Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 01, pp.64465-64472, January, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

ENHANCING THE SECURITY AND DATA TRANSMISSION TIME IN VANET'S CLOUD

[1]Saddam Hussain Shaik, [2,*]Rama Krishna Reddy Guduru and [3]Aurelijus Domeika

[1]Department of Mechanical Engineering, Lovely Professional University, Phagwara, Punjab, India
[2,3]Institute of Mechatronics, Department of Mechanical Engineering,
Kaunas University of Technology, Kaunas, Lithuania

ARTICLE INFO

Article History:
Received 22nd October, 2017
Received in revised form
09th November, 2017
Accepted 28th December, 2017
Published online 31st January, 2018

Key words:
Cloud VANET,
Encryption,
Decryption,
Data Transition Time.

ABSTRACT

Cloud computing stands asan extensively used technology. The world is associated with the web.The on-request benefits gave by the cloud are a database, network, web servers, email, virtual desktop, client relationship administration, and so on.Due to which the vehicular ad-hoc networks (VANET) are enforced to move from traditional vehicular ad-hoc networks to VANET-Cloud. There are some security issues with a cloud. Numerous cryptographic strategies are intended to defeat these issues.For which the cloud storage is increasing day by day, due to this reason, the time for encrypting and decrypting the data is increasing. VANET's are made to deliver the information timely and precise without conceding the security to fulfill the desired requirement. Any delay in vehicle communication leads to disaster (accidents), traffic jam, etc., to overcome these problems the hybrid technique is proposed by means of elliptic curve cryptography, Diffie-Hellman, and quantum AES. The proposed technique will boost the security and reduce the storage and data transmission time in VANET cloud.

Citation: Saddam Hussain Shaik, Rama Krishna Reddy Guduru and Aurelijus Domeika, 2018. "Enhancing the security and data transmission time in vanet's cloud", *International Journal of Current Research*, 10, (01), 64465-64472.

INTRODUCTION

There is such a hugequantity of mischances occurred out and about by the impact of vehicles because of some minor mix-up. That is the reason Safety applications are a most vital factor to reduce the street mishap and death toll of the inhabitants of vehicles. Vanets helps individuals with life wellbeing and dynamic street security to keep away from crashes by helping the drivers with timely and precisedata (like Car speed cautioning, Traffic flag infringement cautioning, Collision chance cautioning) and with the care of all security. Cloud computing [Peter Mell, 2011; Cloud Computing Bible, 2011; http://www.ibm.com/developerworks/cloud/library/cl-cloudserviesliaas] is booming like no other technology in the market. Cloud hosts many of the services like email, search engines, social networks. Cloud has all features that allow theclient to avoid hardware and software, gain flexibility, complete use of resources and especially client access control. The services and applications that run on the distributed network using virtual resources and can be retrieved by common internet protocols and networking standards. The resources are unlimited and virtual that can be customized according to our demand.

Corresponding author:* **Rama Krishna Reddy Guduru,
Department of Mechanical Engineering, Lovely Professional University, Phagwara, Punjab, India.

The physical frameworks which are really operating the software abstracted from the client. Cloud processing contains deployment and service model, Development model where the cloud is found and for what reason.

There are four types of clouds in the deployment model:

- Private cloud
- Public cloud
- Community cloud
- Hybrid cloud

Features of cloud computing

Cloud computing has various features, some of them are as follows:

- On-demand:
- A Broad network access:
- Resource pooling:
- Measured service
- Lower cost:
- Ease of utilization:
- Low barrier to entry:
- Reliability:

Disadvantage of cloud computing

The major aspects of the cloud which are considered as disadvantages are security and privacy, lack of control [Ajey Singh, 2012; Shikha Singh, 2014], downtime [Gehana Booth, 2013], attack vulnerability to a cloud environment [Ajey Singh, 2012] and cost.

These are some issues to be discussed in brief.

- **Security and Privacy:** Security is a key concern in today's world. All the service providers promote their ideas of having latest security techniques. But as it comes to internet computing that is using online applications and storage, the customers feel insecure to share personal and business data with the third party cloud providers. Many best service providers' offers great authentication techniques to customer test.
- **Lack of Control:** Cloud users have less or we can say limited control over the functions provided by the service provider. They have also a limited control over data and services, but not on the infrastructure at the backend.
- **Downtime:** The downtime of a cloud service leads to a great effecton customer services for example reliability. The service provider must handle enormous rush every time. The access is completely hooked on the internet connection. So sometimes when your server is down, the access to the application goes down.
- **Vulnerability to Attack:** As the information is provided over the internet, an attacker can gain access to online applications by using appropriate methodologies. Even the best service providers can be hacked by the attackers.
- **Cost:** The cost at some small scales the cost can be précised. But at a business level, the cost ends up more than expected. The costs are changing, so it should be checkedregularlyor smartly pay first if you know what amount of data you are going to use.

