International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

A Hybrid Method for Secure Communication and Performance Analysis in VANET.

Zehra Afzal, Manoj Kumar

Abstract*: Vehicular Ad-hoc network a subclass of Mobile Ad-hoc network with various features providing Vehicle-to-Vehicle communication, Vehicle-to-RSU communication, Vehicle-to-Trusted Authority Communication. VANET is gaining higher attention now days both in industry and academic area and has become a trending research topic for research but still a lot of improvements is required in this area. Security of data is one of the major challenge in VANET. Encryption of data with the help of various encryption algorithms came up as solution for securing communication in VANET. But existing encryption algorithms used to secure VANET's are complex due to which data are not delivered on time and face a lot of problems like privacy of data ,non-repudiation and cost (i.e. communication cost, computational cost).In our proposed scheme we use a hybrid approach, which contain ECC algorithm(asymmetric algorithm).ECC algorithm is used for encryption of personal details (i.e. Speed, location, device address) and AES algorithm (symmetric algorithm) is used for encryption for safety messages along with output of ECC algorithm. The objective of this hybrid approach is to perform double encryption on personal details for more privacy of personal data (using ECC and AES algorithm) and single encryption on safety messages (using AES algorithm) so safety messages are delivered on time and without any delay.

Keywords: VANET, MANET, ECC, AES, Encryption.

I. INTRODUCTION

According to a survey done in 2018 by WHO (world health organization), the ninth biggest cause of death are traffic accidents because of which around 1.3million people die every year. Prediction of this survey is that in 2030 road accident will become the fifth major cause of death [1]. In European member states in every twelve months 1.8 million people are injured and 48,000 people die due to these road accidents that costs around 160 billion Euros [2]. In addition to these road accidents, traffic jams also lead to wastage of time and fuel. At present people are more dependent on private vehicles or taxi services which lead to increase in number of vehicles. Due to unawareness of traffic rules and increase in no of vehicles accidents are proportional to increase in no of vehicles. Safety of people on roads is thus challenging issue in VANET [3]. Vehicular Ad-hoc network also known as network on wheels provides communication between various vehicular nodes [4].

Revised Manuscript Received on June 15, 2020.
* Correspondence Author
Zehra Afzal*, Computer science and engineering, Shri Mata Vaishno Devi University,Katra,India,18mms014@smvdu.ac.in.
Manoj Kumar, Computer science and engineering, Shri Mata Vaishno Devi University, Katra, India, manoj.kumar@smvdu.ac.in

It is a special type of MANET where mobile nodes are self-supporting and interact with other mobile nodes using infrastructure less environment [5]. Due to large number of accidents, road congestion, and environmental pollution that had caused various serious effects this Vehicular Ad-hoc Network has achieved great interest from previous years. In every country whether that is progressed country or is progressing both had resulted a serious impact both in life and property due to these vehicular accidents. In order to make the journey safe and to minimize the effects due to this network. Intelligent Transportation System (ITS) introduces vehicular Ad-hoc network as a safe and secure infrastructure for moving nodes [6]. Vehicular Ad-hoc Network (VANET) compromises of following main Components OBU (On-Board-Unit), RSU(Road Side Unit) and TA (Trusted Authority) as shown in fig1.OBU is installed on vehicles and is used to receive, process and transmit information related to traffic to other vehicles with the help of DSRC(Dedicated short range communication) Protocol[7,8].DSRC protocol also termed as WAVE(Wireless access in vehicular environment) make use of 802.11p standard for communication among vehicles and transfer of safety messages within interval of(100-300ms) to other vehicles and road-side units[9].RSU(Road side units) are deployed along the banks of roads that is used as an intermediate unit between OBU and RSU and performs authentication process. TA (Trusted Authority is a third party that performs management, maintenance of VANET and registration of OBU and RSU. AP it supports safety applications and provides services for RSU communication.

