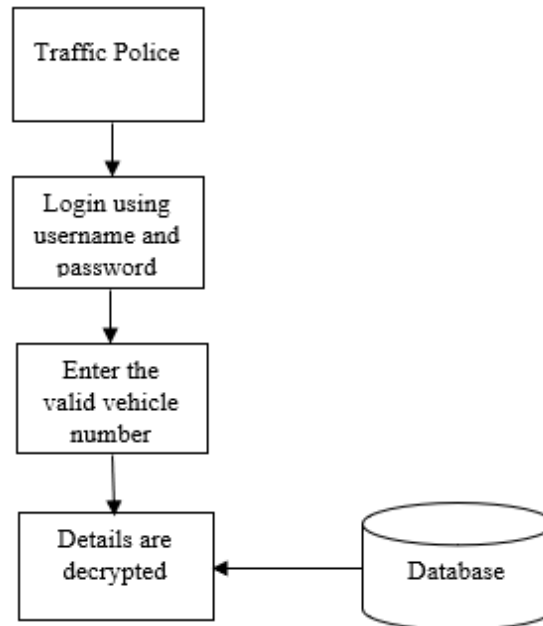
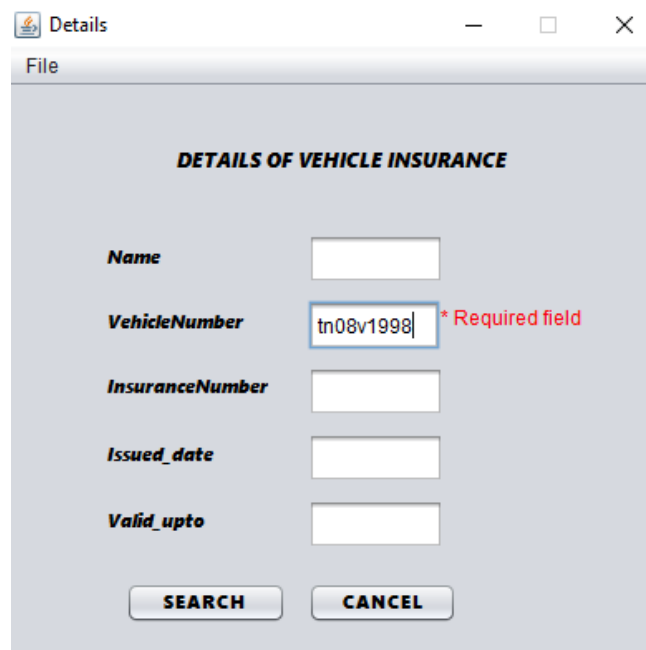


Figure 2: Module for Traffic Police

The user interface provided to the traffic police is shown in Figure 3. The details fetched from the database corresponding to the given vehicle number is shown in Figure 4.



The screenshot shows a window titled "Details" with a menu bar containing "File". The main content area is titled "DETAILS OF VEHICLE INSURANCE". It contains five input fields with labels: "Name", "VehicleNumber", "InsuranceNumber", "Issued\_date", and "Valid\_upto". The "VehicleNumber" field contains the text "tn08v1998" and has a red asterisk and the text "\* Required field" next to it. At the bottom of the form are two buttons: "SEARCH" and "CANCEL".

