Message authentication on vehicular cloud computing

Mousa Mohammed Gharsan
Department of Computer Network,
Faculty of Engineering and IT,
University of Alandalus
alqadaci2013@gmail.com

Fekri M. Abduljalil
Department of Computer Science,
Faculty of Educ., Arts, & Science,
University of Sana'a,
fmabduljalil@gmail.com

Abstract— *Today vehicular cloud computing technology has been realized to provide better services on demand. A smart vehicle provides powerful resources for computing, storage, sensing, and data delivery. In addition, with the combination of smart vehicle with cloud computing allowing the user to access the hardware, data, and software in the vehicle, for example the user can use the vehicle's on board camera to deliver image on demand. In addition, because open commination is used in Vehicular cloud computing (VCC), there is a risk for important message exchange in VCC environment leads to misguiding users, message forgery, modification wrong information sharing. In this paper VC message authentication service framework (VC-MASF) is proposed to address the limitation of message integrity and message's source authentication in VCC applications.*

Keywords: Vehicular Cloud Computing, PKI, Key manager, Symmetric key, Message signature, Message authentication Code.

1. INTRODUCTION:

For the last few years, smarter vehicles, safer, and less stressful driving experiences have been realized. Currently, ordinary vehicles have devices such as GPS, radio transceiver, small-scale collision radars, cameras, on board computers and different types of sensing devices to alert the driver to all types of road safety conditions and mechanical malfunctions. Vehicles are becoming more sophisticated with on-board storage, powerful on-board computing capabilities, significant communication capabilities and less power limitations which are supported by hosts of sensors, actuators, on board radar and GPS [12].

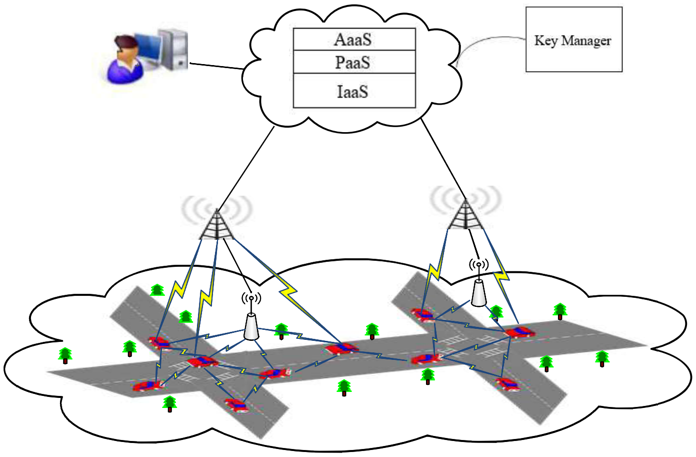


Figure 1: vehicular cloud architecture

The intelligent transportation system plays an important role in road safety, better utilization of traffic signals, traffic management etc…, which aim to improve driving conditions on road and road safety, this known as Vehicular ad hoc network(VANET) [2]**.** VANETs are considered important due to their huge potential and numerous applications. VANETs not only offer immense safety enhancements but also many commercial opportunities. Vehicular Internet: Security & Privacy Challenges and Opportunities. the Vehicular Environment, it is not possible for any user to get the dynamic information from anywhere, anytime. In VANET, the Messages shares between vehicles and with Road Side Units (RSU's) only when the vehicle is within the range of RSU,The vehicles communicate through the supported wireless medium i.e. Dedicated Short Range Communications (DSRC), Wireless Access in Vehicular Environments (WAVE) IEEE 802.11p standard [13].

The vehicles equipped with not only sensors to measure temperature, humidity, wind, etc., but also with cameras and other powerful resources. The large amount of unused storage space and computing power capabilities coupled with on-board provide a unique opportunity to utilize vehicles to be a part of cloud computing. This together with high speed (4G/LTE) connectivity can be a great advantage for a variety of applications[13].

The increasing vehicular cloud computing usage, the significance of security in this area is also increasing, providing security in a vehicular network is more difficult than in other network due to open communication, high mobility and wide range of vehicles. Therefore, there are various security that threaten the security of vehicular cloud computing, these threats can be classified into five parts, namely, confidentiality, authentication, on-repudiation, localization and verification data [12]. In this paper message authentication is addressed, which confirm that the message came from an authorized user and has not been changed in transit. There are various security techniques used for message authentication, but some of the them are not compatible in vehicular cloud network due to their large computation power and time According to researcher's knowledge all the previous researches address the message authentication from vehicular ad hoc communication view, in this message authentication from vehicular cloud computing view is addressed by proposed a vehicular cloud message authentication service framework (VCMASF).

