iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VI **Month of publication:** June 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.53739

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VI Jun 2023- Available at www.ijraset.com*

# VANETs Security Using Cryptography

Reema Sandhu
*Assistant Professor, Government College, Naraingarh*

***Abstract:*** ***The usage of Vehicular Ad-hoc Networks, often known as VANET, is becoming more common as the frequency of accidents in the modern world continues to rise. In situations like these, VANET makes accessible a broad variety of protective applications that may shield people from injury while they are operating motor vehicles. These applications can be used to prevent accidents. Additionally, it lessens the amount of collisions that take place, which in turn lessens the amount of damage that is sustained by cars, drivers, and passengers. By giving information to drivers about the flow of traffic along congested roads, VANETs make it possible for drivers to make better use of the time they have available. On the other hand, two security issues that are tied to the safety of drivers are the protection of an individual's right to privacy about their location and the maintenance of identifying information inside the network. Both of these issues are connected to the network. Many protocols need an infrastructure that enables the efficient distribution of keys, the revocation of keys, and the protection of sensitive communications by utilising a number of different cryptographic techniques in order to defend themselves against a wide variety of attacks and to guarantee that driver privacy is maintained. This is necessary in order to ensure that driver privacy is maintained. It is necessary to do extra work in the fields of computers and communication in order to implement a number of the security methods that are used for encrypting and authenticating V2V and V2I communications. These methods may be found in a variety of places. Because of this, it is essential to carry out research into a broad range of different cryptography-based approaches in order to boost the viability of various cryptography-based protocols and to improve the overall performance of these protocols. Because of the high mobility of nodes in the network, a suitable cryptographic technique is necessary. This method must be able to create short keys and short messages, take a little amount of processing time, and have a sufficient degree of security throughout the length of a key.***

***Keywords: Encryption, Elliptic Curve Cryptosystem, Elliptic Curve Digital Signature, MD5, RSA, DSA.***

## I. INTRODUCTION

The encryption of personally identifiable information is an important development in the area of VANETs that has the potential to assist in the prevention of collisions and the enhancement of the general state of traffic, which may ultimately result in the saving of lives. Encryption is the only method that can guarantee the data's safety as a consequence. The authentication process, which must be based on cryptographic procedures, must be carried out since doing so builds confidence between the user and the supplier of the service. There are three different kinds of authentication methods: ones that rely on signatures, ones that rely on verification, and ones that rely on encryption. After being delivered to the RSU for verification-based authentication, the CA verifies the identify of the vehicle using the information it received. When a vehicle connects to or is within the coverage area of a particular RSU, the RSU will carry out an examination of the vehicle in order to validate the identification that has been validated by the CA. The message in the digital signature is encrypted using the sender's private key, and the recipient's public key is used to decode the message once it has been sent. This painstaking approach ensures that the message will be kept confidential [1]. [Note: In order for digital certificates to function properly, it is necessary for one party to transmit a copy of their certificate to another party, who will then send the copy to the authority that issued the certificate. During the verification procedure, a recipient's public key is used in order to confirm the signature of the entity that is doing the sending. Mathematically speaking, digital signatures and certificates are mathematically equal since they both employ the same public key. One kind of encryption is known as reversible encryption, while the other is known as irreversible encryption. These are the two main categories of approaches that have been suggested so far. When referring to the process of encrypting a communication, the term "reversible encryption" refers to the capability of decrypting the message in order to retrieve the plaintext from the ciphertext. If you decide to use an encryption method that is irreversible, the message cannot be read until it has been first decoded (cipher text). Cryptography and encryption, two of the most basic security technologies, are used to preserve the confidentiality of data sent through vehicle communications. The use of an appropriate cryptographic algorithm is necessary for VANETs [2]. Regular, easily comprehended English may be converted into indecipherable text with the use of cryptography, and vice versa. It is a method of transmitting and receiving information in a particular format that can be read and comprehended only by the individuals who are supposed to receive it.

In addition to protecting data against unauthorised access and alteration, it may also be used for authenticating users, which is a useful feature in its own right. The plaintext is first encrypted at the sender's end using keys, and then it is decoded at the receiver's end using those same keys. This approach is seen in Figure 1.

