# Secure Fully-Automated Taxi Service using ECC

Amar S. Gosavi

Department of Master of Computer Application,
Veermata Jijabai Technological Institute (V.J.T.I)
Matunga, Mumbai, Maharashtra, India

Nikhil B. Khandare

Visvesvaraya National Institute of Technology
Nagpur, Maharashtra, India

## ABSTRACT

This paper creates the secure medium for communication using ECC for fully-automated vehicle network. The proposed protocol given in section 4 achieves the highest level of security and guarantees the safety of vehicles, user, and service provider. The Proposed protocol consists of two phases, key generation, and data transmission. Both the phases are practically being secure and lightweight process because of ECC. Security Analysis of the proposed protocol is given with the help of mathematical proof.

Further modifications and developments of the system are given in future scope section.

## Keywords

ECC (Elliptic Curve Cryptography). Car Automation, Taxi Automation, ECDHP (Elliptic Curve Diffie-Hellman Problem). Secure Communication, Security and Challenges in Vehicle automation.

## 1. INTRODUCTION

Nowadays transportation is required for all people and material to reach correct location. The research is going on to improve transportation services in view of optimization and beneficial way. To improve the profitability of the overall business, transportation takes time, money and manpower. The taxi services a popular way to transfer manpower and material from one location to another location. The leading taxi service companies in India share the profit with car partner. To save the profit share and increase the profit proposed system uses the self-driving car.

In taxi services, the drivers are a major challenge for the taxi companies. As human being have limitations like working capacity and physical fitness. Humans can't work after a limit if they work, like driving car its dangerous for him and other co-passengers with him. One of the best way to avoid human limitations and human interface in taxi services and create the maximum profit from the business is to travel by fully-automated car. Fully-automated car system has multiple securities and challenges [6]. The car communicates on wireless medium with their control station and gets the direction, control, and details about next client to serve. The vulnerable medium between control stations and a car leads to dangerous scenarios [7][8].

The Proposed system will help to create a secure medium of communication between the control station and taxis. Also, this medium is lightweight and heavily secure compared to others. By using the ECC (Elliptical Curve Cryptography) in the system makes it unbreakable from multiple cyber-attacks. ECC is lightweight algorithm to create the lightweight secure medium between the car and a central unit [1].

## 2. PRELIMINARISES

### 2.1 Driver less car

Fully Automated car has various sensors which give the real-time monitoring data. The data is coming from various sensors such as a camera for image and video processing which gives the data related to obstacles, persons, signals, signs, and road.GPS (Global Positioning System) gives the accurate location and direction. Wireless devices like Wi-Fi, Bluetooth helps user to monitor the vehicle. Sound sensors are used for catching the sound waves on road. RADAR helps to detect the object in low light and helps car to travel at night. Lidar also helps to detect the object of visible wavelength. Sensors in car help to get the physical state of the car like speed, turning angle, fuel level and etc. Gyroscope also helps to get angular momentum and accelerometer help to achieve right position on road and speed.

The communication unit communicates with outside world. Processing unit process all raw data and based on the processed data, it gives direction to control unit which acts as muscle in a car and processing unit acts as a brain. Control unit gives the direction to car hardware to execute the command as shown in figure 1.

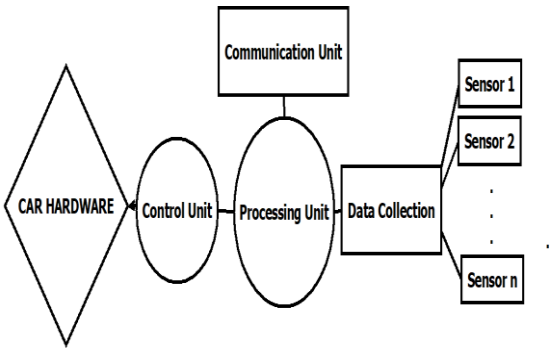


**Figure 1: Architecture of Automated Vehicle**

### 2.2 ECC

ECDLP (Elliptical curve Discreet logarithm Problem) one of the toughest problem based on Elliptical curve cryptography [3][4][5] finding the original private key from the public key is impossible. ECC is lightweight trapdoor function use to generate the key for cryptographic algorithms. ECC beats the RSA considering key size and security as parameter. Since ECC has smaller key size provide better security than bigger key size RSA. The small size of key means less computing power and less amount of energy used in processing. Higher data transfer rate can be achieved using ECC due to lesser key size. ECC function works like following way figure 2.