The remaining of the paper is organized as follows. section 1. reviews the background and related works. section 2. contains the proposed work. section 3. HMAC background. section 4. EC background. Section 5. concludes the paper. section 6. References

1. RELATED WORK

Chenxi Zhang [1] Proposed a message authentication scheme, named RAISE, which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. The proposed scheme provides an efficient identity-based batch signature verification scheme for vehicular communications, which enable vehicles to verify a batch of signatures once instead of one after another and efficiently increase vehicle's message verification speed.

Al-Sultan,others [2] Described that VANET is a subclass of mobile ad hoc network MANET, in which each vehicle acts as a node creating a network in the road with either another node or with a road side unit(RSU)located along the road. Each vehicle is supported with wireless sensing devices, which helps to establish communications between vehicles and RSU.This technology has been used in a range of applications such as predicting the correct route, controlling accidents and avoiding traffic jams and congestion.

Sherali Zeadally,others [3] Presented a lot of attentions from researcher to take care in vehicular network that still need further investigation and innovative solutions due to its interesting and promising applications in vehicular safety services, location based services and traffic congestion avoidance. The main focus must be on safe driving application wherever each vehicle periodically broadcasts messages with its current position, road formation and direction as well as speed.

Khana,others [4] Described that vehicular networks are the suitable networks that enable a communication among vehicles and vehicles to road side unit which can be used for intelligent transportation systems to obtain render safety, comfort and convenience on the road. However, because of lack of infrastructure and centralized administration, it becomes vulnerable to misbehaviors, proposed algorithm DMN-Detection of Malicious Nodes in VANETs improves DMV Algorithm in terms of effective selection of verifiers for detection of malicious nodes and hence improves the network performance.

Papadimitratos,others [5] Described that vehicular networks emerge as one of the most convincing and yet most challenging instantiations of the mobile ad hoc networking technology, security and privacy are critical factors and significant challenges to be met, outline security requirements for vehicular communication systems, provide models for the system and the communication, propose a set of design principles for future security and privacy solutions for vehicular communication systems.

Supriya, others [6] Introduced an overview of vehicular clouds, discussed the security challenges of VC, provide a directional security scheme to illustration an appropriate security architecture that handles several challenges of security in VCs

Abhale, others [7] Described the architecture of vehicular ad-hoc network, introduced the vision and architecture of mobile-vehicular cloud computing, discussed the security challenges in vehicular cloud.

Saurabh.others [8] Proposed an authentication scheme “Message Digest and Location based Authentication (MDLA)” to validate the mobile client and the cloud server participating in the mobile cloud computing, MDLA consists of three key phases, which are registration, authentication, and update. The operations of the scheme MDLA begins if and only if a mobile client is registered with the cloud service provider, used a protocol analyzer to validate the registration and authentication phases.

Mamun ,others [9] Proposed a GS scheme, based on pairing-based construction of Groth with additional properties. He presented a reliable and standard CPA-secure GS solution to a vehicular network application, suggested using of LM (Link Manager) that provides restricted privacy appropriate for a real time VANET environment and protects against DoS (Deny of Service) and Sybil attacks as well. He used batch verification which can significantly improve the performance of signature verification that makes the solution applicable for real life vehicular communication.

Sharma,others [10] Proposed a key authentication scheme for vehicular cloud environment. The proposed scheme for authenticating both the sender and receiver based on the ECC. The scheme also used one-way hash function and concatenation operation for secure communication. The proposed system aims to detect malicious vehicles in the network and maintain overall trust between the vehicles. From the obtained results, it is proved that proposed scheme better results as compared to other

Papadimitratos,others [11] Described security architecture for VC systems aiming at a solution that is both comprehensive and practical, discussed problem of identifying threats and models of adversarial behavior as well as security and privacy requirements that are relevant to the VC, He introduced a range of mechanisms to handle identity and credential management, and to secure communication while enhancing privacy.

