Mr. Rajendra Thakur. 2022, 10:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Safe Vehicular Ad hoc Network: A Survey

M.Tech. Scholar Rajendra Thakur, Assistant Professor Megha Jat
Department of Computer Science,
Patel College of Science & Technology Indore, India
rajendrathakur004@gmal.com, Megha.guptajat@patelcollege.com

***Abstract*- The next generation of vehicle networks is called VANET, and its applications will play a crucial role in ensuring the safety of human lives when they are travelling on highways. When implementing VANET in a practical context, security is one of the most important and obvious elements to consider. Various researchers have previously provided a variety of solutions to the problem, which aims to make it safe against attackers and assaults on networks. In this overview study, explore in depth the many computing approaches that are available, and explain how they relate to vehicular networks. Employing these computational strategies to protect the vehicular network against attackers and assaults. Computing techniques such as trusted computing and cloud computing are examples of some of the several kinds of computing approaches that have previously been covered in VANET. However, there are still other computing methods, such as quantum computing and pervasive computing, that need to debate their connection with VANET and the security of the network.**

Keyword- Application, security, computing methods, trusted computing, cloud computing, pervasive computing.

I. INTRODUCTION

Transportation problems of recent years and traffic activities play an important part in the upbringing of people's day-to-day lives. Therefore, raising the degree of improvement to a higher standard is the most crucial step in developing a better vehicle system. On the one hand, the Transportation system is deteriorating on a daily basis as a direct result of the enormous volume of traffic, and on the other, the number of accidents has substantially increased. Because of the increase in the volume of automotive traffic and the resulting overpopulation around us [1], researchers have been looking into the possibility of linking new technologies to the Vehicular Ad Hoc Network (VANET).

[13] VANET is a fundamentally developing system that raises the level of traffic safety and lowers the number of traffic accidents. A wireless technology known as VANET is responsible for moving the automobile between the nodes and transferring the messages from one node to the next node. Nodes

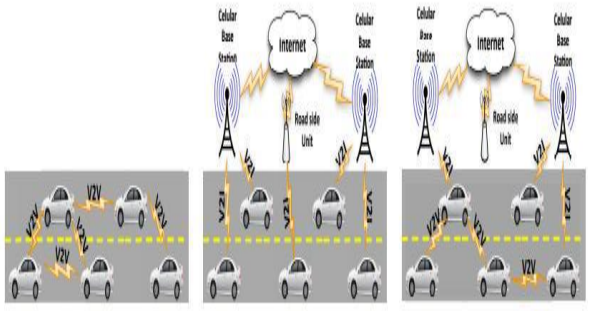

Fig. 1 VANET architecture [3].

II. SECURITY REQUIREMENTS

Safety and confidentiality play a significant part in the development of the VANET's principles, which have helped to make this transportation system one of a kind. In this regard, it is necessary to determine some kind of security requirement in order to satisfy

the requirements for privacy and to ensure secure wireless connection between the two cars. Data transformation in a safe way and with the attacker's protection in mind. In the event of a collision, drivers would be made aware of the scenario, which would assist them in responding appropriately to such an absurd circumstance [13]. The security of the VANET network will decide if there are further issues [2]. In point of fact, each and every communication model has its own unique needs in terms of security.

- Identification
- Authentication
- Element authentication
- Privacy conservation
- Non- repudiation
- Confidentiality
- Availability
- Trust

The verification of the requirements for each individual communication technology may be found in this table. Explain how the communication system works, validate the requirements based on the current state of the system, and ensure that the demands of the vehicle are met, taking into account the circumstances [14].

Identification- Each entity has its own one-of-a-kind value, which distinguishes it from those of the other entities. The Vehicle Identification Number, or VIN, is included in the identifier. The car's identification may be verified by the registration number, which is unique to each vehicle.The process of demonstrating one's distinct identity is referred to as authentication [15]. The authentication step serves as a level of approval and checks that the connection between cars is safe and that an attacker is not interrupting the discussion.