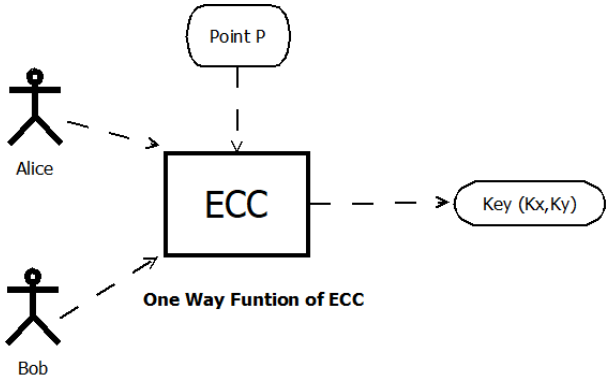


**Figure 2: ECC Block Diagram**

**Point Addition:**
Consider the points P (Px, Py) and Q (Qx, Qy) on elliptic curve E over the finite field F. Line drawn through the above points intersects the curve at R'. The line drawn through R' perpendicular to X axis intersects the curve at R. which denotes the addition of points P and Q on the curve E.

**Scalar Point Multiplication:**
In ECC scalar multiplication is generated by Gq It decides the upper and lower limit of group Q(Qx,Qy) = n . P(Px, Py) where n is belonging to group Gq.

*For example, n=5 then*

$Q=P+P+P+P+P$

$Q=5P \bmod Gq$

Curve is symmetric to X-axis and curve equation is given as $Y^2=X^3+aX^2+b$ and in that A and B are constant values. Where $4A^3 + 27B^2 != 0$. Scalar multiplication of the points which highly secure one-way trapdoor functions.

## 2.3 Secure Mathematical Problem

### *2.3.1 IFP*

Integer Factorization Problem(IFP) difficulty in finding the exact same factors of an integer. If integer I = P*Q finding the exact same P and Q is very hard. because I = (P*Q) = (P1*Q1)=(Pn*Qn). This complexity increases if both P and Q number is the large prime number. The probability of finding the same number is very less.

### *2.3.2 DLP*

Discrete Logarithm Problem(DLP) the problem of finding the unknown number from final number. This is depending on the multiplicative logarithmic cyclic group. The function based on logarithms and power function. G is a generator of group A is number and N is power element. A^N mod G = M where all finding the N from M highly impossible. Same as IFP if all participating number is large prime then the complexity of finding the same number apex level.

### *2.3.3 ECDHP*

Elliptic Curve Diffie Hellman Problem(ECDHP) this is a combination of two secure methods such as ECC and DHP (Diffie Hellman Key exchange problem). For generating the keys, we use ECDHP from the known information finding the secret key of any user impossible. In that, the Alice has private key "A" and Bob has a private key "B" and Point P are known to all. The Alice has a key of PA = P.A same has Bob is PB = P.B the secret share key = P.A.B find any keys not possible from known data member in process.

# 3. PREVIOUS WORK

## 3.1 Potential Cyberattacks on Automated Vehicles

Jonathan Petit at .al [7] has given details in the ITS (Intelligent Transport System) automated vehicle system. Author distinguished two types as self-automated vehicle and cooperative automated vehicles. The cooperative vehicle is connected to an ad-hoc network and communicates with a central control unit. Where central unit controls their activities. Self-automated works as the private vehicle in the normal system.

The author presents the attacking model and its classification on automated vehicle system, signifying details of what target to attack and using relevant media and techniques for same. It also elaborates various ways of how the user can detect the attack. Potential damages caused by the attack on the sensors and system were given in paper

The Author suggested the use of secure digital certificate communication in Vehicular network. It is possible to avoid various cyber-attacks using this certificate. Each party has its certificates. Two types are LTC (Long Term Certificate) and STC (Short Term Certificate) to achieve the good security level.