Cloud attacks and security

The term security refers to provide security to the data available on the cloud. This to maintain the authenticity, integrity, and availability of data. There are some attacks possible on the cloud environment [Ajey Sing, 2012; Shikha Singh et al., 2014; Peter Mell, 2011; Cloud Computing Bible, 2011; http://www.ibm.com/developerworks/cloud/library/cl-cloudserviesliaas.]

Denial of service attack

When the requests to the server exceed the limit of the server then the server goes down, it can be performed by an attacker to reject the user's access or resources from the server the denial of service attack can be more damaging. As per cloud needs, there are numbers of users of the cloud. An attack distributed denial of service attack can be there in a cloud environment.

Cloud malware injection attack

The attempt is to infuse a malicious service or any virtual machine in the cloud.

The specific fill a need for attacker for which it is acquainted with the cloud. The reason might be any similar to information burglary, spying, information modification. This requires the usage of pernicious administration and virtual machine i.e. SaaS, Pass and LaaS separately. The vindictive administration is added to the cloud.

Authentication attack

The authentication is provided in many ways in acloud environment; basically, it is about cryptographical algorithms and revolves around what facts user knows. There is a list of authentication attack and mechanisms .the mechanisms providing authentication to the systems can be attacked if the unauthorized person has advance knowledge of their implementation.

Man-in-middle attack

The attack is performed by anattacker by placing himself within two parties. The aim can be spoofing the information that is being shared among both the parties. The attack can be apassive or active attack.The passive attack will be spoofing the information. On the other side active attack is about modifying or intercepting the information.

Objective of the study

The primary target of this investigation is to upgrade the security, lessen the encryption and decryption time and furthermore decrease the storage volume in Vanet Clouds.Which helps to increase the efficiency by reducing the data transmission time in Vanet clouds.

To achieve the above objectives we have proposed an algorithm based on encryption and decryption using different keys, storage and time took to encrypt and decrypt. The cryptographic algorithms Diffie-hellman, quantum-AES and elliptic curve cryptography is used to achieve the authentication and authorization. Diffie-hellman work as key exchanger between both the parties. Quantum-AES is advanced encryption standard used to treat data as a block for encryption and decryption, Elliptic curve cryptography is used for public key's to compare the keys.

Different cloud authentication schemes

Diffie-Hellman

Diffie-Hellman is the first public key cryptography or symmetric key agreement ever intended, in 1976. Diffie-Hellman permits the sharing of a mystery key between two clients and it is an exponential key understanding. It requires no earlier privileged insights. In Diffie-hellman when two users want to share asecret key, at first, both the parties need to choose two numbers n and p. Let p is an integer and n is a prime number. The setup for the Diffie-hellman algorithm:

Suppose that we have two parties M (Master) and S (Slave), they want to communicate with each other. Both the parties do not want the eavesdropping to know their communication. M and S agree upon and select two numbers n and p, p is primitive root mod n and n is a prime number. Anyone can see these two numbers.

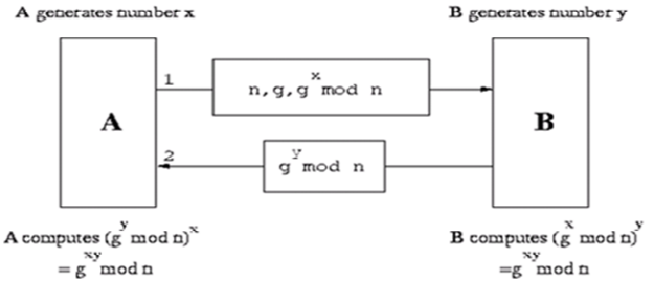

Figure 3.1. Diffie-hellman process

Table 4.1. Private computations

M	S
Choose a secret number a. Compute $X=P^a$ (mod n)	Choose a secret number b. Compute $Y= P^b$ (mod n)

- Public values are exchanged.
- M sends X to S ==X.
- Y ==S sends Y to M.
- M calculates the number $K= Y^a=P^{ab}$ (mod n)
- S calculates the number $K=X^b=P^{ba}$ (mod n)
- Now M and S have same key K.

In Diffie-hellman when two parties want to exchange the data they need to agree on the same key means symmetric key. The symmetric key is used for both encryption and decryption of the messages. The Diffie-Hellman algorithm is used only for exchanging the keys between two parties not for encryption and decryption process.

AES

Modern symmetric-key block algorithm for encrypting the electronic data. AES is an encryption algorithm which replaces the DES. It uses the encryption key and encryption rounds. A block cipher is an encryption algorithm which works on asingle block of the data. AES uses the single key encryption mechanism; it may be 128 bit, 192 bit and 256 bit long. 128-bit key means, it is encryption key length. In AES, encryption and decryption is performed by thesame key, so it is called symmetric encryption algorithm.