Element authentication- The only thing that is needed to fulfil this condition is to demonstrate that each of the participating entities already possess the necessary characteristics in order to join the group; this is known as the attribute authentication requirement [3]. The protection of one's privacy is an important consideration for cars. Because VANET was designed to provide encrypted communication, protecting the privacy of its users became an increasingly pressing concern [16]. When seen from a vehicular point of view, privacy may be said to have been attained. Two connected goals, satisfied untraceability and unlinkability, were also met [17].

Untraceability-The car in question cannot be located in any way (i.e. different achievement of the identical vehicle should not be interconnected).

Unlinkability- It should be impossible for a criminal organisation to connect the distinctive characteristics of a vehicle with those of its operator or owner [18]. Non-repudiation is an additional need for VANETs. This requirement states that users must not be able to refuse to transmit a message in order to keep it as a follow and avoid being accused of sending a fake message. Regarding the confidentiality of group communications, the massage will only be viewed by the authorised person. This is done to ensure that both parties have secure communication. Only members of the group are allowed to read the material [19].

Availability- Each node is on high alert and ready to communicate with the other nodes in order to provide information. This connection is a critical necessity for the security system as it is highly essential to the overall road safety [20].Procedures involving trust must guarantee that the data's integrity and accuracy at all times. Since the data that is significant should not be modified, trust is a fundamental need for communication over the VANET.

Table I Security Requirements in VANET [3].

VANET setting / Sec. Requirement	V2V warning propagation	V2V group communication	V2V beaconing	I2V warning	V2I warning
Entity identification	✓ (all vehicles)	x	✓ (sender)	✓ (sender)	✓ (sender&receiver)
Entity authentication	✓ (sender)	x	✓ (sender)	✓ (sender)	✓ (sender&receiver)
Attribute authentication	x	✓ (sender&receiver)	x	x	x
Privacy preservation	✓	✓	✓	x	✓
Non-repudiation	✓ (sender)	x	✓ (sender)	✓ (sender&receiver)	✓ (sender&receiver)
Confidentiality	x	✓	x	x	x
Availability	✓	✓	✓	✓	✓
Data trust	✓	✓	✓	✓	✓

III. SECURITY CHALLENGES IN VANET

The following is a detailed overview of the security issues that are present in VANET.

- Real Time Requirements Because VANET was able to meet the real time constraints, it was able to give the massages at the precise times that were necessary. Utilize an extremely quick algorithm for cryptography to accomplish this purpose [21].

- The liability associated with maintaining data consistency: Maintaining data consistency is essential in VANET and helps limit the disclosure of unneeded information since authenticate nodes may carry out nefarious actions.

- Key Distribution: Because VANET encrypts messages before sending them, and then decrypts them after the operation is finished, key distribution is a very significant procedure that also serves as the biggest obstacle. This is because VANET uses the key to both transmit and receive messages [22].

- High mobility: Since the nodes in a VANET are linked to each other and transmit signals in order to interact with other vehicles, a high mobility level is necessary for the network. The required speed of mobility must also be high. VANET requires shorter execution time.

- Non-repudiation: In this technique, the node cannot refuse to deliver the messages and signals, but it also does not send them. When it comes to crash re-establishment, it is going to be really important to figure out the correct procedure. [2]

- Data Verification and Privacy: In order to maintain the network's integrity, it is necessary to verify the verification of the data on a regular basis, and maintaining users' privacy is a very important aspect of the VANET [23].

IV. COMPUTING METHODS – VANET SECURITY

Security is still open challenges in vehicular network due to dynamic topology and dynamic behavior of attacker in network. Many security solutions already provided for VANET and in this section, we will review the previous work and also discuss some new computing methods to secure the vehicular network. The Fig. 2 shows the different types of computing methods and in this section provides detail discussion with respect to VANET security [24].