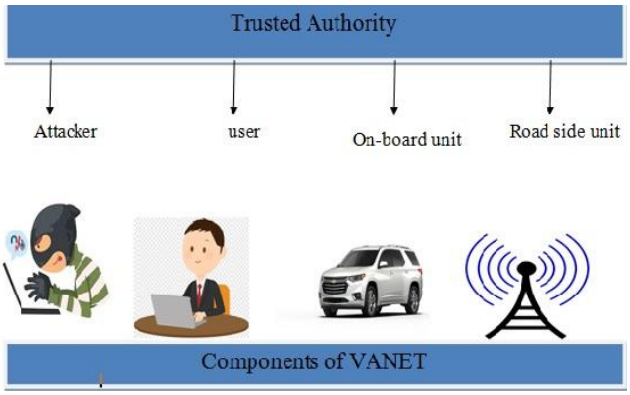


Figure 1: Components of VANET

II. GENERAL MODEL OF VANET

General Model of VANET: VANET comprises of four different types of communications [10].

Figure [2] describes the general model of vehicular ad-hoc network. In-Vehicle Communication: In-vehicle communication is one of the important and significant research area in vehicular Ad-hoc network. This type of communication is used to trace down performance of vehicle that commonly includes laziness and exhaustion of drivers that has a serious impact on driver and public safety. Vehicle-Vehicle Communication: Vehicle-Vehicle communication is another type of communication in Vehicular Ad-hoc Network that provides infrastructure for drivers to communicate warning messages and other important information to other mobile nodes. Vehicle –Roadside unit Communication: Vehicle-Roadside Unit Communication is other important research area in VANET. This type of communication provides weather and traffic information to vehicles. To improve the flow of traffic for ensuring safe driving so to reduce the traffic accidents that will be solved by communicating accurate information to drivers or to the other vehicular nodes VANET is developed. The information that is transferred in vehicular Ad-hoc environment is critical information that must be delivered on time. Any modification to this information by a third party may cause various serious effects that will affect the safety of people on road. So we need to secure this information for efficient transmission of critical time information. Thus Security in VANET is on the top vision for researchers [11].

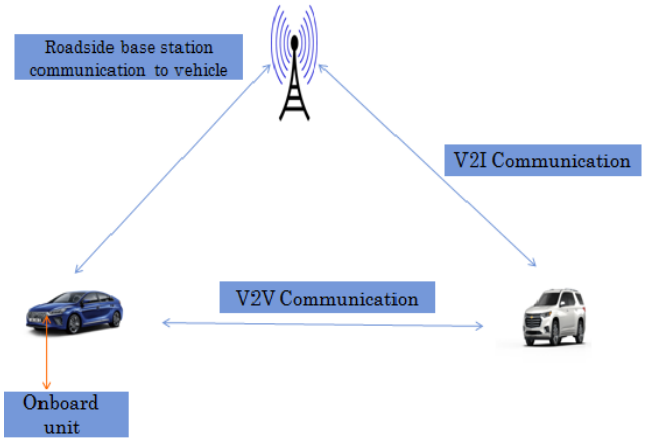


Figure 2: General model of VANET

III. ADVANTAGES OF VANET

Vehicular ad hoc network provides various applications to improve the safety on roads by providing accurate information or warning messages to drivers if there is any road accident ahead or if there is congestion or traffic jam. [12] This information helps to improve the driving experience and also helps to provide some other valuable information to drivers throughout their journey. Vehicular ad hoc network also provides the personal information like speed, location, owner, in case of emergency like theft, accident to the traffic management or central authority. It also alerts two divers if they are about to collide to mend their ways [13]. VANET also provides some other information to vehicles like sharp curve ahead so that they can slow down their speed, condition of road ahead etc. In addition of these safety applications it provides much other comfort application like streaming of videos, online gaming, and electronic payment at toll plaza to avoid traffic jams. VANET also provides information like nearby petrol pump, parking availability, hotel, restaurant etc.