## 3.2 Cybersecurity Challenges Of Systems-Of-Systems For Fully-Autonomous Road Vehicles

Warren Axelrod [6] has given that system has various venerable elements where the attacker can attack and harm the system has major four components Control System (direct control and in-direct control system), Information system, vehicle control system and transmission line used for data transfer from one to another module as shown in the figure 3.

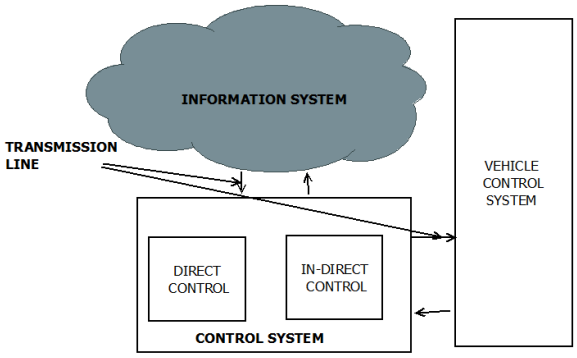


**Figure 3: Modular approach of automated car**

**Control System**
The control system is combination with the Direct and indirect control system. It controls the vehicle during the driving depending on information from an information system. This high-risk system module If an attacker is able to attack this module then system attacker able to do the high level of damage. The control models control the steering, speed, acceleration, breaks etc.

**Information System**
This system consists of various sensors which help to car drive automatically. The data from the sensor are converted into information and given to control system. Depending on information, control unit controls the car. Data consists of the

direction of the vehicle, position on the map, speed, fuel level. Etc. A risk in this system is low as compare to control system.

**Transmission System**
This system is very important for connecting the small module to create the complete automated vehicle driving system. Data is transferred from one module to another module in plan format because of this all internal system required the high availability of data. Hijacking this system has very low probability and but the risk is very high.

**Vehicle Control System**
This is a mechanical model of a vehicle system. How the vehicle control manually by drivers. Driver controls the below machineries like Accelerator, Break, Clutch, Light indication, Signalling. Like the driver, specialized hardware made to control all that machinery of the car.

## 3.3 Security Attacks And Solutions For Vehicular Ad Hoc Networks

The system proposed by J. T Isaac et .al [8] against various attacks on VANNET (Vehicular ad-hoc Network). The author has discussed physical threats/attacks and challenges of the VANNET systems. The author also discussed various solutions for the challenges and attacks. To achieve apex level of security and highly available system for the users. For identifying the unauthorized /malicious vehicle in the network. Author has used Liu's proposed scheme. In Liu's proposed scheme a feedback method is used to generate the honesty level of the car. This feedback is provided by a TDP(Tamper Proof Device) depends on the neighboring nodes. Depending on the honesty score we can identify the malicious vehicle. The author suggested using cryptographic functions or methods to provide security and confidentiality for secure communication between a car and a central control unit (CCU). The author used VIN (Vehicular identification number) to identify each vehicle uniquely. If VIN is compromised then the privacy of the vehicle is also compromised. To overcome this problem, author suggested VIN should be combined with a pseudo-random number. The author suggested the use of a digital certificate which will be able to achieve the required security level.

# 4. PROPOSED SYSTEM

Current taxi services require the driver to drive vehicle manually.

The driver is the important entity in the existing system. The driver has its own physical and psychological limitation such as work timing, health, food and sleep. The driver is important factor in the trip depending upon his driving skills, users gets the trip experience. All humans are not same so all drivers not same, user can hesitate to trust the unknown person but the machines are trusted by the users. So, proposed system overcomes the physical challenge and gives maximum financial benefits to user and service provider. A fully-automated vehicle which is also known as the self-driven car. The self-driven car uses the advanced computing and sensors capacity to achieve the success of the self-driving car.