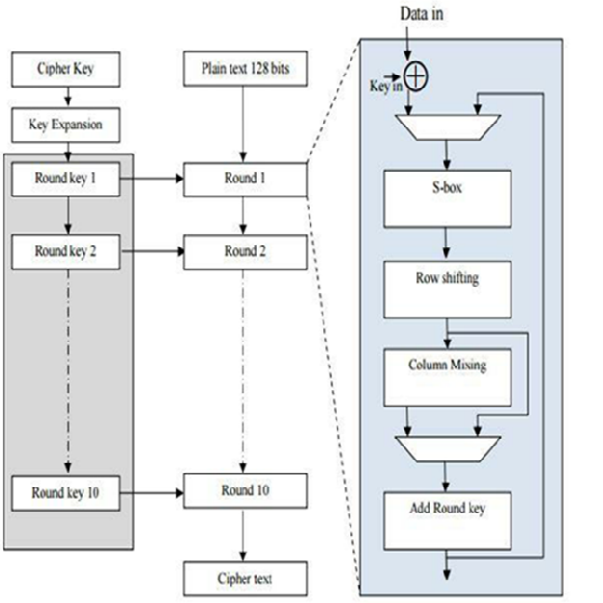

Figure 3.2. AES Flowchart

Different modes of operations in AES:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

Initial version of AES:

There are three versions of AES.

- Advanced Encryption Standard (128-bit)
- Advanced Encryption Standard (192-bit)
- Advanced Encryption Standard (256-bit)

128, 192 and 256 bit is the key length of theencryption process. In anAES-128 bit, thekey is represented in an array 4*4 and it has 10 rounds. In AES-192bit, thekey is represented in an array 4*6 and it has 12 rounds. In anAES-256 bit, thekey is represented in an array 4*8 and it has 14 rounds. Each round has four states except the last round.

The last round in all the version of AES has all the states except mix-column transformation.

- Substitution transformation
- Shift-row transformation
- Mix-column transformation
- Add round key transformation

Substitution transformation replaces each element in an array with S-box values. For example, if anelement in an array is a8 then the value corresponding to a row and 8th column of the S-box is used to replace the a8 value. Shift-row transformation involves the action on the rows of an array. In this first row not shifted at all, 2nd row is shifted towards left by 1 step, 3rd row is shifted towards left by 2 steps and 4th row is moved towards left by 3 steps.

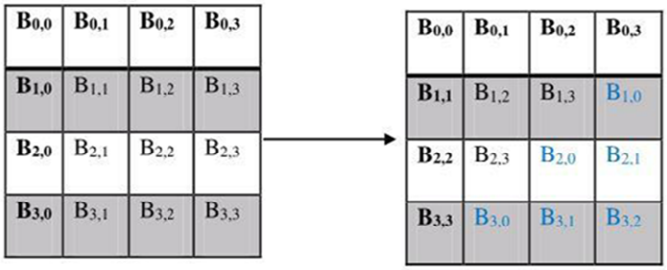

Figure 3.3. Shift-row transformation

Mix-column transposition is involved each column of state array multiplied by thefixed 4*4 array.

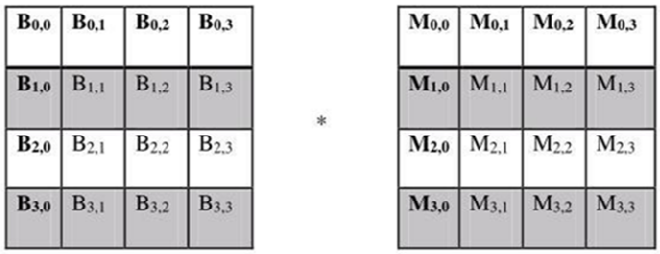

Figure 3.4. mixed columns transposition

Add round key involves the process of XOR which means each element of an array performs the function of XOR with each of the keys.