2. PROPOSED WORK

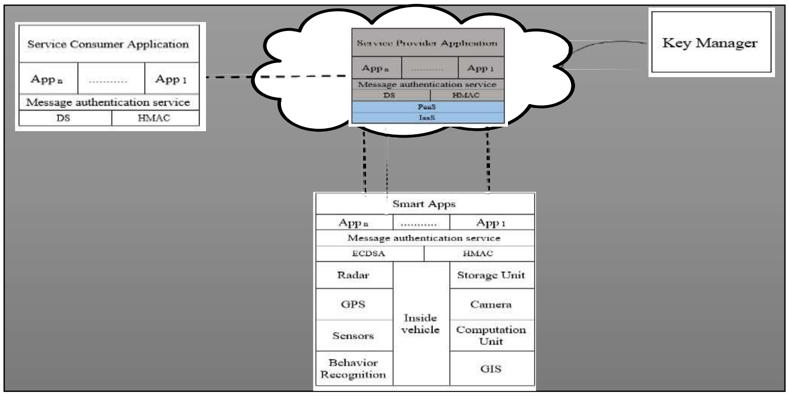


Figure 2: VC-MASF

In the proposed vehicular cloud message authentication service framework (VC_MASF), the message exchange between vehicular cloud applications is two type as the following:

1- Periodic message (Message sent periodically)

2- None periodic message (Message sent on demand)

In periodic message: the proposed message authentication scheme used is HMAC because signing/verifying every message every period of time (for example every 100ms) produce overhead and it is impossible.

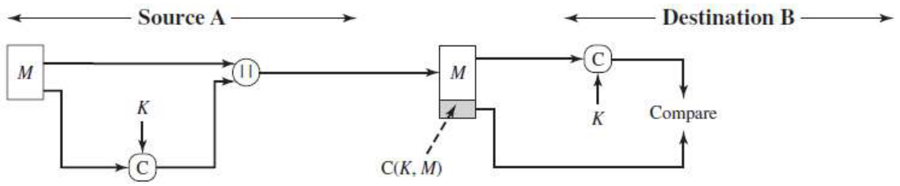


Figure 3: Message authentication Code,source=[16]

HMAC scheme process

1- Registration: In these phase, each vehicle needs to resister itself to a key manager, who is responsible for distributing a pair of private/public (SK/PK) key, and public key certificate to each vehicle. In addition, the key manager also plays a role as a security authority, who is capable of tracing their real identities of vehicles form their certificates. This role is important and necessary specially when criminal events happen. Thereby, during the registration, vehicles/drivers must provide the key manager with the real identity information. The registration process needs to be done before application communication. The Public/ private key generation can be achieved by adopting Elliptic curve private/public generation algorithm, because EC provide high level security with minimum key size comparable to other public key algorithm like RSA, gamal …etc[15]

Public/private generation and public key corresponding certificate distribution algorithm.

ACTIONS:

Step 1: Select an elliptic curve E defined over Zp. The number of points in E(Zp) should be divisible by a large prime n.

Step 2: Select a point P € E(Zp) of order n.

Step 3: Select a statistically unique and unpredictable integer d in the interval [1; n - 1].

Step 4: Compute Q = dP.

Step 5: public key is (E, P, n, Q), A's private key is d

Step 6: getting the public key certificate from certification authority C= E(SK_{auth}, [T||ID||PK]) where SK_{auth} is the private key used by the authority and T is a timestamp

2- Manual authentication &Symmetric Key Establishment:

In these phase, vehicle (V) initiate a mutual authentication process with service provider (SP), SP verifying the vehicle signature and its corresponding public key certificate. A valid signature means that the vehicle is a legitimate user in VCC. The messages that have been signed by vehicle and service provider include secret credentials, which can be used to compute a shared key. Here, Diffie-Hellman key exchange secured with signature could be adopted to establish the shared symmetric key[14], the shard key used for a period of time (time stamp) and need to be reestablished.

$V \rightarrow SP$: $\{aP \mid Cert_V\}PKV$.

$SP \rightarrow V$: $ID \mid bP \mid \{ID \mid aP \mid bP\}SKSP$.

$V \rightarrow SP$: $\{ID \mid bP \mid aP\}SKV$

where aP and bP (a, b ∈ Z q, P is a generator of an addition group G) are random elements of the Diffie-Hellman key establishment protocol, and the shared session key between the Receiver and Sender is K ← abP . When receiving the first message from the Sender, the SP decrypts $\{aP \mid Cert_V\}PK_{SP}$ (| as a concatenation operation) with its private key SK_{SP}, and then verifies the V's public key PK_V in the anonymous certificate $Cert_V$. Then, the SP sends ID | bP | {ID | aP | bP }SKsp to the Sender. The Sender verifies the signature {ID | aP | bP }

on ID | aP | bP . At last, the Sender sends back the signature {IDsp | bP | aP}SKv, and the receiver verify the signature.