In VANET nodes are independent they don't depend on central network. if any node breaks it does not have any effect on other nodes in the network. Vehicular ad hoc network is very large and scalable, that means we can add or remove any number of nodes to this network [14].

In addition to these advantages, VANET also have some challenges that needs to be addressed like high mobility due to which topology changes very frequently and nodes can make connection for a short interval. Privacy, high latency, irregular network density and security which is the most critical issue in VANET that needs to be resolved.

IV. SECURITY CHALLENGES IN VANET

In Vehicular Ad-hoc network developing trust is important among various vehicular nodes to secure integrity and reliability that helps vehicles to collect correct and credible information from surrounding vehicles [15]. Since the vehicular ad hoc network is open i.e. information is transferred in a wireless environment that means data transmission is vulnerable to attacks [16] .so we need to secure this data transmission. In addition, providing security in vehicular network also provides the security requirements as mentioned below:

Authentication: Authentication makes sure that the sender which sends the message and the receiver of a message are legitimate users.

Information verification: Information verification ensures that the message that has been send is not malicious or false

Accessibility: Accessibility makes sure that only intended users can access the information that has been send.

Privacy: Privacy ensures that the personal details such as Speed, Location, Owner's information is hidden from unauthorized nodes.

Availability: Availability ensures that the resources/data is always available on time to the intended users.

Reliability: Reliability is one of the basic requirements that makes sure that data is delivered to destination and transmission of data is reliable.

Integrity: Integrity ensures that the data is delivered from sender to receiver without any alteration.

Various solutions have been proposed to improve the security in VANET but it is still a subject of concern in VANET. Cryptography is one of the best solutions for providing secure transmission of data in vehicular ad-hoc network

V. CRYPTOGRAPHIC SOLUTIONS

Cryptography is the process of securing information and communication with the help of various algorithms so that this information is available or accessible only to the intended users [17]. In cryptography "crypt" means "hidden" or "secret "and "grapy" means "writing" [18]. Therefore, cryptography can also be referred as secret writing. In cryptography process the data that is to be send is termed as plain text that is converted into cipher text by encryption process so that only the intended user can decrypt it that has the key to ensure the security in VANET [19].

Retrieval Number: E1022069520/2020©BEIESP
DOI: 10.35940/ijeat.E1022.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. CRYPTOGRAPHIC ALGORITHMS

Cryptography algorithms are broadly classified into two categories that are described below [20]:

- Asymmetric Cryptographic Algorithms.
- Symmetric Cryptographic Algorithms.

Symmetric cryptographic algorithms: symmetric cryptographic algorithms are those cryptographic algorithms that make use of a single key for encryption and same key for decryption [21]. Also known as Secret key cryptography algorithms [22].

Table [1] describes some of the symmetric key cryptographic algorithms**.**

Drawbacks: Symmetric algorithms make use of a single key for both encryption and decryption of data. So we need to transmit this key along with data to receiver for decryption of data. If any malicious node gets this key, then he will get access to data that needs to be secret.

Algorithm	Key length	Rounds	Block size	Efficiency	Applications
AES	128,192, 256	10 or 12 or 14	128 bits	Fast	Wireless communication, bank
DES	56-bits	16	64 bits	Slow	Image processing
3DES	168, 112 bits	48	64 bits	Fast for hardware but slow for software	Smart card, e-payment
BLOW FISH	128-448 bits	16	64 bits	Fast	Database security, Ecommerce software

Asymmetric Cryptographic Algorithm: Asymmetric Cryptographic Algorithm is that type of cryptographic algorithm that make use of two keys (public and private key) [23]. Public key is a key that is known to everyone and is used for encryption of data and private key is secret that is used for decryption of data. So in this type of cryptographic algorithm only the user which has the private key can decrypt the data [24]. Table [2] describes some of the symmetric key cryptographic algorithms**.**

Algorithm	Key length	Rounds	Blocksize	Efficiency	Applications
RSA	1024-2048 bit	1	192	Slow	Internet banking
DSA	2048-3072bit	16	variable	slow	Web application and email verification
ECC	160 bit	1	80	fast	Key exchange over web and mobile

Drawbacks: An asymmetric algorithm uses longer key for better encryption than symmetric key algorithms that slows down the encryption speed and takes time to deliver the information.