$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

$\oplus$

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

Figure 3.5. Add-round key

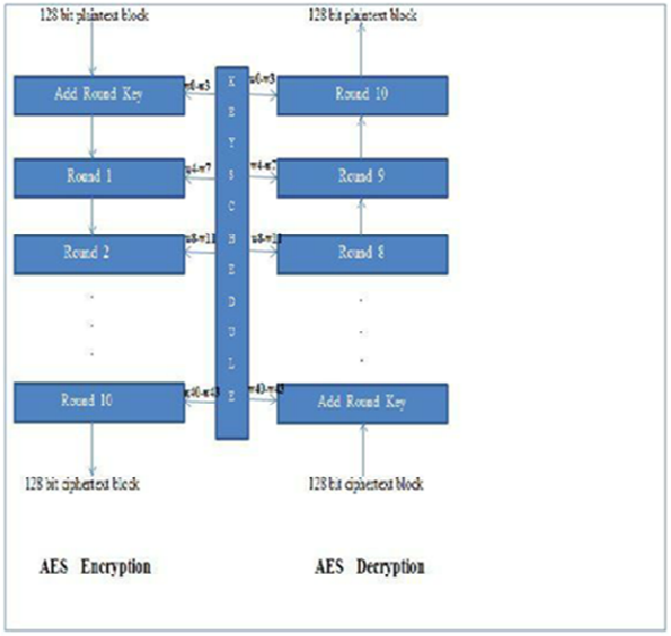

Figure 3.6. Encryption and decryption process off AES

Proposed methodology-ecdhqaes algorithm

Sender's system architecture

Step 1. Register and login with correct login information. Here, we will register with particular details and will use that detail to loginto the panel.

Step 2. Select a file you want to upload. We will select a file which we want to store in the cloud.

Step 3. Select or choose a key for encryption. DH will generate two keys and we will choose the key that we want to use for encryption.

Step 4. Apply QAES on selected file will generate an encrypted file. (We will apply hybrid encryption techniques to encrypt the file.)

Step 5. Apply elliptic curve cryptography on the selected file.

Step 6. Now, Store encrypted file along with encrypted key in thecloud.

Here, we will store the file in cloud

Receiver's system Architecture

Step 1. Login with correct information. Login with personal details with which we have registered.

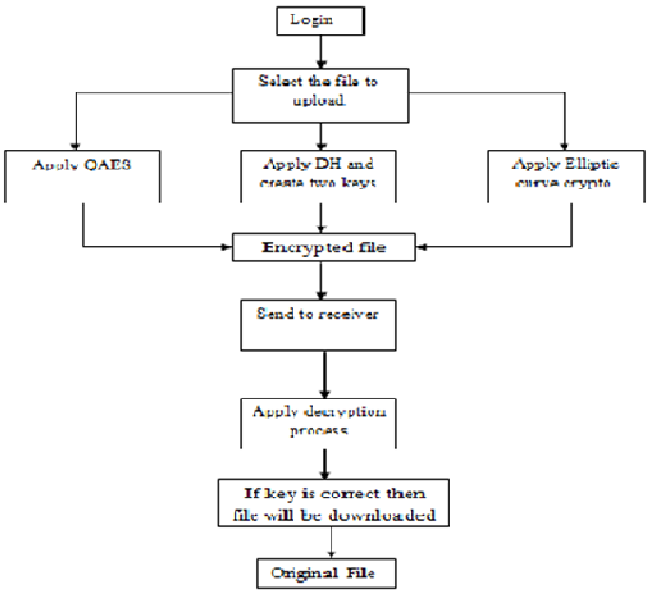

Figure 3.7 Flow chart of ECDHQAES

Step 2. Select a file which you want to download from the cloud.

We will select a file which we want to download from the cloud.

Step 3. Enter correct key to download file.

If thekey is correct then allow access to download otherwise denied access to download.

Step 4. Apply correct AES key on encrypted file. - If thekey is correct then decrypt and allow access to the file otherwise denied accessibility.

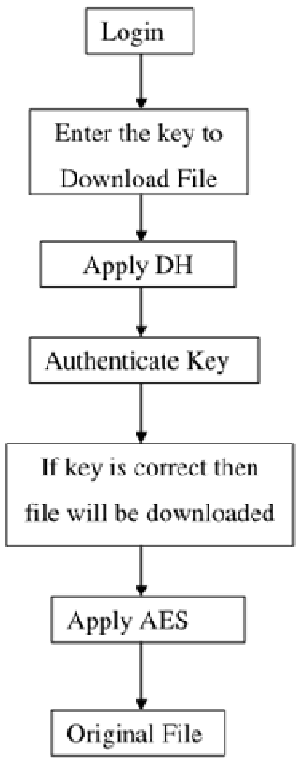

Figure 3.8. Flow chart of decryption

RESULTS AND DISCUSSION

To attain the encryption /decryption process in QAES with 128 bit must followthe belowsteps:

- The quantum secret key is generated over the Quantum channel using BB84 protocol.
- The sender and the receiver parties check the online compatibility for the generated secret key.
- The system used Diffie-hellman key exchanger method between client and cloud.
- Cloud simulates by Cloudsim and creates VM and broker environment.
- Cloud stores the encrypted data.
- An appropriate key length (128, 192, 256 bits) will be chosen by sender and the receiver using classical channels in order to perform the encryption/decryption process.
- The two parts deploy the selected final secret key to the symmetric encryption algorithm (AES).
- Encrypt the first block input file (PI -128bits) by the AES stages.
- The decryption beginsby the end of the Encryption (inverse methodology).
- After completion of process, analysis of storage and time on the cloud side

The design and simulation of the cloud environmentare carried out in Cloudsim simulator. The below steps has been performed to simulate the cloud environment.