3- HMAC computing and Verification: Having the shared key between sender and receiver. The sender can use it to compute a HMAC of a message, and then sends a tuple (ID, message, HMAC) to receiver (CS). Since the receiver has the shared key, it can verify the HMAC and then accept or reject the message.

In none periodic message: the proposed message authentication scheme used is DS, because signing/verifying only to message requesting on demand which doesn't produce overhead. The message digital signature can be achieved by adopting Elliptic curve digital signature algorithm (ECDSA), because ECDSA provide high level security with minimum key size comparable to other public key algorithm like RSA, Elgamal …etc[15]

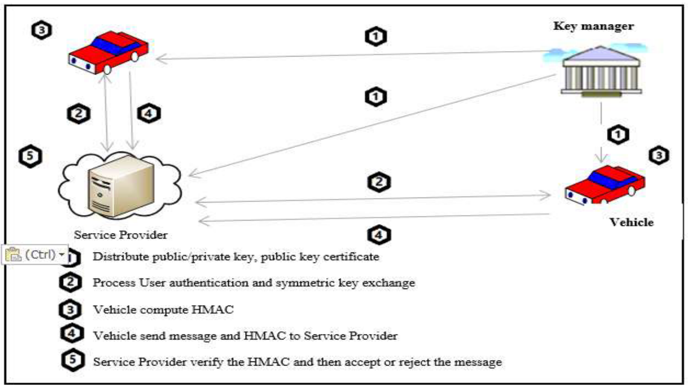

Key manager
Service Provider
Vehicle
(Ctrl)
1 Distribute public/private key, public key certificate
2 Process User authentication and symmetric key exchange
3 Vehicle compute HMAC
4 Vehicle send message and HMAC to Service Provider
5 Service Provider verify the HMAC and then accept or reject the message

Figure 3: VC-MASF

DS scheme process [17]

1- Registration: In these phase, each vehicle needs to resister itself to a key manager, who is responsible for distributing a pair of private/public (SK/PK) key, and public key certificate to each vehicle. In addition, the key manager also plays a role as a security authority, who is capable of tracing their real identities of vehicles form their certificates. This role is important and necessary specially when criminal events happen. Thereby, during the registration, vehicles/drivers must provide the key manager with the real identity information. The registration process needs to be done before application communication. The Public/ private key generation can be achieved by adopting Elliptic curve private/public generation algorithm, because EC provide high level security with minimum key size comparable to other public key algorithm like RSA, Elgamal …etc[15]

Public / private key generation and public key corresponding certificate distribution.

ACTIONS:

Step 1: Select an elliptic curve E defined over Zp. The number of points in E(Zp) should be divisible by a large prime n.

Step 2: Select a point P € E(Zp) of order n.

Step 3: Select a statistically unique and unpredictable integer d in the interval [1; n - 1].

Step 4: Compute Q = dP.

Step 5: public key is (E, P, n, Q), A's private key is d

Step 6: getting the public key certificate from certification authority C= E(SK_{auth}, [T||ID||PK]) where SK_{auth} is the private key used by the authority and T is a timestamp

2- Signing message:
In these step, sender compute hash value of a message H(M), Signing the message using its private key: sign $sender_{PRV}$ H(M)||M, and then send M, signature, certificate to receiver.

Signing message algorithm

INPUT: Message m, private key d.

OUTPUT: Signature (r, s).

ACTIONS:

Step 1: Select a statistically unique and unpredictable integer k in the interval [1; n - 1].

Step 2: Compute kP = (x1, y1) and r = x1 mod n. (Here x1 is regarded as an integer, for example by conversion from its binary representation.) If r = 0, then go to step 1 (This is a security condition: if r = 0, then the signing equation s = k-1{h(m)+dr} mod n does not involve the private key d.)

Step 3: Compute k^{-1} mod n.

Step 4: Compute s = k-^{1}{h(m) + dr} mod n, where h is the Secure Hash Algorithm (SHA-1).

Step 5: If s = 0, then go to step 1. (If s = 0, then s^{-1} mod n does not exist; s-^{1} is required in step 3 of signature verification.)

Step 6: The signature for the message m is the pair of integers (r; s).