VII. PROPSED METHODOLOGY

As already discussed above both symmetric and asymmetric algorithms, have some drawbacks. If symmetric algorithms are used for encryption process, it does not provide much security because it has a single key. If any malicious node gets that key, we will lose the privacy of personal data but it takes less time so safety messages are delivered on time. And if Asymmetric algorithms are used for encryption process it will provide us privacy of information but at the same time it takes too much time due to which safety messages are not delivered on time leading to various accidents.

In our proposed methodology we have resolved these drawbacks by making a hybrid model. In this hybrid model we have used both (symmetric and asymmetric) algorithm for encryption and decryption process. Symmetric algorithm is used for encryption of safety messages as they take less time and these messages must be delivered on time. Asymmetric algorithm is used for encryption of personal details as they provide privacy of data more than symmetric algorithm. Out of all the symmetric algorithms and Asymmetric Algorithms the algorithms used in our hybrid model are AES and ECC.

Advanced Encryption Standard (AES) is a Symmetric cryptographic algorithm that uses single key for both encryption and decryption [26]. Out of all Symmetric cryptographic algorithm AES is used in our proposed methodology because it is fast takes less time for encryption and decryption and is more secure [2]. Elliptic Curve Cryptography (ECC) is an Asymmetric cryptographic algorithm that has separate public and private key for both encryption and decryption [24]. Advantage of ECC over other Asymmetric Cryptographic Algorithms is that provide the same security like RSA that is commonly used but with smaller key size, low power consumption, and less memory that is why it is used in our proposed methodology [14].

Fig depicts the working flow of proposed methodology:

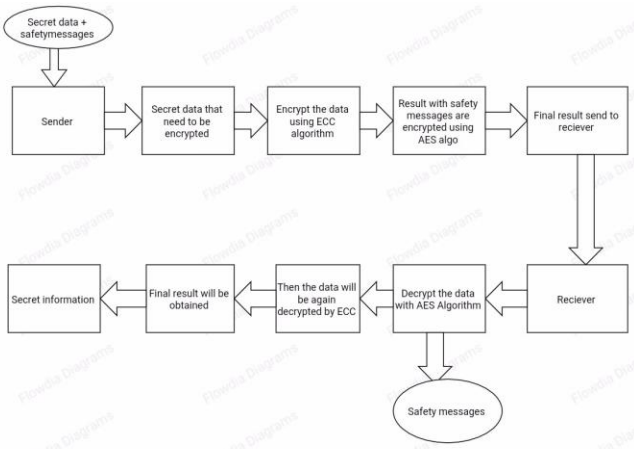


Figure 3: Proposed methodology.

VIII. ALGORITHM

A) Encryption process:

Step1: Sender takes the input that is to be transmitted to the receiver securely. Input consists of two parts safety messages and personal information (e.g. location, speed).

Step2: In this step the sender sends the personal data (i.e. first part of input) for encryption using Asymmetric algorithm (i.e. ECC).

Step 3: Encryption using ECC algorithm is performed on personal data and output is produced.

Step4: In step 4 safety messages (i.e. second part of input) along with the output of step 3 are send for double encryption using AES cryptographic algorithms.

Step5: Encryption using AES algorithm is performed in this step 5 and the output is send to the receiver.

B) Decryption process:

Step6: Receiver receives the data from the sender that is encrypted and starts its decryption to get the desired information.

Step7: In step 7 receivers sends the data for decryption using symmetric algorithm (i.e. AES).