- Firstly we run the cloud.java file of an algorithm which is on thesimulator and it waiting for the client.
- In the second step, when thecloud is running successfully then we run the client of that particular algorithm.
- In the next step, we can check the value in the console mode.

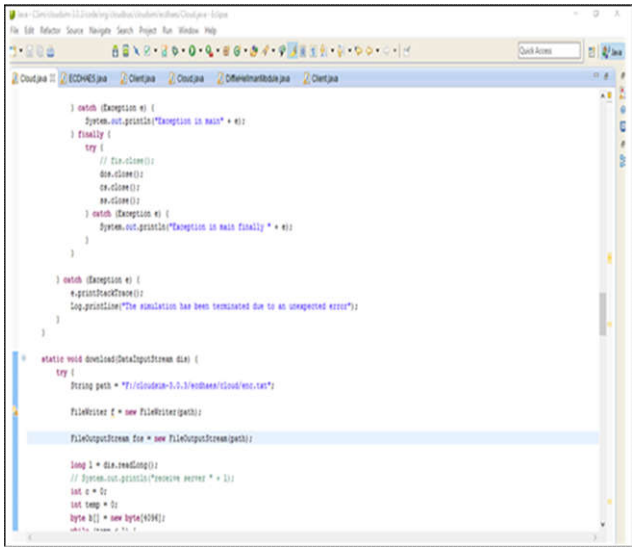

Figure 4.1. Simulation environment

In Fig. 4.1, shows the Cloudsim simulator, in which cloud.java, client.java files for both algorithms means DHAES (previous one) and ECDHQAES (Proposed one).

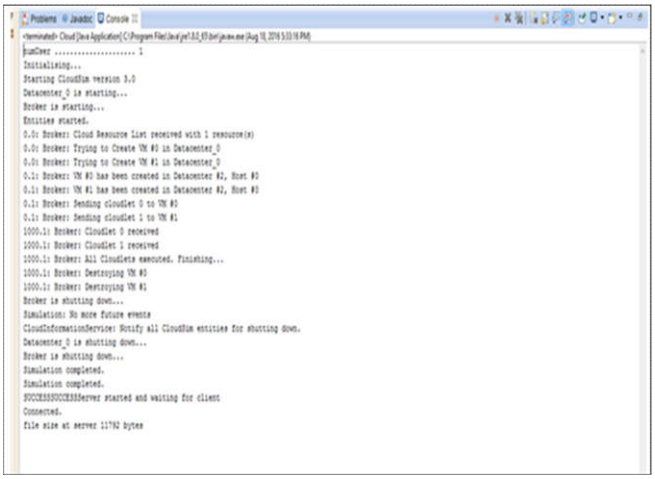

Figure 4.2. Running cloud

In Fig. 4.2, shows the running cloud on the simulator. When we run the cloud.java file from simulation environment then it waiting for the client and before that broker is started and then thecloud is successfully running.

Filename- File1

File size- 12473 bytes

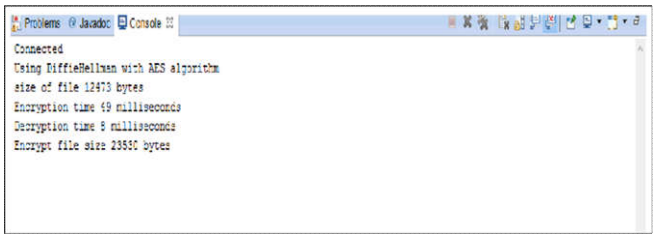

Figure 4.3. Encryption using DHAES algorithm

In Fig. 4.3, shows the result of File 1 using DHAES algorithm. It encrypts the file and then decrypts the same file within 57ms. File size after encryption is 23530 bytes.

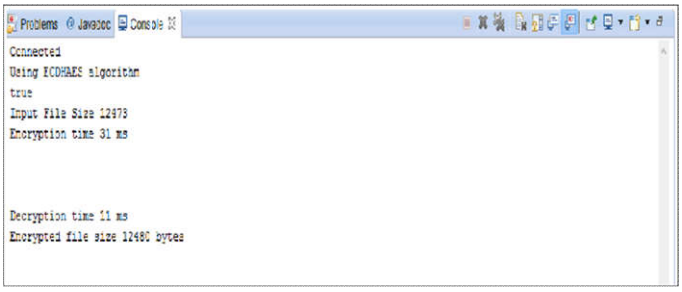

Figure 4.4. Encryption and decryption time

In Fig. 4.4, shows the encryption, decryption time and encrypted file size which is calculated by using ECDHQAES Similarly, we have simulated for file2 and file3 and the results are listed below.