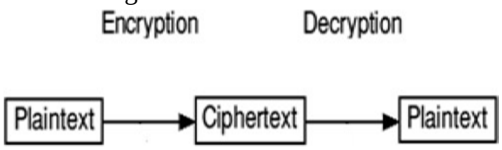



Figure 1: Encryption process

In general, several different kinds of cryptographic approaches are used [3].

*A. Symmetric Cryptography*

Those who have the key are the only ones who are able to decode the encrypted file and see the information that is stored inside it. The private key need to be guarded closely because of the fact that it may serve both as an encryption and decryption device. A successful symmetric technique for the transmission of data is one that ensures the confidentiality, availability, and integrity of the data that is being delivered.

*B. Asymmetric Cryptography*

In an asymmetric method, one key is used for the encrypting process, while the other key is put to use during the decrypting procedure. Nevertheless, there is a possibility that the two keys are, in fact, related to one another in some kind. To phrase it another way, the general population is aware of what the key is. The person who was the one to produce the private key in the first place is the one who is responsible for ensuring its safety. The approach, which is also known as public key cryptography, is one that involves a significant amount of math and is, as a result, one that takes much more time to complete than the symmetric method. Both sides of this key have been given a cutting. For data that has been encrypted using a public key, the matching private key is required in order to decode the information. By utilising a digital signature to authenticate the sender and make sure that the message was not tampered with while it was in transit, asymmetric approaches provide not only integrity, availability, and secrecy but also authenticity and non-repudiation. These benefits are in addition to the benefits that are provided by integrity, availability, and non-repudiation. Because of this, it is impossible to disprove the message's accuracy. Asymmetry is essential so that digital signatures may be utilised in either way without being rendered invalid.

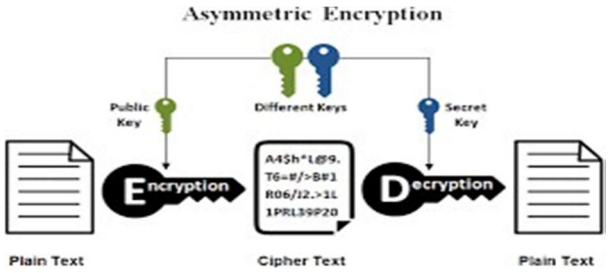



Figure 3: Asymmetric Key Encryption

As can be seen in Figure 3, asymmetric cryptography is distinguished by "the deployment of distinct encryption and decoding keys." [Citation needed] The Digital Signature Method (DSM), Rivest Shamir-Adleman (RSA), Diffie-Hellman (DHA), and Elliptic Curve Digital Signature Algorithm are examples of well-known asymmetric algorithms (ECDSA). RSA and ECDSA are both popular choices when it comes to using asymmetric encryption algorithms [4].

## II. RELATED WORK

For the aim of ensuring the security of VANETs, the IEEE 1609.2 standard suggests implementing an asymmetric Public Key Infrastructure that is digitally signed with an Elliptic Curve Digital Signature Algorithm (PKI/ECDSA). It may take more time and effort to analyse this information, which means that any necessary safety alerts may be postponed for a longer period of time. Given this circumstance, the use of symmetric cryptographic systems is strongly recommended. During the process of coming up with trust grouping tactics, the surrounding cars are taken into consideration as well. [5]

In order to solve the problems that arise with authentication, Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri foresaw the development of a technique known as Short-lived Key Management. Yong Hao developed a distributed key management architecture for cooperative message authentication in VANET [6] as a solution to the prohibitive computational cost of the group signature implementation. The creators of [7,8] envisioned CPPA approaches that depended on PKI and made use of public-private key pairs as well as associated certificates in order to safeguard the identity of the vehicle. [Click Here] Henry David Edward Moreno [9] proposed a solution for the VANET network that would assure the safe transit of communications by encrypting data in a variety of ways, some of which included RSA, ECC, and MQQ. This solution was intended to be implemented. Uzma Khan and colleagues [10] presented a comprehensive investigation of previously unknown malicious nodes and a variety of cryptographic strategies that may be used to protect against the damage that could be caused by these nodes. Digital signatures are becoming more recognised as a trustworthy technique of authenticating communications and transferring information. After that length of time had passed, R. Rivest came up with the idea of using the MD5 algorithm to solve the problem of data encryption [11]. In Wagen's [12] proposal for a hybrid solution, which utilises asymmetric and symmetric cryptographic algorithms, as well as hardware that comprises both symmetric and asymmetric cryptography modules, the authors sought to strike a balance between performance and security. This method combines symmetric and asymmetric cryptographic algorithms in order to strike a balance between the need for security and the need for usability.