3- Signed message verification:
In these step, the receiver verifies the certificate of sender, if it is legitimate user in VCC, the receiver verifying the signed message using sender public key :very senderPK (H(M)), In addition the hash value compared with the hash, the hash value H is obtained after the manual verification to check whether message integrity is guaranteed.

Signing message verification

INPUT: Message m, signature (r, s);Public signing key Q(x,y) , the signature components r and s, and the base point G(x,y)

OUTPUT: Accept or reject signature.

ACTIONS:

Step 1: Verify that r and s are integers in the interval [1; n - 1].

Step 2:. Compute w = s-^{1} mod n and h(m).

Step 3: Compute u1 = h(m)w mod n and u2 = rw mod n.

Step 4: Compute u1P +u2Q = (x0, y0) and v = x0 mod n.

Step 5: Accept the signature if and only if v = r

3. BACKGROUND IN HMAC

In this section a quick introduction to the theory of message authentication based on hash function (HMAC) is introduced . Chapter 12.2 of William stalling book [16] provides a background of HMAC. MAC (Message authentication code) is an alternative authentication technique involves the use of a secret key to generate a small fixed-size block of data, known as a cryptographic checksum or MAC, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key. When A has a message to send to B, it calculates the MAC as a function of the message and the key: where
M= input message
C = MAC function
K= shared secret key
MAC = message authentication code
The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC. If we assume that only the receiver and the sender know the identity of the secret key, and if the received MAC matches the calculated MAC, then
1. The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the MAC, then the receiver's calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to know the secret key, the attacker cannot alter the MAC to correspond to the alterations in the message.

2. The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper
MAC.
3. If the message includes a sequence number (such as is used with HDLC, X.25, and TCP), then the receiver can be assured of the proper sequence because an attacker cannot successfully alter the sequence number.
A MAC function is similar to encryption. One difference is that the MAC algorithm need not be reversible, as it must be for decryption.
A MAC, also known as a cryptographic checksum, is generated by a function C of the form T = MAC (K, M) Where M is a variable-length message, K is a secret key shared only by sender and receiver, and MAC (K, M) is the fixed-length authenticator, sometimes called a tag. The tag is appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by precomputing the tag.
A MAC derived from a cryptographic hash function. The motivations for this interest are
1. Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES.
2. Library code for cryptographic hash functions is widely available. In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.

HMAC Algorithm

Defining algorithm terms.

H = embedded hash function (e.g., MD5, SHA-1, RIPEMD-160)

IV = initial value input to hash function

M = message input to HMAC (including the padding specified in the embedded hash function)

Y_i _ i th block of M, $0 > i < (L – 1)$

L _ number of blocks in M

b _ number of bits in a block

n _ length of hash code produced by embedded hash function

K _ secret key; recommended length is n; if key length is greater than b,

the key is input to the hash function to produce an n-bit key

K+ _ K padded with zeros on the left so that the result is b bits in length

ipad _ 00110110 (36 in hexadecimal) repeated b/8 times

opad _ 01011100 (5C in hexadecimal) repeated b/8 times

Then HMAC can be expressed as
HMAC(K, M) = H[(K+ _ opad) || H[(K+ _ ipad) || M]]
Algorithm

1. Append zeros to the left end of K to create a –bit string K+ (e.g., if K is of length 160 bits and b = 512, K will be appended with 44 zeroes).

2. XOR (bitwise exclusive-OR) K+ with ipad to produce the -bit block Si .

3. Append to Si`.

4. Apply H to the stream generated in step 3.

5. XOR K+ with opad to produce the b-bit block So .

6. Append the hash result from step 4 to So.

7. Apply H to the stream generated in step 6 and output the result.

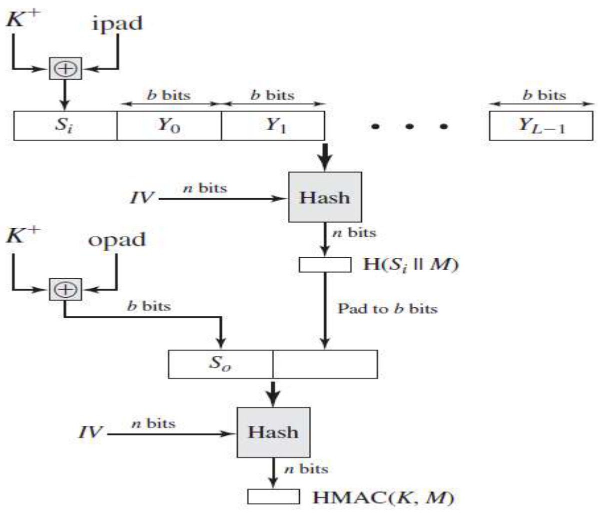


Figure 4: HMAC algorithm, source=[16]