Table 4.1. Result of ECDHQAES

File Name	E+D(Time)	File size(bytes)	Encrypted file size(bytes)
File1	31+11=42 ms	12473	12480
File2	32+12=44 ms	12178	12192
File3	11+2=13ms	295	304

We have simulated the same files in DHAES Algorithm (which is currently using) we got the below results.

Table 4.2. Result of DHAES

File Name	E+D(Time)	File size(bytes)	Encrypted file size (bytes)
File1	49+8=57 ms.	12473	23530
File2	67+8=75 ms.	12178	23120
File3	30+1=31 ms.	295	582

From the above results, we can absorb that security and encryption and decryption time of ECDHQAES is less compared to DHAES also reduces the storage on the cloud.

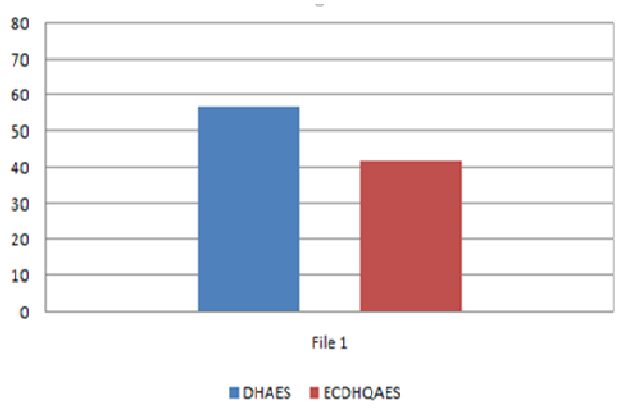

Figure 1. Comparison between E+D time (File1)

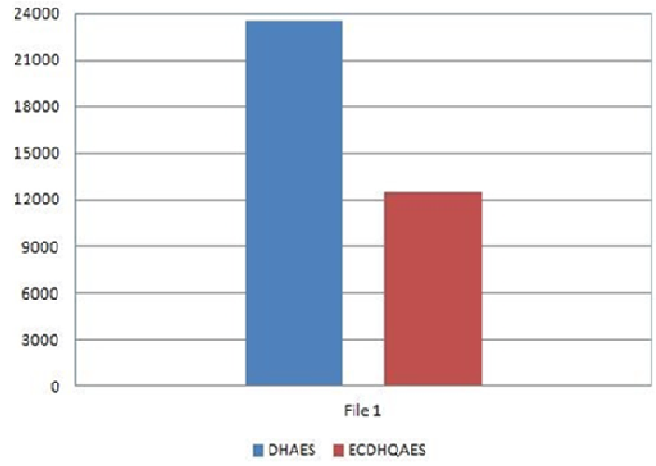

Figure 2. Comparison between encrypted file sizes (File1)

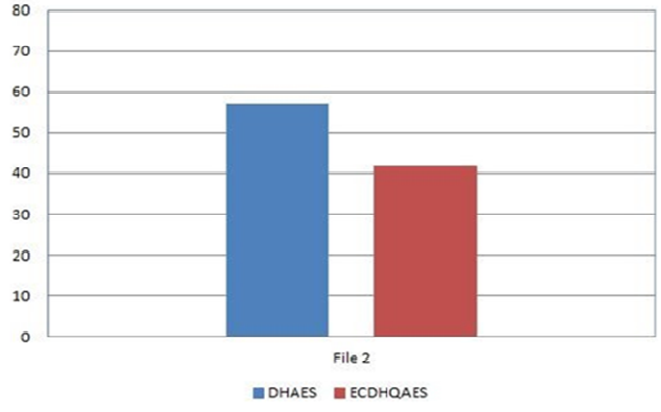

Figure 3. Comparison between E+D time (File2)

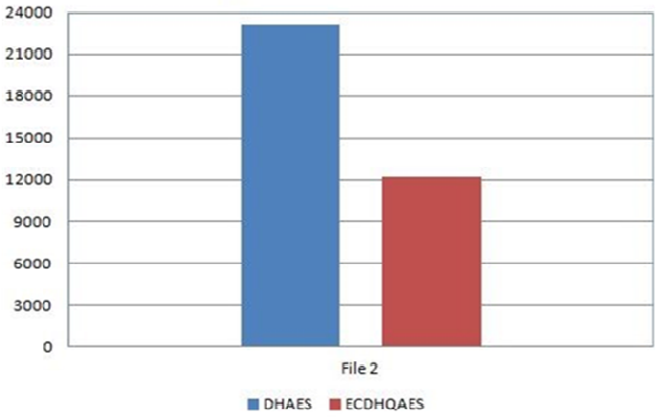

Figure 4. Comparison between encrypted file sizes (File2)