Step8: Decryption of data using AES algorithm is performed from which we get one output i.e. safety messages within a specific time interval and is delivered to receiver so he can take appropriate action on time. And 2nd output that needs further decryption.

Step9: In step 9 output 2nd from step 8 is send for further decryption using Asymmetric algorithm (i.e. ECC). Step10: Decryption using ECC algorithm is performed on 2nd part of output that produces the result (i.e. personal information).

IX. PERFORMANCE EVALVATIOM PARAMETERS

Our proposed model in security analysis provides authentication, confidentiality and integrity of send information. The experiment is performed in MATLAB. Performance analysis in done based on computation time and throughput.

A. Computation time: It is the time taken by our proposed algorithm to produce a desired output. It consists of two parts:
a) Encryption time: It is the time taken by our cryptographic algorithms to produce a cipher text from a pain text
b) Decryption time: It is the time taken by our cryptographic algorithm to produce a plaintext from a cipher text.

B. Key size: key size is the length of key in bits used by cryptographic algorithms .it determines the complexity of algorithm.

C. Throughput: Throughput is defined as the summation of total data encrypted or decrypted to the total computation time .It is measured in bytes per second. It consists of two parts:
a) Encryption throughput: total input size (in bytes)/total Encryption computation time.
b) Decryption throughput: total input size (in bytes)/ total Decryption computation time.

X. SIMULATION RESULTS.

The simulation result of the proposed method is shown in table .The simulation of vehicular network is performed in MATLAB.

Figure shows the GUI of our proposed models. It displays the list and sequence of steps to be performed in our proposed method.

Figure 4: GUI of Proposed Algorithm

Figure [5] shows the nodes deployed that needs to communicate with each other with their location and speed.

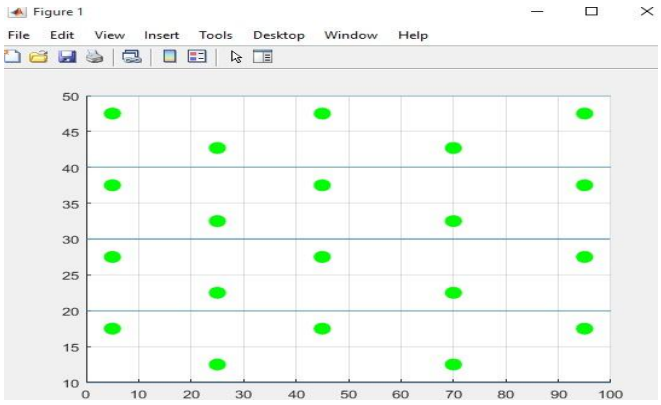
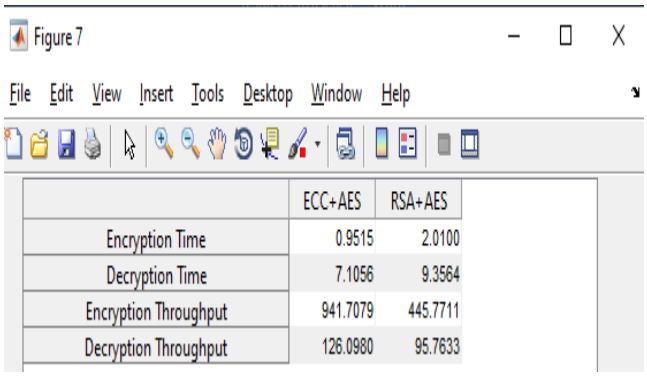


Figure 5: Node Deployment in VANET

Fig [6] describes the simulation results our Proposed algorithm (ECC+AES) based on performance measures described above in comparison with previous Hybrid Algorithm used i.e.(RSA+AES).