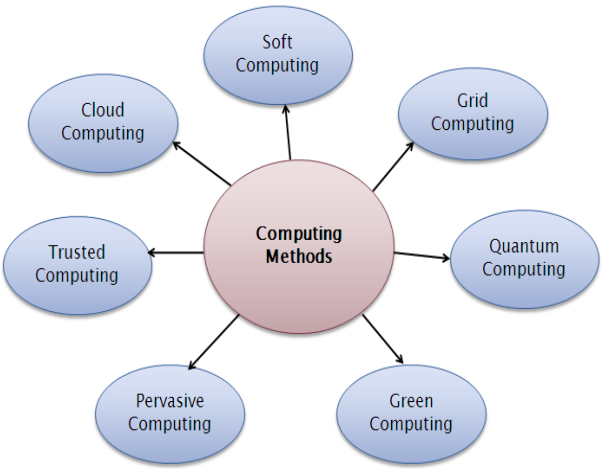

Fig. 2 Different types of computing methods.

1. Cloud Computing and VANET

Completion of the cloud computing application, including obtaining the advanced requirements and delivering the appropriate resources, services, and programmes Consequently, apps that use cloud computing aim to provide a competent output in order to tackle such issues [25]. Cloud computing is one of the most exciting new developments in the field of information technology. It is distinguished by its technological, financial, and user-friendly qualities. Cloud computing is the most recent iteration of a computational mode that proposes a pioneering production replica for organisations seeking to implement information technology without incurring significant upfront costs [26].

This enables the organisations to realise potential gains. The following are some of the most important aspects of cloud computing: fault tolerance, loose coupling, service orientation, pay per use, the ability to supply services on demand, and cost effectiveness, among other things. Computing on the cloud makes it easier for businesses and educational institutions to build new technologies. The use of communication nodes to communicate from one car to another's vehicle through VANET, which employs wireless networks and sensors to perceive the data, is currently the hottest issue in the automotive industry. Although the form of VANET is provided to MANET (mobile ad-hoc network), the behaviour of VANET is not the same as that of MANET [2].

There are several concerns with VANET that may be resolved using the cloud. Cost and security are also key challenges for VANET. Therefore, security is a big

and crucial component for VANET as it proposes an early detections system that would commence danger (risk warning) for drivers. Plausibility checks [3,] logic receiving beacons [4,] and tamper proof GPS [5] are the three approaches that have been suggested to secure vehicular systems from hackers who intentionally re-get the area of the vehicle in which the vehicle is located. There are two types of methods that may be used to recommend data-centric security and authentication in automotive networks: responsive and active security [27].

An active location integrity model, a passive location truthfulness model, and lastly a position integrity model [2] are the three varieties of replica that may legitimate and merge the position of information in a Vehicular Cloud (VC). Although a localization method that relies on insolvency malevolent data is referred to in the given study [7], the authors of Tang et al. [6] recommended a way to observe if the accurate position of a collection of associated vehicles by using the locations of hug vehicles. This method is known as "Secure Relative Location Determination in Vehicular Network" (SRLD) [7]. Using a state as the location of the justification methodology, Yan et al. in [8] created a method to ensure that vehicle locations are accurate. It is preferable to use an encryption technique in order to transform the location into a key (also known as a geo-lock); as a result, it is possible to increase the position error staying power in transportation networks.

2. Grid Computing and VANET

Vehicular ad-hoc network with grid computing energetically uses significant data to execute computations for solve traffic associated issues and the motive is to develop intelligent vehicles, in which vehicle prepared with wireless networking and computers can cooperate, solves the transportation problems of vehicles. V Grid, vehicles play the major responsibility mobile sensors (collecting data) and mobile routers (transmit data), also connected cooperatively to appearance of a global grid computer. High density car uses the high-density potential node to perform the distributed computations [28]. VGrid computing network ability can facilitate safety applications for vehicle driver and self-sustaining to disaster situation. Joey et al. [2] introduce proposed framework V Grid. This framework proposes the unique functional elements such that unchanging road side sensor, vehicle sensor, central management canter and variable message signs and also per pose two-line merging scenario into one.