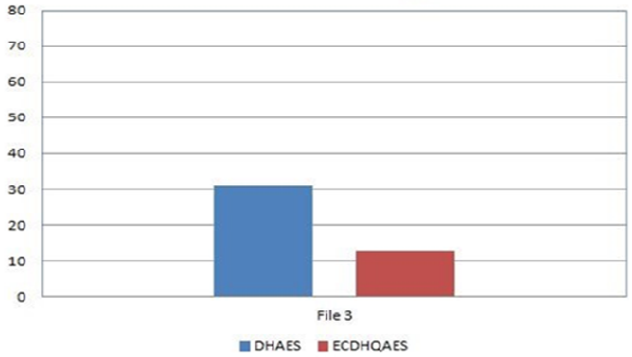

Figure 5. Comparison between E+D time (File3)

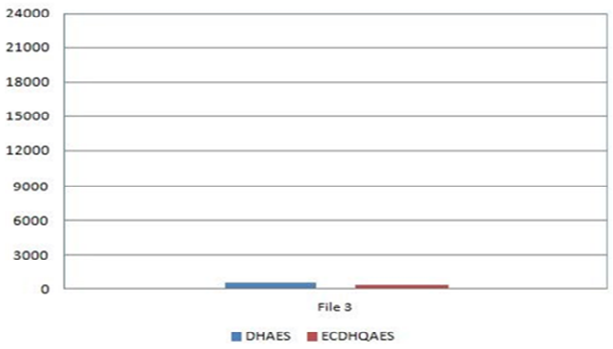

Figure 6. Comparison between encrypted file sizes (File3)

The graphsshow the encryption + Decryption time and encrypted file size of thefile (File 1). The E + D time in the graph, theBlue bars shows the DHAES and red shows the ECDHQAES. The proposed algorithm takes less time for encryption and decryption as compared to DHAES and same in the case of encrypted file size.

Conclusion

Cloud computing is becoming a great approach to the business world and private use. As the cloud is widely used security is an important constraint.In this research, we have reviewed the cloud computing with its authentication techniques, like various methods and techniques for implementing different levels of security using various cloud authentication and authentication schemes. There are many outbreakson cloud, identity and access management holds the key to it.The proposed algorithm is based on encryption and decryption

using different keys, storage and the time taken by encryption and decryption process. This algorithm will reduce the encryption and decryption time of the selected file, which significantly decreases the data transmission delay and also reduce the storage. The size of the file is reduced which directly affect the storage area in bytes. The major concern was security. The cryptographic algorithms Diffie-hellman, quantum-AES and elliptic curve cryptography is used to achieve the authentication and authorization. Diffie-hellman work as key exchanger between both the parties. Quantum-AES is advanced encryption standard used to treat data as a block for encryption and decryption.Elliptic curve cryptography is used for public keys to compare the keys. Public cloud is unsecured to access, store and manage the data. The algorithm will work for public cloud as well as thenon-cloud environment. The data transmission delay in vanets will significantly decreases.

REFERENCES

Aditya Harbola, Deepti Negi, Deepak Harbola, 2012. "A NEW A3 Kerberos Model" *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 2, Issue 3, March, pp.- 290-293.

Aeri Lee, 2015. "Authentication scheme for smart learning system in the cloud computing environment", J *ComputVirol Hack Tech* (2015), @ Springer-Verlag France.

Ajey Singh, Dr. Maneesh Shrivastava, 2012. "Overview of Attacks on Cloud Computing", *International Journal of Engineering and Innovative Technology* (IJEIT) Volume 1, Issue 4, April.

Allen Oommen Joseph, Jaspher W. 2014. Kathrine and Rohit Vijayan, "Cloud Security Mechanisms for Data Protection: A Survey", *International Journal of Multimedia and Ubiquitous Engineering* Vol.9, No.9.

Cloud Computing Bible. 2011 Wi/ey Publishing, Inc., Indianapolis, Indiana, p25.

Cristian PERRA, 2015. "A Framework for User Control Over Media Data Based on a Trusted Point", IEEE International Conference on Consumer Electronics (ICCE)-, 978-1-4799-7543-3/15/02015 IEEE.

Dhaval Patel, M.B. Chaudhari, 2014."Data security in cloud computing using digital signature", *International Journal For Technological Research In Engineering* Volume 1, Issue 10, June-2014, ISSN (Online): 2347 - 4718.

Dinesha H A CORI, Agrawal V K CORI, 2012. "Multi-level Authentication Technique for Accessing Cloud Services", ICCCA, 2012 *International Conference* on, vol. no., pp.1-4, 22-24 Feb.