	ECC+AES	RSA+AES
Encryption Time	0.9515	2.0100
Decryption Time	7.1056	9.3564
Encryption Throughput	941.7079	445.7711
Decryption Throughput	126.0980	95.7633

Figure 6: Simulation results in comparison with previous algorithm

Fig [7, 8] shows the simulation results of proposed algorithms in comparison with previous hybrid algorithm graphically:

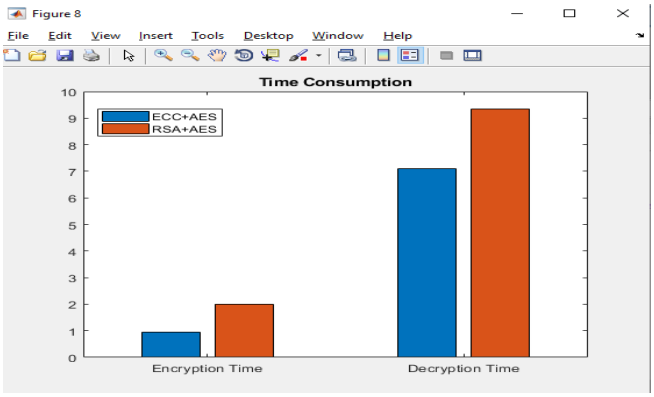


Figure 7: Time consumption of proposed algorithm in comparison with previous algorithm.

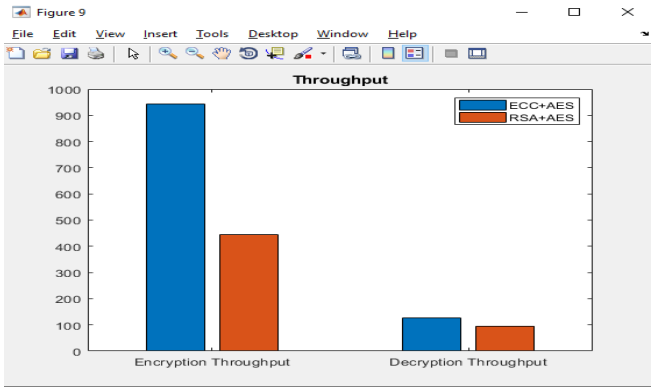


Figure 8: Throughput of proposed algorithm in comparison with previous algorithm.

XI. CONCLUSION

Vehicular ad-hoc network security now a day is a trending topic for researchers. Due to lack of proper security mechanism, various accidents occur in VANET. So to avoid these accidents and for smooth flow of information we used a new security mechanism for this vehicular ad-hoc network. In our paper we used a hybrid model that contains both symmetric algorithm (i.e. AES) and asymmetric algorithm(i.e. ECC) to overcome the drawbacks they have .AES algorithm is used for encryption and decryption of safety messages only so they are delivered on time and ECC is used for encryption and decryption of personal details as it takes long time but provide more security .so in this hybrid model we achieve both the goals i.e. delivered safety messages on time and provide more security to personal details that overall increase security of VANET.