3. Green Computing and VANET

Vehicular ad-hoc network is the category of MANET. Vehicular network moves the vehicle boundaries of wireless nodes by using sensor. Sensors sense the data and communicate one vehicle to the other vehicle. VANET basically depend on a smart cars and base stations these base stations allocate the information through the wireless nodes. Rashid et al. [4] purpose green vehicle communication Green vehicle transportations necessities are accessible to illustrate the consequence of using vehicular technology and test using NS-2 to calculate the average delay time per trip and average throughput for three different situations are existing and spotlights some major requirement for green vehicle communication [29]. In this figure the ORDC monitors and controls the operational rescue that involves multiple teams [4]. The Fig. 3 shows the operation model in green computing in vehicular environment.

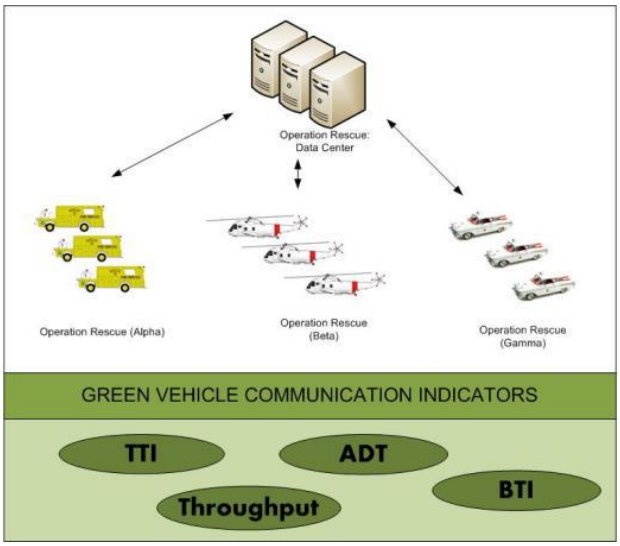

Fig. 3 Operation rescue modal [4].

Suganyal et al. [5] demonstrate a model of Authentication Structure with Restricted Privacy-Preservation and Non-Repudiation automobile way to compact with strengthens green automobile communication for urban procedures defend. Author illustrates the green computing technology on VANET using ACPN method. ACPN is the privacy conservation that contains authentication and

validity process. Catalogue some VANET challenges to show the affect future vehicle communication and much better results as compare to recent vehicles such that design of the vehicle , hardware capacity, create the new VANET technologies in markets, new wireless broadcast sachem implement , major issue is security so, so introduce the privacy models and use the beneficial technologies in VANET [30].

4. Soft Computing and VANET

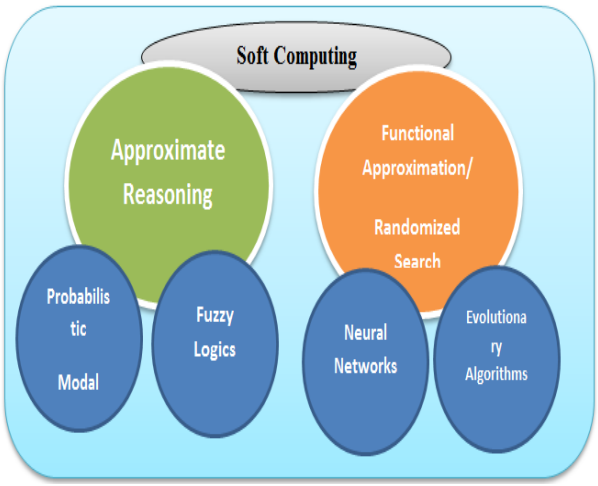

Fig. 4 Soft computing [4].

Collection of the computational techniques of the computer science is the part of the soft computing also artificial intelligent, machine learning and very complex phenomena also refer to the soft computing very low cost and computational methods [31]. Previous computational modal investigate only relatively simple system and modern complex computing include biological method, medicine, management science etc. both systems (simplicity and complexity) are relative and conventional throughput [6]. Soft computing contains residents like fuzzy sets, neural networks, and genetic algorithms [7]. The basically soft computing as instigate human nature and intelligent and Fig. 4 describes the soft computing. Soft computing is not a homogenous body is to adventure the acceptance for fuzziness and improbability to achieve the controllability.