## 4.1 System and Communication Model

VCM (Vehicle Control Module) controls the vehicle action, and motion. With the help of data from sources such as sensor and CCM(Central Control Module), the VCM control the vehicle. All decisions are taken care of by VCM. VCM act's like the driver for that car and shares the data with CCM and get environmental data from various car sensors. VCM has sensors, GPS, speedometer, accelerometer, gyroscope, and RADAR which gave raw data of physical environment.

CCM is connected with multiple cars in the same geographic location with the help of wireless network (taxi network) and it also communicates with the UCM(User Control Module). UCM has functions like payment, complaint and booking.

The user has to access this module and book the taxi and payment should be done trip starts.. CCO acts as a controlling bridge between UCM and VCM. CCO confirms payment details with the Bank. All the four models communicate as shown in figure 4

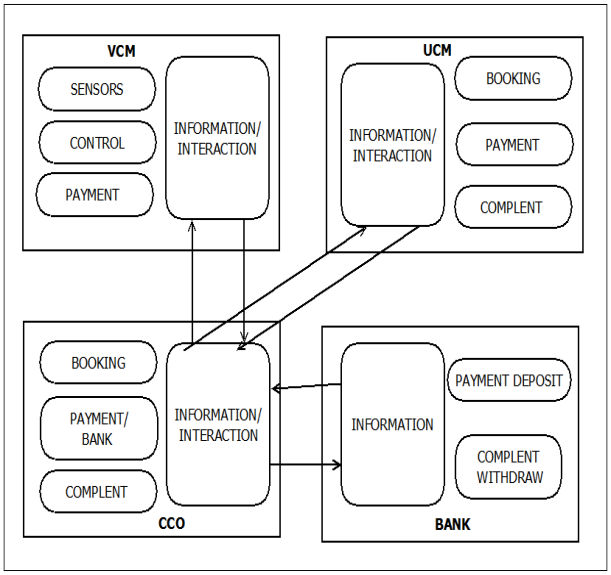


**Figure 4:System and Communication Model**

## 4.2 System and Communication Flow

The user starts the process and first completes the preliminary activities such as user verification, validation, sharing location (source, destination). The locations are important in the process of assigning a taxi. Three parties (VCM, CCO and UCM) create the shared secrete key using ECC. CCO selects the nearest taxi of user's location to which reduces the waiting time and makes process convenient. CCO calculates the trip payment amount, If the payment is done then a taxi is assigned to that request. If the taxi reaches the destination, then the trip is completed. The flow of these processes as shown in figure 5

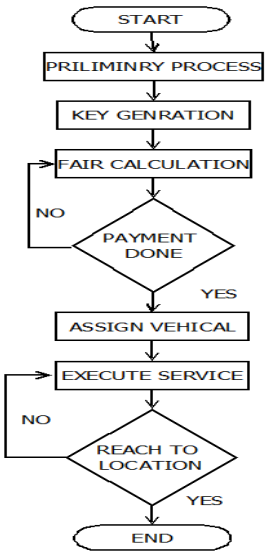


**Figure 5:System and Communication Flow**

## 4.3 Proposed Protocol

The protocol is divided into two phases key generation and secure data transmission that phases make the system highly enhance the security level of the system against the various cyber-attacks. That two models can be describe as follows.

*Notation used*

*PO: Point on Curve E(x,y)*

*G: generator group*

*D: hash function of respective elements.*

*N: random challenge number*

*UN: Unique Number*

*UID: User ID*

*VID: Vehicle ID*

*TID: Trip ID*

*SL: Source Location of User*

*DL: Destination location of User*

*VL: Vehicle Location*

*T: Start Time of Trip*

*Tu: max time limit of user*

*Tc: car current time*

*CCO: Central Control Office*

*UCM: User Control module*

*VCM: Vehicle control module*

*UCMPR: User private key*

*UCMPU: User public key*

*CCOPR: Central office private key*

*CCOPU: Central office public key*

*VCMPR: Vehicle private key*

*VCMPU: Vehicle public key*

*SK: two parties shared keys.*

*E: Encryption*

*D: Decryption*

*KEY: Shared secrete Key.*

### *4.3.1 Key Generation*

In this process of key generation, all three parties have their key pairs public and private key which uses to create the shared secret symmetric key for secure encryption and decryption process. In the algorithm, PO is a point on an elliptic curve same point for all parties using the ECCDHP one of the hard-mathematical problem to solve. The knowing the shared secret key to the attacker is negligible. "." Indicate the elliptical point addition process for each point. In the key, we get two points of a key are x and y coordinate anyone we can be used as the key for next algorithm. The key generation can explain as follows in figure 6.