## III. METHODS

### *A. Symmetric Methods*

#### *1) Hash Algorithms*

As input, it accepts a message of any length, and as output, it outputs something known as the message digest, which is constrained to a certain length. Hashing is done primarily for the purpose of comparing the digest of the data that was initially saved with the digest of the data that is currently stored in its current form. This is the main aim of hashing. It provides a digital digest that may be used in order to identify whether or not the contents of a message or programme have been changed in any way. The basic objective of a hash function is to produce a one-of-a-kind digital fingerprint. This fingerprint may then be used to verify that the data included in a message or programme has not been altered while it was being sent. It is used to assess whether or not an adversary was successful in adding a malicious piece of code, which is frequently referred to as a software virus. This may be done by analysing the code. A method called a one-way hash, which does not encrypt or decode the data, may be used to rebuild the original data set so that it can be used again. The original digest and the digest of the current state should be very similar to one another if the data are safe to use. MD5 and the SHA family are only two examples of the many different hashing algorithms that are used in today's computing world. The hashing method is a one-way approach that not only assures the data's integrity but also limits the transmission of viruses [4] when it is utilised effectively. This is because the hashing method is a one-way technique.

#### *2) Message Authentication Code (MAC)*

Using the MAC protocol, malicious nodes in a network are stopped from broadcasting unauthorised and altered messages in order to prevent a chain reaction that might lead to a traffic accident. A message and a hidden key are required in order to do this task. Using the secret key, the recipient of the message validates both the authenticity of the message as well as the sender's claim to ownership of the shared secret key. If the sender's secret key and the recipient's secret key are different, then the hash value will be different as well. This leads one to believe that the communication was not delivered by a different sender than the one who initially sent it. Because of this, the message is authenticated by utilising the message authentication code (MAC), and the use of RSUs makes it possible to finish the verification process in a timely manner. You may choose from the following four major types of MACs:

*a)* Hash-function based,
*b)* Stream cypher based,
*c)* Block cypher based, and unconditionally secure using
*d)* Block cyphers and hash functions.

Hash-based MACs, also known as HMACs, are currently the most used approach for producing MACs. HMACs include the utilisation of a secret key in order to get a hash value. In the past, the most common approach of generate MACs was via the use of block cyphers. HMAC has the potential to concurrently guarantee both the integrity of the data and the user's authentication [4].

*3) TELSA*

The TELSA secure source authentication system, which was first created by Adrian Perrig and his colleagues and was subsequently used for multicasting and broadcasting, was one of the earliest systems of its kind. The protection of sensitive data is accomplished by the use of symmetric key cryptography with postponed key disclosure. It is feasible for VANET to minimise delays that are caused by signature delays since symmetric key encryption is substantially speedier than asymmetric key encryption. The receiver will keep the information that was supplied by the source in storage until the associated key can be decrypted. TESLA is having trouble with non-repudiation despite the fact that it does not need any faith between receivers and also uses low-cost operations. This is due to the fact that TESLA uses low-cost operations. In addition, the time synchronisation that occurs between the various nodes of the TESLA network is only partially correct. [13].

*B. Asymmetric Methods*

*1) Public Key Infrastructure*

Encryption and decryption are both accomplished with the use of a PKI's public and private keys. In many different PKI-based systems, there is a need for a Certificate Authority, often known as a CA, to act as a reliable third party. There is a connection made between the broadcasts that are sent out by each vehicle and the signatures and public-key certificates that are connected to them. When encrypting anything, the recipient's public key is the one that is utilised. The sending of a message will be halted until a digital signature and certificate have been appended, which will lead to an increase in the expenses associated with communication. Automobiles and the Public Key Infrastructure (PKI) both need anonymous public keys in order to protect users' identities and maintain their conditional anonymity. To put it another way, the process of certificate revocation and other problems related to certificate management could have a significant influence on PKI. There is an issue with the present implementations of PKI in VANET security because they utilise a lot of delay and a sophisticated computing process to validate the validity and authenticity of cars [14]. This creates a problem for the security of the VANET. The Public Key Infrastructure (PKI) is a procedure that is both time-consuming and computationally complex, which contributes to this inefficiency.