REFERENCES

1. Ali, Ikram, Alzubair Hassan, and Fagen Li. "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey." Vehicular Communications (2019).
2. WHO, Global status report on road safety 2015, http://www.who .int /violence _injury _prevention /road _safety _status /2015 /en. (Accessed19 March 2018).
3. Goyal, Amit Kumar, Gaurav Agarwal, and Arun Kumar Tripathi. "Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey." (2019).
4. Abbasi, Arshad Ahmed, and Adnan Shahid Khan. "A review of vehicle to vehicle communication protocols for VANETs in the urban environment." Future Internet 10.2 (2018): 14.
5. Lim, Kiho, and D. Manivannan. "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks." Vehicular Communications 4 (2016): 30-37. [6] Shrestha, Rakesh, Rojeena Bajracharya, and Seung Yeob Nam. "Challenges of future VANET and cloud-based approaches." Wireless Communications and Mobile Computing 2018 (2018).
6. Dedicated Short Range Communications (DSRC), available: http://grouper.ieee .org /groups /scc32 /dsrc /index .html. (Accessed20 March 2018).
7. O. Hyunseo, Y. Chungil, A. Donghyon, C. Hanberg, 5.8 GHz DSRC packet com-munication system for ITS services, in: Gateway to 21st Century Communica-tions Village, VTC 1999-Fall, IEEE VTS 50th Vehicular Technology Conference, 1999, pp.2223–2227 (Cat. No. 99CH36324 [9]Vehicle Safety Communications Project Report, National Highway Traffic Safety Administration, U.S. Department of Transportation, 2006.
8. Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." International Journal of Distributed Sensor Networks 11, no. 8 (2015): 745303
9. Kaur,R.,Singh, T.P.&Khajuria,V.(2018,May).”Security issues in vehicular ad-hoc network (VANET).In 2018 2nd International conference on trends in Electronics and Informatics (ICOEI),pp.884-889.IEEE,2018.
10. H. Hartenstein and K. Laberteaux, “VANET-Vehicular Applications and Inter-Networking Technologies”, John Wiley & Sons, February 2010
11. Rasheed, Asim, Saira Gillani, Sana Ajmal, and Amir Qayyum. "Vehicular ad hoc network (VANET): A survey, challenges, and applications." In Vehicular Ad-Hoc Networks for Smart Cities, pp. 39-51. Springer, Singapore, 2017.
12. Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." International Journal of Distributed Sensor Networks 11, no. 8 (2015): 745303
13. Rajdeep Kaur, Tejinder Pal Singh and VinayakKhajuria, “Security Issues in Vehicular Ad-hoc Network(VANET)”, Department of Computer Science and Engineering, Chandigarh University, Mohali, India. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore ISBN: 978-1-5386-3570-4
14. Amrish Kumar and Shri Niwashn Sir, “Implementation of VANET in Transportation using Wireless Sensors”, Computer Science & Engineering Subharti Institute of Engineering & Technology, Meerut, India. International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882, Volume 4, Issue 6, June 2015. [17] Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, “Security and Trust Preserving VM Migrations in Public Clouds”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.
15. S C Rachana, Dr. H S Guruprasad, “Emerging Security Issues and Challenges in Cloud Computing”, International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967
16. Shakeeba S.Khan , Prof.R.R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms”, International Journal of Innovative Research in Compute and Communication Engineering, Vol. 3, Issue 1, January 2015. [20] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, “Efficiency of Modern Encryption Algorithms in Cloud Computing”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 6, November – December 2013 ISSN 2278-6856
17. Rachna Arora, Anshu Parashar, “Secure User Data in Cloud Computing Using Encryption Algorithms”, Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926
18. Kalpana Parsi, Singaraju Sudha. ”Data Security in Cloud Computing using RSA Algorithm”. International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.https://en.wikipedia.org

19. Kalkundri, Ravi U., Rajashri Khanai, and Kalkundri Praveen. "Survey on Security for WSN based VANET using ECC." International Annals of Science 8.1 (2020): 30-37. [25] Patel, Kuntal. "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files." International Journal of Information Technology 11.4 (2019): 813-819.
20. Rizal, Muhammad, Elviawaty Muisa Zamzami, and Muhammad Zarlis. "Cryptographic Symmetry Analysis with AES Algorithm for Safeguarding Data at Government Agencies." IJISTECH (International Journal of Information System & Technology) 3.1 (2019): 131-139.

AUTHORS PROFILE

Zehra Afzal has done B.tech from Baba Ghulam Shah Badshah University, Rajouri(J&K). She is Pursuing M.tech in computer science from Shri Mata Vaishno Devi University, Katra, (J& K). She has published a research paper in scopus indexed journal .Her area of interest includes digital image processing, machine learning and Ad-Hoc networking.

Manoj Kumar received B.tech and M.tech degree in computer science and engineering from Kurukshetra University, kurukshetra.He is pursuing PhD in area of Wireless Mesh Networks from SMVD University,katra. He has more than 16 years of teaching experience both undergraduate and postgraduate level.He has published several research paper in peer reviewed international journals and conferences.