4. BACKGROUND IN ELLIPTIC CURVES:

In this section a quick introduction to the theory of elliptic curves (EC) is introduced. Chapter 10.3 of William stalling book [16] provides a background of elliptic curves arithmetic and elliptic curve cryptography. For simplicity, I will restrict background to EC over Finite group. Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA. As we have seen, the key length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA.This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. A competing system challenges RSA: elliptic curve cryptography (ECC). ECC is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. Elliptic curve cryptography makes use of curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used applications: prime curves over Zp and binary curves over GF($2m$) . For prime curve over Zp , we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p - 1 and in which calculations are performed modulo p.

*y*2 mod *p* = (*x*3 + *ax* + *b*) mod *p* (10.1)

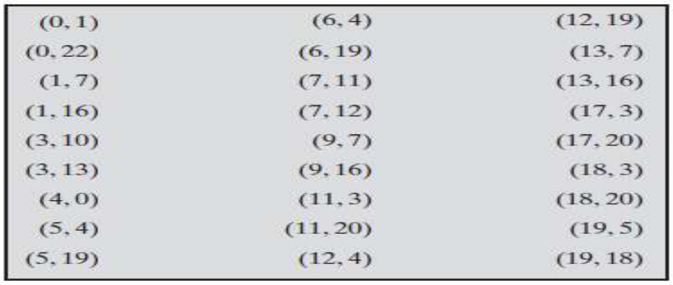
For example, Equation (10.5) is satisfied for *a* = 1, *b* = 1, x = 9, y = 7, α= 1, p = 23

72 mod 23 = (93+ 9 + 1) mod 23

49 mod 23 = 739 mod 23

3 = 3

Now consider set consisting of all pairs of integers that satisfy Equation (10.5), together with a point at infinity *O*. The coefficients a and b and the variables *x* and *y* are all elements of *Zp*, example, let *p* = 23 and consider the elliptic curve *y*2 = *x*3 + *x* + 1. In this case, a = b = 1. For the set E23(1, 1), we are only interested in the integers in the quadrant from (0, 0) through (*p* - 1, *p* - 1) that satisfy the equation mod *p*. Figure 5 lists the points (other than *O*) that are part of E23(1, 1), Figure 6 plots the points of E23(1, 1); note that the points, with one exception, are symmetric about *y* = 11.5.



(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

Figure 5: Points on the Elliptic Curve E23 (1,1)

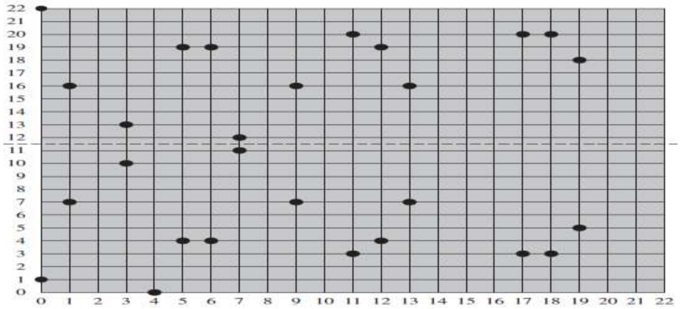


Figure 6:The Elliptic Curve E23(1, 1)

It can be shown that a finite abelian group can be defined based on the set Ep(a, b) provided that (x3 + ax + b) mod p has no repeated factors. This is equivalent to the condition

$(4a^3 + 27b^2) \bmod p \neq 0 \bmod p$ **(10.2).**

The rules for addition over E*p*(*a*, *b*) , correspond to the algebraic technique described for elliptic curves defined over real numbers. For all points *P*, *Q* _ E*p*(*a*, *b*) :

1- $P + O = P$

2- If $P = (xP, yP)$, then $P + (xP,-yP) = O$. The point $(xP,-yP)$ is the negative Of P , denoted as $-P$. For example $E23(1, 1)$, in , for $P = (13, 7)$, we have $-P = (13, -7)$.
But -7 mod 23 = 16 . Therefore, $-P = (13,16)$, which is also In $E23(1, 1)$
.