## IV. ALGORITHMS

*A. Symmetric Key Algorithms*

*1) AES*

It is a symmetric block encryption approach with a block size of 128 bits, and it is sometimes referred to by its original name, which is the Rijndael algorithm. It uses different keys with lengths of 128, 192, and 256 bits to encrypt each of these distinct blocks. After each of these blocks has been encrypted, the ciphertext is created by combining all of the encrypted blocks together. It is built on a substitution-permutation network, often known as an SP network, which incorporates input-to-output replacements for certain substitutions and bit shuffles for some permutations [5]. An SP network may also be referred to by its alternative name, the substitution-permutation network.

*2) Features of AES*

- SP Network: It operates using a structure that is based on an SP network
- Key Expansion: During the initial stage, it just uses one key, but later on, it expands to utilise numerous keys for each each round.
- Operation on Byte Data: Because the AES encryption algorithm operates on byte data, it interprets the 128-bit block size as 16 bytes while it is carrying out the encryption process.
- Key Length: The number of rounds that need to be completed is determined by the length of the key that is being used to encrypt the data. There are 10 rounds for a key size that has 128 bits, 12 rounds for a key size that has 192 bits, and 14 rounds for a key size that has 256 bits.

*3) DES*

The Data Encryption Standard, more often referred to as DES, is a symmetric-key block cypher that makes use of a Feistel structure that has 16 rounds. An implementation of a Feistel Cipher can be seen here. This implementation of a Feistel Cipher is an implementation of a Feistel Cipher. Despite the fact that DES uses 64 bits for each block, the effective key length of the algorithm is just 56 bits long. This is due to the fact that eight of the key's sixty-four bits have been set aside specifically for use as check bits. The Data Encryption Standard (DES) is susceptible to a broad range of attacks since it encrypts plaintext using a key that is 56 bits long. These attacks may be carried out with the help of modern technology. Because of this, double DES and triple DES were

invented; each of them uses a key that is either 112- or 168-bits long, and as a consequence, they provide a far better degree of protection than DES [15].

*4) Double DES*

The encryption technique known as Double DES makes use of two distinct instances of DES, each of which has a key size of 112 bits, and applies them both to the same plain text in order to create an encrypted version. Both times, the keys that were used to encrypt the data were different, and in order to decode the data, it was essential to have both of the keys accessible. First, a plain text that is 64 bits in length is fed into the first DES instance, and then, using the first key, the plain text is changed into a 64-bit version of the middle text. Following this step, the 64-bit middle text is fed into the second instance of DES, where it is transformed into 64-bit cypher text by making use of the second key. the second significant piece of evidence. However, double DES uses a key that is 112 bits long, but the amount of security it provides is only 256 rather than 2112 due to the fact that double DES can be circumvented using a meet-in-the-middle attack [15]. Although double DES uses a key that is 112 bits long, the amount of security it provides is only 256 rather than 2112.

*5) Triple DES*

A form of encryption known as Triple DES involves using three distinct iterations of the Data Encryption Standard (DES) algorithm on the same plaintext. In order to choose the key combination that should be used, it makes use of three separate methods. The length of the key is 168 bits long. There are 168 bits in total. In the first situation, each of the employed keys is one-of-a-kind. In the second scenario, on the other hand, two of the keys are the same and one of the keys is one-of-a-kind. In the third scenario, every single key is the same as the one before it. This encryption technique delivers a total security level of 2112 while only using 168 bits of key due to the fact that Triple DES may also be attacked by a meet-in-the-middle attack. Because of the small size of the blocks, there is a greater potential for collision assaults, as well as a greater potential for sweet32 attacks [15].