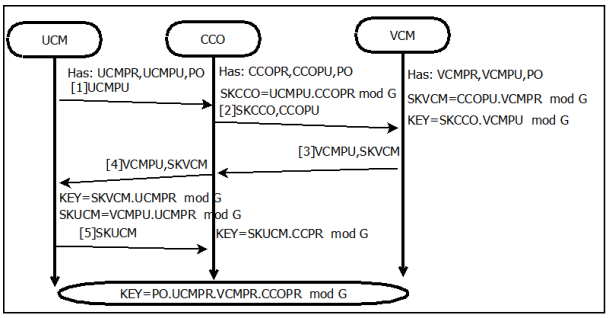


**Figure 6: Key Generation**

**Step1**
UCM send request as their public key UCMPU to CCO. Where UCMPU= PO.UCMPR.

**Step2**
Now CCO received public key of UCM as UCMPU then CCO calculate the SKCCO = UCMPU.CCOPR is equal to SKCCO = PO.UCMPR.CCOPR and send own public key to VCM.

**Step3**
VCM calculate the KEY = SKCCO.VCMPR = PO.UCMPR.CCOPR.VCMPR. Then calculate their own SKVCM=CCOPU.VCMPR now send their public key CCO and SKVCM to CCO.

**Stpe4**
CCO forward VCM packet to UCM and check SKVCM and public key of VCM is VCMPU

**Step5**
UCM calculate the share symmetric secrete KEY = SKVCM.UCMPR = PO.UCMPR.CCOPR.VCMPR and calculate their own SKUCM and send the CCO

**Step6**
CCO calculate their shared secrete key such as KEY = SKUCM.CCOPR = PO.UCMPR.CCOPR.VCMPR mod G

### *4.3.2 Secure Data Transmission*

After the key generation, a secure symmetric key for next phase of the protocol is generated. The key is used for encrypting and decrypting and to transfer data securely between communication parties. Which create the highly secure communication channel.