3- If $P = (xp, yp)$ and $Q = (xQ, yQ)$ with P Z $-Q$,then $R = P + Q = (xR, yR)$ is determined by the following rules:
$xR = (l2 - xP - xQ) \bmod p$
$yR = (l(xP - xR) - yP) \bmod p$
where

$$\lambda = \begin{cases} \left(\dfrac{y_Q - y_P}{x_Q - x_P}\right) \bmod p & \text{if } P \neq Q \\ \left(\dfrac{3x_P^2 + a}{2y_P}\right) \bmod p & \text{if } P = Q \end{cases}$$

4- Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.
For example, let $P = (3, 10)$ and $Q = (9, 7)$ in $E23(1, 1)$. Then

$$\lambda = \left(\frac{7 - 10}{9 - 3}\right) \bmod 23 = \left(\frac{-3}{6}\right) \bmod 23 = \left(\frac{-1}{2}\right) \bmod 23 = 11$$

$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$

$$y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$$

So $P + Q = (17, 20)$. To find $2P$,

$$\lambda = \left(\frac{3(3^2) + 1}{2 \times 10}\right) \bmod 23 = \left(\frac{5}{20}\right) \bmod 23 = \left(\frac{1}{4}\right) \bmod 23 = 6$$

$xR = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$

yR = (6(3 - 7) - 10) mod 23 = (-34) mod 23 = 12

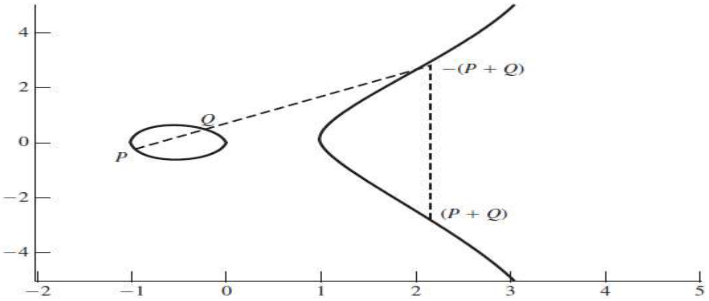


Figure 7: Geometric description of the addition of two points

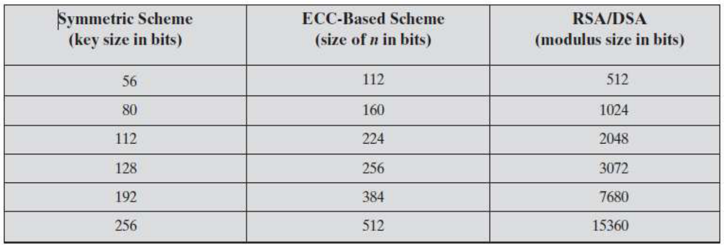
Elliptic Curve Cryptography

The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of modular exponentiation. To form a cryptographic system using elliptic curves, we need to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm. Consider the equation *Q* = *kP* where *Q P* _ *EP*(*a*, *b*) , and k 6 *p* . It is relatively easy to calculate *Q* given and *P* , but it is relatively hard to determine given *Q* and *P* .This is called the discrete logarithm problem for elliptic curves. We give an example taken from the Certicom Web site (www.certicom.com).Consider the group E23(9,17) . This is the group defined by the equation y^2 mod 23 = (*x*3 + 9*x* + 17) mod 23. What is the discrete logarithm *k* of *Q* = (4, 5) to the base *P* = (16, 5) ? The brute-force method is to compute multiples of P until is found *T*hus,

P = (16, 5); 2*P* = (20, 20); 3*P* = (14, 14); 4*P* = (19, 20); 5*P* = (13, 10);6*P* = 17, 32; 7*P* = 18, 72; 8*P* = (12, 17); 9*P* = (4, 5). Because 9*P* = (4, 5) = *Q* , the discrete logarithm to the base *Q* = (4, 5) is *k* = 9 . In a real application, k would be so large as to make the bruteforce approach infeasible. In the remainder of this section, we show two approaches to ECC that give the flavor of this technique.

Security of Elliptic Curve Cryptography

The security of ECC depends on how difficult it is to determine k given kP and P. This is referred to as the elliptic curve logarithm problem. The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method. 10.3 compares various algorithms by showing comparable key sizes in terms of computational effort for cryptanalysis. As can be seen, a considerably smaller key size can be used for ECC compared to RSA. Furthermore, for equal key lengths, the computational effort required for ECC and RSA is comparable [JURI97]. Thus, there is a computational advantage to using ECC with a shorter key length than a comparably secure RSA.