*6) IDEA*

The International Data Encryption Algorithm, which is sometimes referred to as IDEA, is a block cypher that is both publicly available and completely free to implement. It is designed to serve as a replacement for the Data Encryption Standard (DES). A block is considered to be the conventional size of 16 bytes, which is equivalent to 128 bits. It is executed on 64-bit blocks by using a key that is 128 bits in length, and it is composed of a succession of 8 rounds. The functioning of a block cypher will typically take place in rounds the vast majority of the time. Following the application of some of the key to the round in the first step, more procedures will be performed on the data in the following steps. The ciphertext for the block is formed after ten to sixteen rounds, and the size of the ciphertext exactly matches that of the plain text block. The round key is a component of the encryption key that is used by the round's own one-of-a-kind block, which is a part of the encryption key. The use of a key scheduling method allows for the development of a number of round keys, with the employment of an encryption key serving as the point of origin for the process. In order to generate the round keys, this technique performs many operations, including XOR and multiplication, on the original encryption key. These are the only two examples. [6]

*7) RC4*

RC4 is an abbreviation that stands for Rivest Cipher 4, which was first developed by Ron Rivest in 1987 for RSA Security. These cyphers are known as variable-key-size stream cyphers, and their operation consists on traversing a stream of data byte by byte in order to decipher it. It is one of the stream cyphers that is used the most often owing to the simplicity with which it can be implemented and the quickness with which it performs. It uses a key size of either 64 bits or 128 bits, depending on your preference. Software applications such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and the IEEE 802.11 standard for wireless LAN all make use of it [10].

Encryption Process

- After receiving a plain text file and a secret key from the user, the encryption engine will proceed to produce the keystream with the assistance of the KSA and PRGA Algorithms.
- The plain text is now byte-by-byte combined with this keystream using XOR, and the result is the encrypted text.
- The material that has been encrypted is then delivered to the person who is supposed to receive it; this person will subsequently decode the text in order to get the original plain text.

*8) RC5*

The symmetric key algorithm known as RC5 was first conceived of by Ron Rivest, who is also credited with its invention. This method, which makes use of just the most basic of computer operations and can be executed with a reduced amount of RAM, is particularly effective. It offers a changeable number of rounds as well as a variable bit size key so that flexibility may be introduced. [Case in point:] [Case in point:] [Case in point:] When using the RC5 technique, it is the user's responsibility to provide a plain text block size, the number of rounds, and 8 bits of the variable length key. When the parameters have been chosen, they will not be altered for any particular implementation of the cryptographic technique that is used. A block of plain text may be 32 bits, 64 bits, or 138 bits in size. These are the three potential options for the size of the block. There is no upper limit on the number of bits that can make up the length of the key; it might be anything from 0 to 2040. The length of the plain text and the ciphertext that is created as a consequence of applying the RC5 method is the same. The plain text message that will be encrypted using RC5 is divided into two blocks, each of which consists of 32 bits. The message will then be encrypted. It does this by producing two subkeys, which are then put into the two blocks according to their corresponding positions, therefore forming two new blocks. This, in turn, closes off the one-time operation and brings it to an end. After then, the method of the rounds begins. During each round of the procedure, several operations, including bitwise XOR, left circular shift, and addition to the succeeding subkey, are carried out for the freshly built blocks. For example, [10].

*B. Asymmetric Key Algorithms*

*1) Diffie-Hellman Algorithm*

1976 was the year that Whitfield Diffie and Martin Hellman worked together to develop a first-of-its-kind practical method for exchanging information over an unsecured channel. This collaboration led to the creation of the first public key algorithm, which was then patented in the same year it was developed. [16] It is a protocol for exchanging keys that lets two parties to construct a mutual secret while chatting over a public channel. The protocol was developed by the National Security Agency (NSA). The completion of this task does not require the transmission of any data over the internet. It is a pair of public and private keys that uses the ElGamal algorithm and is analogous to the RSA method. Due to the fact that one can only do back calculations in a logarithmic fashion, this provides an extremely high level of security and makes it very difficult to breach. The steps that go into the creation of this algorithm are listed in the following order: -

*a)* The first party selects two prime numbers, g and p, and then communicates those numbers to the second party.
*b)* The second party chooses a secret number, which we'll refer to as a, and then computes ga mod p before sending the result back to the first party, which we'll refer to as A. Nobody receives the confidential number; only the result is sent to anybody else.
*c)* Following this, the first party chooses a hidden number b and then calculates the result B, which is then sent to the second party.
*d)* The second party is given the number B, and they compute the number B modified by p and v.
*e)* In a similar manner, the first party is given the number A and is responsible for computing Ab mod p.