Figure 3:Details of Vehicle Insurance



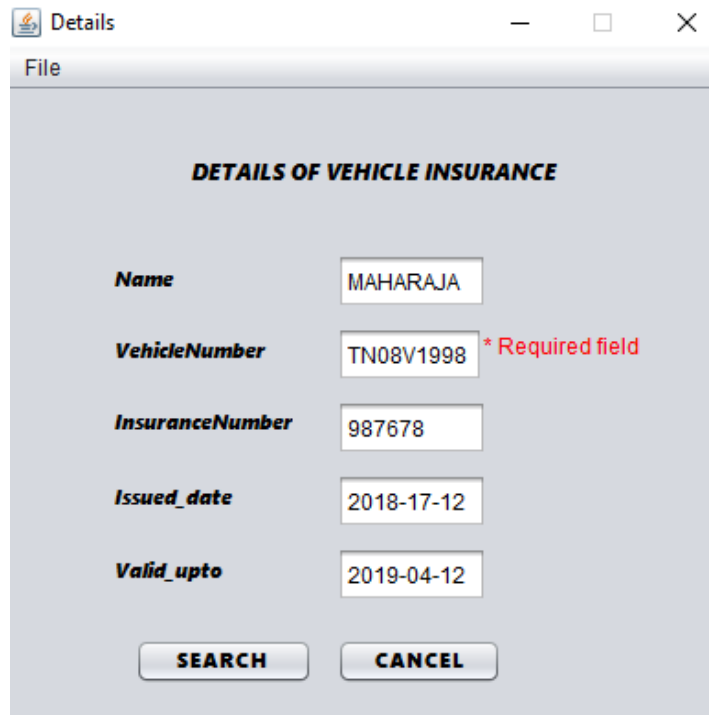


Figure 4: Retrieving Details of Vehicle Insurance

The encrypted version of the data stored in the database is shown in Figure 5.

name	vehiclenum	insurancenum
mOU3jPLhVksikl0p9f/xoQ==	0TQGDcPYOdYM6nqiMinuiA==	++h4nB40pKOPBm206NzD/w==
1z0T3zK4lxknaogZzsZFng==	6AWTIMSYDWKbAGQihTRpPg==	BUaVy7Y7Qc7Uln5T5MM6Nw==
JL6iV8hZhE8oXg0kiALMog==	7B/La4bBCnRB+G0oFqQTRg==	lke8VhmeHKpZJPVy3rwZGg==
Wb49kA/igz8/LqNXbGw4MQ==	DDQFxdWlglvcuPsCsL1jLQ==	YspKRUYN7JuxoUH7u1oN1g==
kmcDVG1RrFGZWRp90G5m4Q==	K3MrI9+0ssT4uGnteGpnAg==	4K178/BEYQGSVxwzIG0FA==
kmcDVG1RrFGZWRp90G5m4Q==	KAHw7xnJj10YvNu2Uqe+TQ==	tbF07nw8gMseQU2iy5LbLQ==
5HCWkpM1H+R6RqCS2S1tVg==	kcFeN7gRb/xEcYzc3tViPg==	wM+RCFqQkIcga19tRfPqnA==
4yOmXWxBZLSHSB/kg0Ih1A==	NqnHS17/3FBk873twjJvZA==	sx5IGLa3KEc4yyYTm0BmPg==
mOU3jPLhVksikl0p9f/xoQ==	RX+nKVDN9w9S2D6UaKq67Q==	mXph4jREq2Ki0n0eamuSBA==
NDgFX3uuXCajbSL40CYMQQ==	V1v8Uj+fbF5uWcTcbEqNQQ==	ZTggMQE8UVJYvqzbQSeTjg==
GQd9JZDjIaCOQJ9DnsJd/Q==	VogGb44v+g1tcWk061KJGw==	oIr6QDGmsw3+XMxA1BSKsw==
A2s/WcCuX5Wg2uC4e7Ei7w==	Yg6DIntn3CJnWaa8AyHAhg==	B/d7HMo1q5o+JbzSWZnpUQ==
+360E/JM/1HWb+xQ30aRgw==	YzYvFpvGQhAVn0c5V5XhgQ==	vu/J77Wpv2PY9eTf75QMAg==

Figure 5: Encrypted details of data in the database

## V. CONCLUSION AND FUTURE WORK

The major constraint for the drivers is to carry the vehicle insurance while driving. In this paper, a secure authentication protocol to provide online verification of vehicle insurance to the traffic police is proposed. The proposed protocol provides security service to the personal details present in the insurance certificate. The protocol helps the drivers by avoiding need of bringing and keeping the insurance copy during travel. The protocol is secure and easy to implement in real time by using the suggested network topology. This work can be extended to identify the theft vehicles by analyzing the database. Also, this work can be extended to trace the misplaced vehicles in crowded open parking areas and the vehicles not taken from the vehicle stand for very long duration.