5. Trusted Computing and VANET

In the recent years trust play vital role in the security and challenge activities and grown popularity the main component of trusted computing is the trusted computing group (TCG) the TCG improve the security in computer networks through TPM [9]. According to the A.L thorp Trust is the key security module of any system. [32] Trusted computing modules establish the trust and increase the security levels and protect the hackers. Irshad et al. [8] proposed trusted modal for vehicular ad- ad hoc networking environment. The proposed modal contains two different models. First module based on attacker and the attacks as well as second module based on trust and trusted computing technologies. Fig. 5 describes the trust and trusted model in VANET.

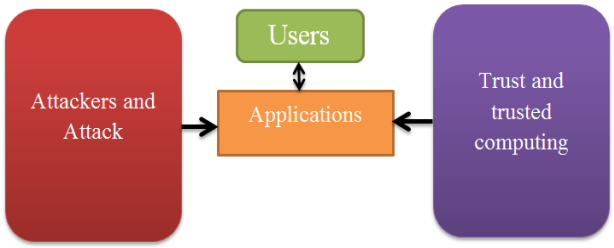

Fig. 5 VANET trust and trusted modal [10].

Irshad et al [10] introduced the proposed modal for the trusted computing Vehicular ad-hoc network. In this paper a protocol is proposed which is constructed on a property-based attestation (PBA) similarly recognized as Vehicular Property established attestation Protocol (VPP).

6. Quantum Computing and VANET

Quantum computing is the combination of the concept quantum physics and computer science these computers are more powerful and fundamental. The ability of quantum computing is to very efficiently process the algorithms which are more difficult to processing [11]. Quantum computing performance is very efficient and reliable and also Quantum computing Speculative computational system that make direct use of quantum-mechanical occurrences and its work millions of time faster and provide quick response. [33] The indication of Quantum computing is very attractive appears the quantum consequence and possibility of parallel data processing as well as the Quantum Computers prototype, demonstrates that this expertise could be used for applied application. The quantum modal of road traffic which can track the evaluation of traffic and transportable time of vehicles. Proposed modal was confirmed against the cellular automata modal. The traffic modeling contains VANET system or GPS systems. Propose

modal cellular automata traffic creates a replication environment. This modal authenticates the against cellular automata modal and openhanded equivalent result.

7. Pervasive Computing and VANET

Pervasive computing is also known as a ubiquitous computing and exists anywhere. Pervasive is an emergent tendency acquaintance with microprocessor and allowing them communicate information's. Pervasive computer hypothesis the collective computing environment also imperceptible access computer systems.

Pervasive computing trusts on the convergence of wireless technologies, advanced, electronics and the Internet. The basic idea of pervasive computing is gaining the more power and faster results time savings and perfume the action huge amount of data. These systems are the combination of collaboration among task and sentimental. Sinishibu et al. [12] build a modal automatic mobile that uses the pervasive computing behind the concept is use (VANET) vehicular ad- network. This paper illustrates Universal Computing for Automobiles and Methodology to Maximize User Suitability and Security Using VANETs. VANET provide the reliability and efficiency to transfer data. Data implement by using sensors and Ultra sound generator also provide the safer environment as compare to the older environment.

V. CONCLUSION

According to the findings of this survey report, a secure VANET is necessary for end users to connect with other end users and also with roadside units (RSU). The implementation of security in a vehicle context is made more difficult by the dynamic topology of the environment as well as the behaviour of potential attackers. There has been a significant amount of progress made in this area, but ensuring user and data safety remains a difficult challenge for the automotive sector. This article highlighted the link between the various Computing Methods and how they operate together to protect the Vehicular Ad hoc Network (VANET) from attackers and attacks. It also provided an in-depth discussion of the various Computing Methods. These computing technologies will supply novel solutions and defend against the unpredictable behaviour of an attacker in a vehicular network.

REFERENCES

[1] S. Gilani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular Ad Hoc networks," Conference Paper, 2013.

[2] R. Shringar, R. Manish, K. Nanhay, and S. Ambedkar, "Security challenges, issues and their solutions for Vanet," India International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 5, 2013.

[3] N. Siddiqui, M. Shahid Husain, and M. Akbar "Analysis of security challenges in vehicular adhoc network," in Proc. Department of Computer Science & Engineering, Integral University, Lucknow, India ACEIT, 2016.