If the solution to step 5 is the same as the solution to step 4, this indicates that the two individuals will arrive at the same conclusion regardless of the sequence in which they multiply their exponents.

$(g^a \ mod \ p)^b \ mod \ p = g^{ab} \ mod \ p$

$(g^b \ mod \ p)^a \ mod \ p = g^{ba} \ mod \ p$

The results that are acquired after steps 4 and 5 will be taken as the shared secret key, and it will be used to encrypt any data that is going to be transferred [16].

*2) ECDSA*

Verifying digital signatures generated using elliptic curve cryptography requires the use of an algorithm known as the Elliptic Curve Digital Signature Algorithm (ECDSA), which is recommended by the current IEEE1609.2 standards for secure VANET communications. ECDSA, which offers network security by applying a digital signature for messages broadcast over the network, has been included into a few of the suggested methods for VANET authentication. These methods are intended to improve network safety. These are the many strategies that have been proposed up to this point. The effectiveness of the authentication process is negatively impacted as a result of the inclusion of ECDSA, since a number of studies have shown that this results in an ongoing increase in the cost of computation. Because of this, the verification process takes longer, and the performance of the authentication systems in VANET suffers as a direct consequence [17].

*3) RSA (Ron Rivest, Adi Shamir and Leonard Adelman)*

The RSA technique makes use of two asymmetric keys, only one of which is made publically available while the other is kept a closely guarded secret. The public key is a key that may be released to anybody and is used for the purpose of encrypting communications. It is also known as the universal key. Messages that have been encrypted using the public key may be decoded with the assistance of the private key if the private key is known. The difficulty of factoring a very large number into two or more parts is one of the determining factors in determining whether or not an RSA cryptographic technique will be successful. The size of the key defines how difficult it will be to factor the numbers, and the larger the size of the key, the more complex factoring the integers will be. The steps that are detailed below make up the procedure that is followed in order to generate the keys for the RSA algorithm [18]:

*a)* At random, choose two separate prime integers p and q that have bitlengths that are comparable.

*b)* Perform the calculation n = p q, where n serves as the modulus for both the public key and the private key, and the length of its representation, which will be stated in bits and referred to as the key length.

*c)* To get the totient function of n, compute (n) = (p)(q), which is equal to (p 1) (q 1) = n - (p + q -1), where is Euler's function. Find an integer e such that 1 e (n) and gcd(e, (n)) = 1; in other words, make sure that e and (n) are both prime numbers. e is the public key exponent, and it has a bitlength that is not very long and Hamming weight results that are not very high. However, in some configurations, it reveals itself to have a lower level of security if the values of e are lower than 3.

*d)* Find d by solving the equation d = d e1 (modulo n); in other words, d is the multiplicative inverse of e (modulo n). This may be expressed more simply as: find d assuming that de is less than one (modified by n) A common method for computing this is known as the extended Euclidean algorithm. When using the pseudocode found in the section under "Modular integers," inputs a and n correspond, respectively, to the values e and (n). The value d is preserved for use as the exponent of the private key.

*e)* The modulus n and/or the encryption exponent e are included inside the public key. It is essential that the modulus n and the decryption exponent d be kept a secret, and the private key includes both of these values. In order for the calculation to be accurate, p, q, and (n) must all be kept a secret.