Dr. Venkatesa Kumar, V. and Murugave1, A. 2015. "Ensuring consistency file authentication over encrypted files in the cloud", 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS), 978-1-4799-6818-3/15/0 2015 IEEE.

Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani, 2014. "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", 978-1-4799-2027-3/14/$31.00 02014 IEEE.

Gaurav Raj, Ram CharanKesireddi and Shruti Gupta, "Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256bit Encryption in Cloud", 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015, 02015 IEEE.

Gehana Booth, Andrew Soknacki, and Anil Somayaji, 2013. "Cloud Security: Attacks and Current Defenses", 8th Annual symposium on information assurance (ASIA' 13), June 4-5, Albany, Ny.

http://www.ibm.com/developerworks/cloud/library/cl-cloudserviesliaas.

Jen-Ho Yang, Pei-yu Lin, 2014. "An ID-Based User Authentication Scheme for Cloud Computing", 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 0 IEEE.

Kawser WazedNafi, TonnyShekha Kar, sayedAnisul Hoque, Dr. M. M. A Hashem, 2012. "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 10.

Ms. JasmmBhambure, Ms. Dhanashrl Chavan, Ms. Pallavi Band, Mrs. Lakshmi Madhuri, 2014. "Secure Authentication Protocol in Client-Server Application using Visual Cryptography", *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 4, Issue 2, February, pp.556-560.

Nivedita Shimbre and Prof. Priya Deshpande, 2015. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm" *International Conference on Computing Communication Control and Automation*, 0 IEEE DOI-10.1109/1CCUBEA.2015.16.

Peter Mell, Timothy Grance, 2011. "The NIST Definition of Cloud Computing", Recommendations of the National *Institute of Standards and Technology, September, Special Publication* 800-145.

S.1Shaik Hussain and V. Yuvaraj, 2015. "A secure data access control method using aes for p2p storage cloud", ieee Sponsored 2nd International Conference on *Innovations in Information, Embedded and Communication systems* (ICJJECS)2()15, 0 IEEE.

Sandeep Sahu, Aditi Bhadona, 2015. "Data Privacy over the Cloud Using Differential Evolution Algorithm", International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 - 8616 Volume 4, Special Issue September.

Shigeaki Tanimoto, Toshihiko Moriya, Hiroyuki Sato and Atsushi Kanai, 2015. "Improvement of Multiple CP/CPS based on Level of Assurance for Campus PKI Deployment", IEEE SNPD 2015, June 1-3, Takamatsu, Japan.

Shikha Singh, Binay Kumar Pandey, Ratnesh Srivastava, Neha Rawat, PoonamRawat, Awantika, 2014. "Cloud Computing Attacks: A discussion with Solutions", *Open Journal Of Mobile Computing And Cloud Computing*, Volume l, Number l, August.

Shobha Rajak, Ashok Verma, 2012. "Secure Data Storage in the Cloud using Digital Signature Mechanism" *International Journal of Advanced Research in Computer Engineering technology* volume 1, issue 4, june, issn: 2278 1323.

Shui.Han, J.X, "Ensuring data storage through a novelthird-party auditor scheme in cloud computing", *IEEE computer science and technology,* pp-264-268.

Sowmiya Murthy, "Cryptographic secure cloud storage model with anonymous authentication and automatic file recovery" *ICTACT journal on soft computing*, vol. 05, oct.-2014.

Subhash Chandra Patel, Ravi Shankar Singh, Sumit Jaiswal, "Secure and Privacy Enhanced Authentication Framework for Cloud Computing", *Second international conference on electronics and communication systems* (icecs 8/15/02015 IEEE. '2015), 978-1- 4788-7225

Tien-Ho, C., Hsiu-lien Y. and Wei-Kuan, S. 2015. "Elliptic Curve Cryptosystem (ECC) based on dynamic ID-Based remote mutual authentication", IEEE Sponsored 2nd *International Conference on Innovations in Information, Embedded and communication systems* (ICJJECS), 2015 IEEE

Wang, J.S., Liu, C.H., Lin, G.T.R. 2011. "How to Manage Information Security in Cloud Computing", IEEE, pp. 1405-1410.

Wei-Tsung su, WoChen Liu, Chao-Lieh Chen, Tsung-Pao Chen, 2015. "Cloud Access Control in Multi-layer Cloud Networks", International Conference on Consumer Electronics-Taiwan (ICCE-TW)-, 978-1-4799-87450/15/02015 IEEE.

YaserFuad Al-Dubai and Dr. Khamitkar S. D. 2014. "Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control", *Global Journal of Computer Science and Technology: B Cloud and Distributed* Volume 14 Issue I Version 1.0 Year 2014.

****