[4] G. Samar, A. H. Wafaa, and A. Salihy, "Security analysis of vehicular Ad Hoc networks (VANET)," National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia.

[5] M. Newlin Rajkumar, M. Nithya, and P. HemaLatha, "Overview of Vanet with its features and security attacks," International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 1, 2016.

[6] R. Kruse, "Introduction to the soft computing and intelligent data analysis," in Proc. 47th Hawaii International Conference on System Science, Magdeburg: Rudolf Kruse Otto von Guericke University, 2014.

[7] A. Negi, K. V. Krishna, and K. Kishore, H. Kumar, "Performance evaluation of soft computing paradigms for collision detection and routing scheme in VANETs," International Journal of Computer Science & Information Technology Research Excellence, vol. 4, no. 3, 2014.

[8] I. Ahmed Sumra1, H. Hasbullah1, J. lail, and M. Rehman, "Trust and trusted computing in VANET," Research Gate, vol. 1, no. 1, April 2011.

[9] A. L. Thorp, "Attestation in trusted computing: challenges and potential solutions," Technical Report, 2010. [Online]. Available: http://www.rhul.ac.uk/mathematics/techreports

[10] I. Sumraa, H. Hasbullaha, J. Mananb, I. Ahmadc, and M. Y. Aalsalemd, "Trusted computing in vehicular ad hoc network (VANET)," Computer Science Journal, vol. 1, pp. 928-933.

[11] M. Bernas and J. Wisniewska, "Quantum road traffic model for ambulance travel time

estimation," Journal of Medical Informatics & Technologies, vol. 22, pp. 257-264, 2013.

[12] S. Shibu1 and S. Jain2, "Pervasive computing for automobiles: An approach to maximize user convenience and safety using VANETs," International Journal of Computer and Electrical Engineering, vol. 2, no. 6, 2010.

[13] V. Prakaulya, N. Pareek, and U. Singh, "Network performance in IEEE 802.11 and IEEE 802.11p cluster based on VANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212713.

[14] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun 121, 503–526 (2021). https://doi.org/10.1007/s11277-021-08647-1

[15] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[16] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[17] U. Singh, M. Shukla, A. K. Jain, M. Patsariya, R. Itare, and S. Yadav, Trust Based Model for Mobile Ad-Hoc Network in Internet of Things, vol. 98. 2020.

[18] M. Muwel, P. Mishra, M. Samvatsar, U. Singh, and R. Sharma, "Efficient ECGDH algorithm through protected multicast routing protocol in MANETs," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212743.

[19] U. Singh, V. Vankhede, S. Maheshwari, D. Kumar, and N. Solanki, Review of Software Defined Networking: Applications, Challenges and Advantages, vol. 98. 2020.

[20] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[21] V. K. Saurabh, R. Sharma, R. Itare, and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212712.

[22] A. S. Chouhan, V. Sharma, U. Singh, and R. Sharma, "A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212740.

[23] L. Baghel, P. Mishra, M. Samvatsar, and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212741.

[24] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[25] A. Sharma, D. Bhuriya, and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375688.

[26] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570906.

[27] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212719.

[28] D. Wagh, N. Pareek, and U. Singh, "Elimination of internal attacksfor PUMA in MANET," in Proceedings of the International Conference on

Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212710.

[29] R. Parihar, A. Jain, and U. Singh, "Support vector machine through detecting packet dropping misbehaving nodes in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212711.

[30] S. Waskle, L. Parashar and U. Singh, "Intrusion Detection System Using PCA with Random Forest Approach," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 803-808, doi: 10.1109/ICESC48915.2020.9155656.

[31] A. Bhawsar, Y. Pandey and U. Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 809-814, doi: 10.1109/ICESC48915.2020.9156009.

[32] S. Nihale, S. Sharma, L. Parashar and U. Singh, "Network Traffic Prediction Using Long Short-Term Memory," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 338-343, doi: 10.1109/ICESC48915.2020.9156045.

[33] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08647-1