Symmetric Scheme (key size in bits)	ECC-Based Scheme (size of *n* in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Figure 8:Comparable Key Sizes in Terms of Computational Effort for Cryptanalysis, Source =certicom

5. CONCLUSION

Increasing vehicular cloud computing usage, the significance of security in this area is also increasing, providing security in a vehicular network is more difficult than in other network due to open communication, high mobility and wide range of vehicles. Therefore, there are various security issues that threaten the security of vehicular cloud computing and the one of the challenges task is to provide message authentication in VCC. The network has always the possibility of attacks that leads to misguiding users, message forgery, modification, and extortion by man-in-the-middle attacks, wrong information sharing are possible due to the open communication nature. In the proposed work, the main aim is to provide a message authentication in vehicular cloud using the proposed VC-MASF.The proposed VC-MASF is also aim to detect malicious vehicles in the network and maintain trust between the vehicles and the cloud enviroment.

6. REFERENCES

[1] *Chenxi Zhang.“On Achieving Secure Message Authentication for Vehicular Communications ,thesis requirement for the degree of Doctor of Philosophy in Electrical and Computer Engineering Waterloo, Ontario, Canada, 2010.*

[2] *Saif Al-Sultan, Moath M.Al-Doori,AliH.Al-Bayatti,HussienZedan.“ A comprehensive survey on vehicular Ad Hoc network, Journal of Network and Computer Applications, 2013*

[3] *Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen ·Angela Irwin · Aamir Hassan.“Vehicular ad hoc networks (VANETS): status, results, and challenges, Springer Science+Business Media, LLC 2010.*

[4] *Uzma Khana, Shikha Agrawal , Sanjay Silakari.“ Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks, International Conference on Information and Communication Technologies (ICICT 2014).*

[5] *P. Papadimitratos, V. Gligor , J-P. Hubaux.“ Securing Vehicular Communications - Assumptions,Requirements, and Principles".*

[6]*Ms. RajbhojSupriya K, Dr..S.V.Gumaste.“Security Challenges Addressed in Vehicular cloud computing“,International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015.*

[7] *Ms. Ashwini Abhale, Mr. Sumit Khandelwal., Prof. Uma Nagaraj “Shifting VANET to Cloud - Survey.",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013 ISSN: 2277 128X*

[8] *Saurabh Dey , Srinivas Sampalli , Qiang Ye “A Light-weight Authentication Scheme Based on Message Digest and Location for Cloud Computing".*

[9] *Mohammad Saiful Islam Mamun , Atsuko Miyaji ,Hiroaki Takada “A multi-purpose Group Signature for Vehicular Network Security".,2014 International Conference on Network-Based Information Systems.*

[10] *Manish Kumar Sharma , Rasmeet S. Bali , Arvinder Kaur “Dyanimc Key based Authentication Scheme for Vehicular Cloud Computing".,2015 International Conference on Green Computing and Internet of Things (ICGCIoT).*

[11] *P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya*

Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux ,"Secure Vehicular Communication Systems: Design and Architecture ",arXiv:0912.5391v1 [cs.CR] 30 Dec 2009.

[12] *Md Whaiduzzaman, MehdiSookhak, AbdullahGani, RajkumarBuyya," A survey on vehicular cloud computing ",* Journal ofNetworkandComputerApplications40(2014)325–344.

[13] *Kamran Zaidi, Muttukrishnan Rajarajan "* Vehicular Internet: Security & Privacy Challenges and Opportunities, Future Internet 2015, ISSN 1999-5903 ,www.mdpi.com/journal/futureinternet

[14] Douglas R. Stingson, "Cryptography: Theory and Practice, third edition," CRC Press, 2005.

[15] Sneha Charjan,D.H.Kulkarni "Quantum Key Distribution by Exploitation Public Key Cryptography (ECC) In Resource Constrained Devices, "International Journal of Emerging Engineering Research and Technology ,Volume 3,Issue 7,2015.

[16] William Stallinds "CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE" ,FIFTH EDITION.

[17] N. Koblitz, A Course in Number Theory and Cryptography, 2nd edition, Springer-Verlag,1994.

[18] Don B. Johnson, Alfred J. Menezes, Elliptic Curve DSA (ECDSA): An Enhanced DSA