**REFERENCES**

- [1]. "Online Identity Management needs a Universal Answer", White Paper, Verizon, 2012.
- [2]. Hovav, Anat, and Ron Berger. "Tutorial: identity management systems and secured access control." *Communications of the Association for Information Systems* 25, no. 1 (2009): 1-10.
- [3]. B. Schneier, "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1996
- [4]. Gordon W. Romney and Donald W. Parry, "A Digital Signature Signing Engine to Protect the Integrity of Digital Assets", IEEE, 2006.
- [5]. [https://infogalactic.com/info/Driving\\_licence\\_in\\_India](https://infogalactic.com/info/Driving_licence_in_India)
- [6]. Na, Zhu, and Xiao Guo Xi. "The application of a scheme of digital signature in electronic government." 2008 International Conference on Computer Science and Software Engineering.
- [7]. Narendra Kumar Menta and T. Sivakumar, "Component Based Architecture for Online Identity Management System", International Conference on Innovations in Engineering and Technology for Sustainable Development (IETSD-2012), Bannari Amman Institute of Technology, Vol.3, p.no. 28-32, 3-5 September 2012.
- [8]. Robert Kofler, Robert Krimmer, Alexander Prosser and Martin-Karl Unger, "The Role of Digital Signature Cards in Electronic Voting", Proceedings of the IEEE 37th Hawaii International Conference, 2004.
- [9]. Charney S. The evolution of online identity. *IEEE Security & Privacy*. 2009 Sep;7(5)
- [10]. Siu F. Yeung, John C. S. Lui, David K. Y. Yau, "A Multi-key Secure Multimedia Proxy Using Asymmetric Reversible Parametric Sequences: Theory, Design, and Implementation", *IEEE Transactions on Multimedia*, Vol. 7, No. 2, April 2005, pp. 330 – 338.
- [11]. T. Sivakumar, T. Anusha, and A. Ummu Salma, "A Novel Approach for Online Identity Management System Using Aadhaar Unique Identification Number", National Conference on Recent Trends in Information and Communication Technology (RTICT 2013), Bannari Amman Institute of Technology, 12<sup>th</sup> & 13<sup>th</sup> April, 2013.
- [12]. T. Ylonen, T. Kivinen, M. Saarinen, T. Rinne, S. Lehtinen, "SSH Protocol Architecture" Study Guide.
- [13]. V. Anitha and R. Leela Velusamy, "Authentication of Digital Documents using Secret Key Biometric Watermarking", *International Journal of Communication Network Security*, Volume-1, Issue-4, 2012.
- [14]. William Stallings, "Cryptography and Network Security-Principles and Practice", Pearson Education, New Delhi, 2013.
- [15]. [www.uidai.gov.in/](http://www.uidai.gov.in/)
- [16]. Zhao, Xiao-Ming, and Mei-Ren Zhang. "Application of RSA digital signature technology in circulation of electronic official documents." *Computer Engineering and Design* 26, no. 5 (2005): 1214-1216
- [17]. Stuart Haber, Burt Kaliski and Scott Stornetta, "How do digital timestamps support digital signatures?" *CryptoBytes*, vol. 1, no. 3, RSA Laboratories, 1995, pp. 14-15.
- [18]. Chaum, David :Blinding for Unanticipated Signatures. In: Chaum, David; Price, Wyn (Ed.):Advances in Cryptology, EUROCRYPT '87. Springer-Verlag, Berlin 1987, S.227 –233
- [19]. Rivest, R.: Cryptography and Information Security Group Research Project: E-Voting. In: <http://theory.lcs.mit.edu/~cis/voting/voting.html> accessed on 2001-11-19