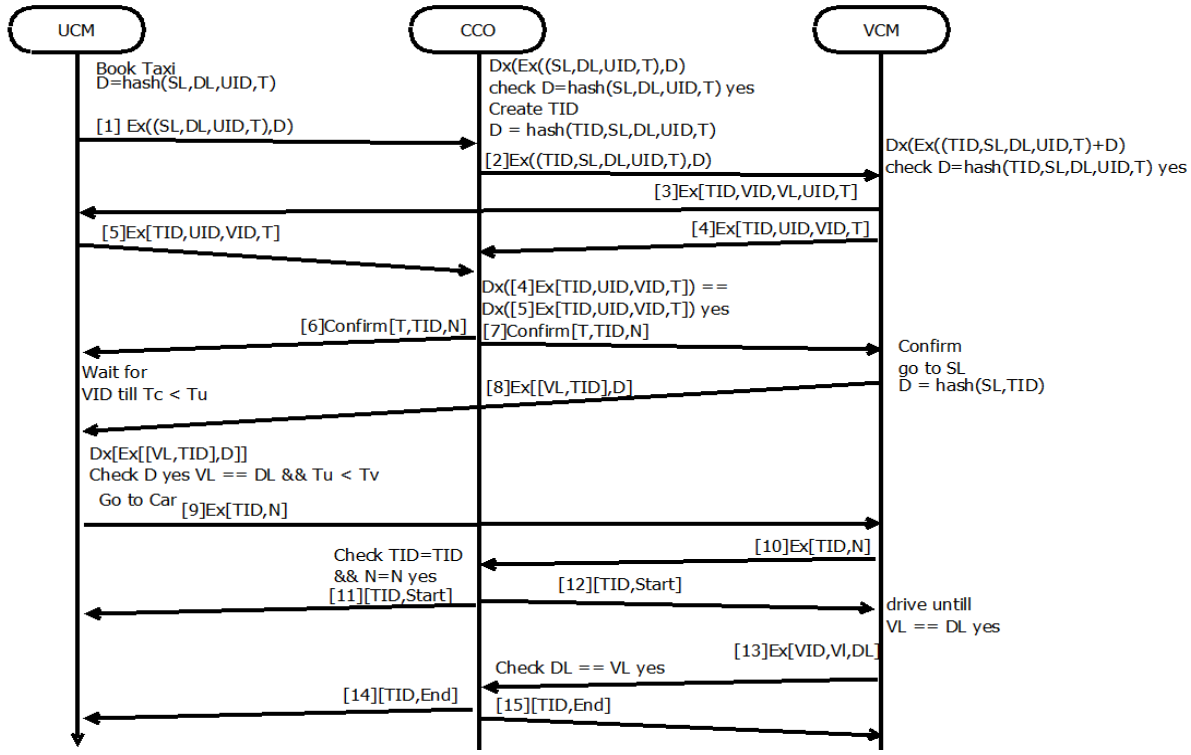


**Figure 7: Secure Data Transmission**

**Step1**
UCM create a request at start UCM calculate is packet hash for avoiding tempering during transfer packet on the network. UCM send its SL, DL, UID and T and the hash of all encrypted data to CCO.

**Step2**
CCO decrypt data and calculate the D(hash) value of the received packet is equals then go further. CCO generate the TID for specific trip id send the D = hash(TID,SL,DL,UID,T)

**Step3**
VCM decrypt the received data packet and check the data packet is matched or not if matches then direct send packet to UCM with the TID.

**Step4**
VCM verify the TID with CCO with respect to UID and Time T.

**Step5**
UCM performs the same step like step 4 which guarantees the TID generated successfully. TID is hash function of all id and a random unique number TID= hash(UID,VID,UN) .

**Step6**
Confirm the TID and send the encrypted data packet with time and n is a random challenge for the user to enter at the start of the trip to VCM 2 step of verification to verify the user.

**Step7**
Confirm the TID and send the encrypted data packet with time and n is a random challenge for the user to enter at the start of the trip to UCM step of verification to verify the user.

**Step8**
VCM check the hash value of data is matched then confirms the user source location to reach and pick up the user to drop at location DL. VCM send its location to UCM.

**Step9**
If VL matched with SL and Tu is less than Tc then vehicle reach the location. UCM send the encrypted random challenge n with VCM and confirm that TID.

**Step10**
VCM check that random number is equal to generated random number by sending to CCO if number matched then send TID start packet to UCM and VCM.

**Step11**
TID start packet send to UCM as acknowledgement.

**Step12**
TID start packet send to VCM as acknowledgement.

**Step13**
The VCM sends regularly current location to CCO to check and verify the car in on the right road.

**Step14 & 15**
Taxi reached location then CCO sends the trip end packet to UCM and VCM.

## 5. SECURITY ANNALYSIS

The system uses the principle of a classical secure mathematical problem such as DLP, IFP, DHP, and ECC which helps securing system. The proposed system and protocol is secured against the various popular cyber-attacks. The security features of the proposed system can be explained as follows.

Phishing is most common attacks on the cyber communication system. The current system suggests all system entity should have id's which will help to identify each user and it is verified with the message digest. Each user has its key pairs are unique also makes phishing impossible.

TID= hash(UID,VID,UN)

The proposed system has time factor which makes Denial-of-Service (DoS) attacks impossible. After the time the session

and TID get expired since the waiting time period is very less which does not affect.

UID wait till Tc < Tu (current time of car is less then max waiting time for user)

Brute Force Attack also not possible on the systems using the ECC which make the uncompromised key pair. Getting value using brute force is not possible.

[1]Ex((SL,DL,UID,T),D)

[2]Ex((TID,SL,DL,UID,T),D)

[3]Ex[TID,VID,VL,UID,T]

[4]Ex[TID,UID,VID,T]

The system is also securing from man-in-middle attacks the proposed key generation is the combination of ECC and DLP which makes impossible for an attacker to attack the system.