## V. CONCLUSION

The differences between the several data encryption algorithms that are employed today have been brought to light, and it is now the responsibility of the user to choose the one that is most appropriate for their requirements in light of the conditions that now exist. It has been shown that the probability of a collision is reduced according to the size of the key, and as a consequence, the method will be more foolproof if the key is of a greater size. Even though symmetric is much quicker and needs less computation power than asymmetric, the latter is still being used widely because it is more secure and offers encryption, authentication, and non-repudiation [18]. Even though symmetric is much quicker and requires less computation power than asymmetric, it is still being used widely because of these benefits. The reason why asymmetric is still more popular is because it provides a higher level of safety, despite the fact that symmetric is far more efficient and requires considerably less computational resources. The hybrid encryption method is used in SSL/TLS certificates, and it is utilised during "TLS handshakes," which are exchanges of information that take place between servers and web browsers. During these handshakes, the identities of both parties are checked using the private key and the public key, respectively, to ensure that they are who they claim to be. Following that, the data are hidden from prying eyes by using symmetric encryption with the assistance of a session key, which enables the most efficient data transmission that is possibly conceivable. At this time, more group encryption key-management systems for VANETs are being developed and are now in the process of being developed. between the nodes as a result of the use of the major management techniques It is used in applications that need a high level of security, such as those used by the police and the government, both of which are examples of locations where the use of VANETs has become increasingly widespread. The protection against data being altered and the safeguarding against it being created against a variety of threats, which can be achieved by using a variety of encryption techniques [19]. [Citation needed] The protection against data being altered and the safeguarding against it being created against a variety of threats.