KEY=PO.UCMPR.VCMPR.CCOPR mod G

Replay attack also not possible because each trip has their own id which makes replay attack impossible.

TID= hash(UID,VID,UN)

The message digest gives protection from modification of data packets any active attack not possible or alteration of data in data packets.

Securing the control system is one of the big challenges in the proposed system but all communication uses an encrypted and secure channel of data transmission which makes the control system secure

The system data is secure with an apex level of security so no one can misuse the data.

## 6. CONCLUSION AND FUTURE SCOPE

ECC is lightweight and the highly secure way to generate keys. Minimum computer power is used during the process of communication because of small key size. With help of secured communication channel taxi communicates with user directly. Also, payment is done through user's wallet for the trip price. CCS and bank communicate for confirmation of trip amount deduction. The user will reach the destination with minimum challenges and effort. The limitation of a human being is overcome by use of machine which gives more profit to the taxi company with minimum efforts. Also, periodic maintenance of taxi should be done on time which makes taxi safe house for the user.

The system can be implemented for cargo transportation and carrier vehicles. A major concern in the proposed system is when physical damage/ physical attacks take place on system or sensor.

Adding the recovery mechanism from physical damage, finding the nearest fuel station is the enhancement to the existing system. Also scheduling the taxis during peak hours and optimizing the waiting time is another challenge.

## 7. REFERENCES

[1] Amar S Gosavi and Nikhil B Khandare. Securing VoIP Communication using ECC. International Journal of Computer Applications 179(46):13-21, June 2018

[2] Khandare, Nikhil B. "Performance Analysis of Cryptographic Protocols to Enhance SMS and M-Commerce Security."

[3] Ray, Sangram, G. P. Biswas, and Mou Dasgupta. "Secure multi-purpose mobile-banking using elliptic curve cryptography." *Wireless Personal Communications* 90.3 (2016): 1331-1354.

[4] Ray, Sangram, Rachana Nandan, and G. P. Biswas. "ECC based IKE protocol design for internet applications." *Procedia Technology* 4 (2012): 522-529.

[5] Ray, Sangram, and G. P. Biswas. "Establishment of ECC-based initial secrecy usable for IKE implementation." *Proc. of World Congress on Expert Systems (WCE)*. 2012.

[6] Axelrod, C. Warren. "Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles." Emerging Technologies for a Smarter World (CEWIT), 2017 13th International Conference and Expo on. IEEE, 2017.

[7] Petit, Jonathan, and Steven E. Shladover. "Potential cyberattacks on automated vehicles." IEEE Transactions on Intelligent Transportation Systems 16.2 (2015): 546-556.

[8] Isaac, Jesús Téllez, SheraliZeadally, and José Sierra Camara. "Security attacks and solutions for vehicular ad hoc networks." IET communications 4.7 (2010): 894-903.

[9] Ray, Sangram, Urbi Chatterjee, and G. P. Biswas. "Efficient and Secure Communication Architecture for E-Health System."

[10] Hankerson, Darrel, Scott Vanstone, and Alfred Menezes. "Elliptic Curve Arithmetic." Guide to Elliptic Curve Cryptography (2004): 75-152.

[11] Saxena, Neetesh, Bong Jun Choi, and Rongxing Lu. "Authentication and authorization scheme for various user roles and devices in smart grid." IEEE transactions on information forensics and security 11.5 (2016): 907-921.

[12] Braga, A., et al. "Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones." The 9th Intl. Conf. on Emerging Security Information, Systems and Technologies. 2015.

[13] Thomas, Minta, and V. Panchami. "An Encryption Protocol for end-to-end Secure Transmission of SMS." Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on. IEEE, 2015.

[14] Saxena, Neetesh, and Narendra S. Chaudhari. "A secure approach for SMS in GSM network." Proceedings of the CUBE International Information Technology Conference. ACM, 2012.

[15] Miller, Victor S. "Use of elliptic curves in cryptography." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985.