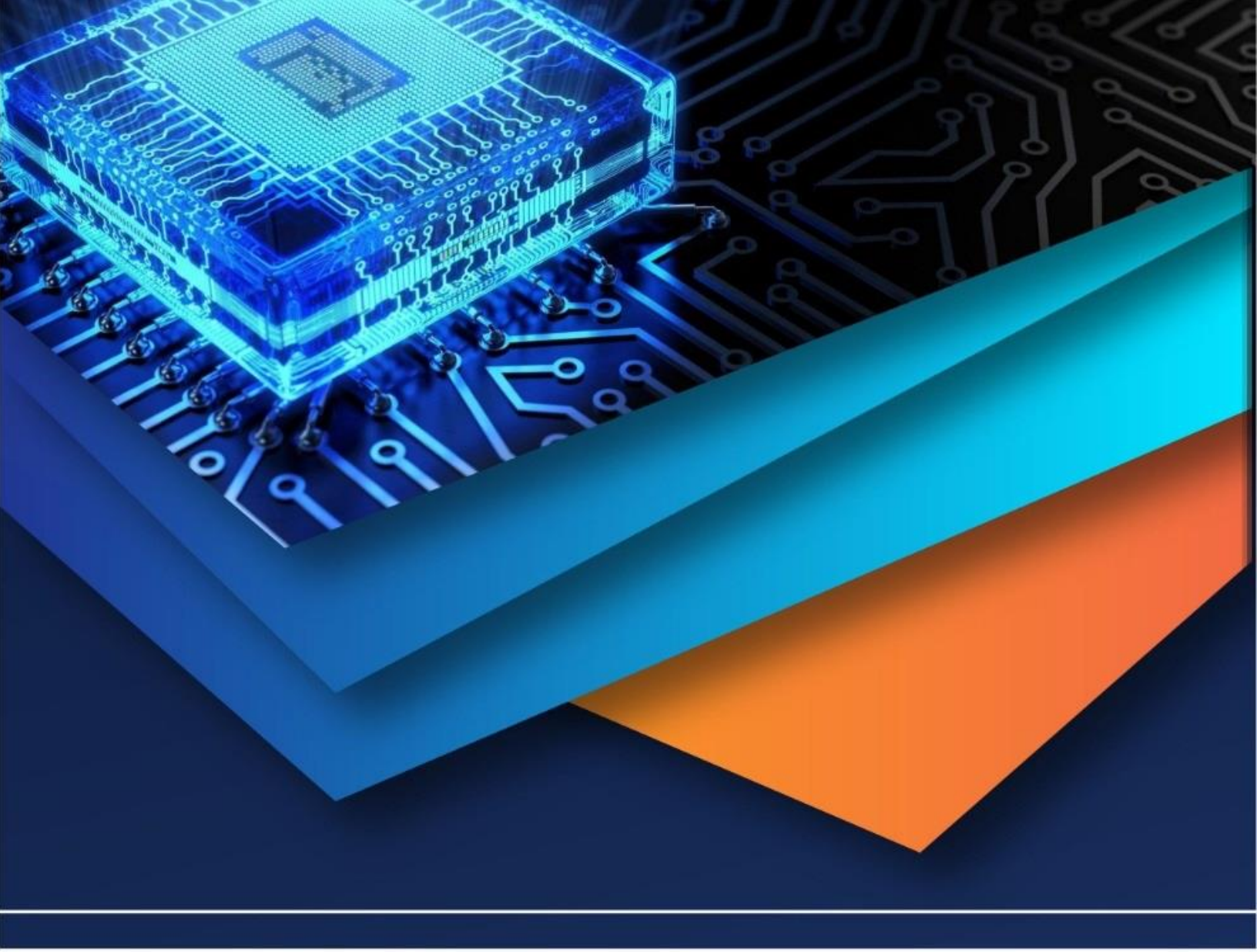
## REFERENCES

[1] T.W. Chim, S.M. Yiu, Lucas C.K. Hui, “VSPN: VANET-Based Secure and Privacy-Preserving Navigation “in Transactions On Computers (IEEE, February 2014 Vol. 63, No. 2 ).

[2] Greeshma TP, Roshini TV “A review on privacy preserving authentication in VANETs” in International conference on control, power, communication and computing technologies (ICCPCCT), (IEEE, Departmentof Electronics and Communication, Vimal Jyothi Engineering College, Kannur ,2018).

[3] M. Ali Mohammadi, and A. A. Pouyan, “Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET”, in International Journal of Scientific & Engineering Research, Feburary 2014 Volume 5, Issue 2

[4] Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc, and Song Hand "A Survey of RFID Authentication Protocols Based on Hash-Chain Method" (State Polytechnic of Ujung Pandang, Indonesia DEBI Institute, Curtin University of Technology, Australia, 2008).
[5] Stefano Busanelli, Gianluigi Ferrari and Luca Veltri "Short-lived Key Management for Secure Communications in VANETs " in Wireless Ad hoc and Sensor Networks (WASN) Laboratory (Department of Information Engineering, University of Parma, Italy, 2011).
[6] Yong Hao, Yu Cheng, Chi Zhou, Wei Song, Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro , "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs" (IEEE, MARCH 2011)
[7] Raya M, Hubaux JP "Securing vehicular ad hoc networks" in Journal of Computer Security, 2015, pp39–68
[8] Lin X, Lu R, Zhang C, Zhu H, Ho PH, Shen X "Security in vehicular ad hoc networks (IEEE Communication,2008) pp 88–95
[9] Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro "Impact of Asymmetric Encryption Algorithms in a VANET" (DCOMP/UFS, Universidade Federal de Sergipe, Aracaju/SE-Brasil,2015)
[10] R. Engoulou, "Securisation des vanets par reputation des noeuds ", thesis report, Ecole Polytechnique de Montreal, 2013.
[11] R. Rivest, "The MD5 Message-Digest Algorithm," (RFC 1321, 1992).
[12] Wagan Chowdhury, P.Tornatore, M.Sarkar, S.Mukherjee, B.Wagan, AA Mughal, B.M Hasbullah "VANET Security Framework for Trusted Grouping Using TPM Hardware," in Communication Software and Networks, 2010.
[13] http://cdn.intechopen.com/pdfs-m/12879.pdf
[14] https://www.tutorialspoint.com/cryptography/images/public_key_cryptography.jpg
[15] Venkatamangarao Nampally , Dr. M. Raghavender Sharma , Dr. K. R. Balaji, "Traditional Data Encryption Methods for VANET", in International Journal Of Advance Scientific Research And Engineering Trends, 2017
[16] https://www.hypr.com/diffie-hellman-algorithim/
[17] T.Punitha ,M.Sindhu , "Pairing Based Elliptic Curve Cryptosystem for Message Authentication ",in International Journal For Trends In Engineering & Technology , March 2015 ) pp 87-90.
[18] Karamjeet Singh, Chakshu Goel , "Using MD5 AND RSA Algorithm Improve Security in MANETs Systems", in International Journal of Advances in Science and Technology , June 2014
[19] Saad Ali Alfadhli , Songfeng Lu, Abdulaziz Fatani, Haider Al-Fedhly and Mahmut Ince "SD2PA: a fully safe driving and privacy-preserving authentication scheme for VANETs" ( Human-centric Computing and Information Sciences , 2020)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY