Recent Security Solutions For VANET Communications: A Systematic Review

[1]Megha V Kadam*,[2]Dr.Vinod M Vaze, [3]Dr.Satish R Todmal,

[1]Research Scholar, Shri.JJT University, Churella, Jhunjhunu(Rajasthan), megha.desai1@gmail.com
[2]Professor and Ph.D guide, Shri.JJT University, Churella, Jhunjhunu(Rajasthan), vinod.vaze@gmail.com
[3]*Ph.D guide,* Shri.JJT University, Churella, Jhunjhunu(Rajasthan), srtodmal@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract- In wireless network which is now widely deployed in urban areas for intelligent transport system (ITS) called Vehicular Ad Hoc Networks (VANETs). Due to the open nature of VANETs, they are vulnerable to various security threats as such networks are mainly depends on control, communication and computing technologies. The fault or malicious vehicles in VANET may lead to serious accidents and public assets lost due to miscommunications based on vehicle sensor data. Therefore, if the detection of such sensor data is not effectively handled then it may lead to traffic jams, road accidents, etc as most of the vehicles wrongly redirected by face traffic alerts. Thus providing reliable communications among the V2V or V2I is the first research problem. There are different security solutions presented to achieve the efficient an reliable VANET communications under the domain of cryptography, trust-based, and hybrd. The aim of this paper is to take the review such recent works for network security. The outcome of this paper claims the various research gaps identified from the literature review.

Keywords- Cryptography, Trust based, Routing, Vehicular Ad Hoc Networks, Security, Reliabiltiy.

I. INTRODUCTION

The With the wide use of the savvy transportation framework (ITS) and the course of action of remote correspondence movements, vehicular off the cuff frameworks (VANETs), as the colossal piece of ITS, have happened to focal giganticness in the present flood hour gridlock the board. VANETs give in a surprising manner relationship for drivers and connect with them to display touchy traffic information to various drivers, for instance, scene avoiding cautions, condition conditions and state of vehicles, which can improve traffic board capacity and flourishing. In any case, with the comprehensive shared traffic information and the more sorts of utilization customers need, for instance, in-vehicle media distraction, vehicular long range nice correspondence and territory based affiliations, a single vehicle has compelled estimation and most distant point resources, which prompts oblivious planning limit [1]. Starting late, a few examinations have proposed the probability of vehicular conveyed figuring (VCC) that solidifies cloud and VANET. VCC is another viewpoint that conspicuously effects traffic the board and street flourishing [2] and it has been made to vanquish the burdens in VANET. These days, VCC is considered as the key measure to improve and develop ITS [3]. Oraliu et al. [4] first proposed the probability of self-overseeing vehicular fogs (AVCs). In AVCs, different vehicles with unlimited resources are viewed as ace systems [5]. This is a social affair of, everything viewed self as, adequate vehicles that contribute their figuring, perceiving, correspondence, and physical resources for the cloud. Vehicles' focal points and the information exchanged from the vehicles with the cloud can be used by various vehicles in fundamental association [6]. There are two modes in AVCs, zero-establishment vehicular fogs, and structure based vehicular fogs. The basic mode can give a powerfully determined correspondence structure because of the high convenientce of interstate vehicle focus focuses, which prompts the shy of framework correspondence time and the loss of assigned assets. In light of this, this paper is essentially rotated around the zero-structure self-ruling vehicular mists, which couple of specialists have considered. Furthermore, it is sensibly amazing to appropriate keys of vehicles because of the run of the mill for zero-foundation vehicular mists [7]. Hence, an able and secure key association appear, which can oversee dynamic get-togethers and outfit endorsement comparatively as gathering with less figuring and correspondence overhead is basic. In the examination of AVCs, most examinations basically center around the security challenges [2,3,7,8], the arrangement what's more, traffic stream control [1,9–13], Besides, among these present shows in the a dynamic framework, a colossal portion of them have would in general check yet dismissal to propose an assertion similarly as secret show. In this paper, as appeared by the dangers in AVCs, we propose a profitable what's undeniably, secure key transport show to guarantee secure correspondence and the course of action of the traffic data in AVCs. The basic obligations gave are as indicated by the going with: The proposed key affiliation show relies on the Chinese Reminder Theory (CRT) and affirmations open key cryptography (CLPKC) [14], which supports an essentially secure and gainful attestation and solicitation in AVCs. The colossal central purposes of the show are that reestablishing keys during the customers' join and leave exercises are performed beneficially. Also, it grasps the underwriting the official's issue in the open key structure (PKI) [15]. With execution examinations, this proposed show gets a promising result from a predominant exchange off among limit and security than other current plans explored in the sythesis. This show is considered as an unequaled change in AVCs.Review of Trust-based and Cryptography based Routing Solutions for Vehicular Ad Hoc Networks (ITS) and the grouping of remote correspondence pushes, vehicular without any preparation structures (VANETs), as an essential bit of ITS, have happened to fundamental significance in present-day traffic the board. VANETs give entrancing relationship for drivers and connect with them to offer delicate traffic information to various drivers, for instance, trouble avoidance alarms, condition conditions and state of vehicles, which can improve traffic the official's advantage and flourishing. In any case, with the all-inclusive shared traffic data and the more sorts of occupations clients need, for example, in-vehicle keen media diversion, vehicular individual to singular correspondence and region based associations, a solitary vehicle has constrained estimation and cutoff assets, which prompts ignorant preparing limit [1]. Starting late, a couple of examinations have proposed the probability of vehicular circulated processing (VCC) that joins cloud and VANET. VCC is another point of view that clearly effects traffic the heads and street security [2] and it has been made to crush the drawbacks in VANET. These days, VCC is considered as the key measure to improve and develop ITS [3]. Oraliu et al. [4] first proposed the probability of autonomous vehicular fogs (AVCs). In AVCs, different vehicles with unfathomable resources are viewed as ace systems [5]. This is a get-together of, so to speak, self-overseeing vehicles that contribute their preparing, seeing, correspondence, and physical resources for the cloud. Vehicles' great conditions and the information exchanged from the vehicles with the cloud can be used by various vehicles in essential movement [6]. There are two modes in AVCs, zero-establishment vehicular fogs, and structure based vehicular fogs. The fundamental mode can give an intelligently unflinching correspondence structure because of the high minimization of road vehicle focuses, which prompts the shy of framework correspondence time and the loss of doled out assets. In light of this, this paper is essentially rotated around the zero-framework self-ruling vehicular mists, which a few analysts have pondered. With the wide utilization of AVCs, the importance of security is moreover on the trek. An irrefutably cautious examination reveals that endless the outstanding security burdens are exacerbated by the trademark features of AVCs [7]. Furthermore, it is consistently amazing to scatter keys of vehicles by ethicalness of the ordinary for zero-establishment vehicular fogs. In like manner, a gainful and secure key affiliation show up, which can arrange excellent gatherings and outfit underwriting correspondingly as riddle with less figuring and correspondence overhead is basic. In the examination of AVCs, most examinations essentially center around the security challenges [2,3,7,8], the structuring what's more, traffic stream control [1,9–13], yet in the sythesis, only a few examinations have kept an eye on a particular reaction for these security challenges in AVCs. In addition, among these present shows in the a dynamic framework, a colossal fragment of them have kept an eye on assertion at any rate dismissal to propose an affirmation similarly as security appear. In this paper, as appeared by the hazards in AVCs, we propose a gainful in like manner, secure key dispersal show to guarantee secure correspondence and the insurance of the traffic data in AVCs. The fundamental obligations gave are as per the going with: The proposed key affiliation show relies on the Chinese Reminder Theory (CRT) and certificateless open key cryptography (CLPKC) [14], which supports a safe and reasonable confirmation and puzzle in AVCs. The genuine central purposes of the show are that strengthening keys during the customers' join and leave exercises are performed adequately. Furthermore, it comprehends the request the board issue in the open key establishment (PKI) [15]. With execution appraisals, this proposed show gets a promising result from a dominating exchange off among capability and security than other current plans discussed in the piece. This show is considered as an unavoidable change in AVCs.Review of Trust-based and Cryptography based Routing Solutions for Vehicular Ad Hoc Networks.

Section II presents a review of recent methods. Section III presents the comparative study and research gaps. Section IV presents the conclusion and future work

II. Literature Review

In this section, we present of trust based and cryptography based routing solutions for vehicular ad hoc networks. The systematic review of the cryptography based and trust based routing solution for VANET are as following.

A. *Cryptography Based Methods*

In [16], Dhanya and Dr.L.Pavithira propose an enhance the existing unsaturated VANET cluster model with Security implementation using keyed-Hash Message Authentication code technique introduced the security model using Keyed-Hash Message Authentication technique making the VANET model full designed well.

In [17], Alhan, An., and Chawla using OPNET multiplication instrument for the show of Data Gather based (DGRP) guiding show, build a standard for the multifaceted design of the Vehicle Ad-Hoc framework zone similarly as apply the encryption on data or packs and after that strategy the five-arrange come in this framework zone

In [18], Yeh, L.- Y., Chen, Y.- C., and Huang propose an Attribute-Based Access Control System (ABACS) for crisis administrations with security affirmation over Vehicular Ad Hoc Networks (VANETs). ABACS plans to improve the proficiency of salvages prepared by means of crisis interchanges over VANETs. ABACS could choose crisis vehicles that could most fittingly manage a crisis and safely delegate the specialist to control traffic offices to the alloted crisis vehicles. Utilizing epic cryptographic primers, ABACS acknowledges secrecy of messages, aversion of arrangement assaults, and fine-grained access control

In [19], Chim, T. W., Yiu, S. M., Hui, L. C. K., and Li, V. O. K, propose the VANET-based Secure and Privacy-protecting Navigation (VSPN) Author exhibited the route conspire that used the online street data gathered by a vehicular impromptu system (VANET) to direct the drivers to wanted goals in a continuous and disseminated way. The proposed plan has the benefit of utilizing constant street conditions to register a superior course and in the meantime, the data source could be appropriately validated.

In [20], Jiang, S., Zhu, X., and Wang, L, Author present a productive unknown group confirmation plot (ABAH) to supplant the CRL checking process by ascertaining the hash message validation code (HMAC). The region into a few areas, wherein street side units (RSUs) oversee vehicles in a restricted way. They embrace nom de plumes accomplish security protecting and acknowledge bunch validation by utilizing a personality based mark (IBS). At long last, They use HMAC to stay away from the tedious CRL checking and to guarantee the uprightness of messages that may lose all sense of direction in past group validation.

In [21],Shen, J., Wang, C., Castiglione, A., Liu, D., and Esposito, creator propose a novel directing convention named dependability assessment based steering convention (TERP). In our convention, the reliability of every individual were determined by the cloud contingent upon the quality parameters transferred by the relating vehicle. Likewise, as indicated by the dependability given by the cloud, vehicles in the system pick solid forward hubs and complete the whole course. The investigation depicted that our convention can viably improve the decency of the reliability judgment.

In [24], creator proposed systems for area uprightness extend from the utilization of locally available radar gadgets and GPS to more straightforward strategies that depend on data combination. They likewise address approaches to upgrade the accessibility of area data by choosing and keeping up stable steering ways.

In [25], Author utilizing gathering/ring marks, pseudo-personality based and PKI-based methodologies have been proposed to accomplish very successful protection saving validations. They send the nom de plume component over the roadside units so as to help decentralized common personality confirmation and proprietorship approval of vehicles, in an approximately coupled or a compound way. These structures gave thorough Level 3 security and raceability of vehicles.

B. Trust Based Methods

In [22], author utilizing trust the board framework. In the framework, fluffy rationale were utilized to define loosely observational learning. Together with fluffy rationale, chart hypothesis were received to construct a novel trust model for ascertaining hub trust esteem. To shield against expanding assaults to confide in the executives frameworks, for example, criticizing and harboring, we propose a separating algorithm. A productive reliability rot strategy was additionally intended to determine the contention about rotting authentic trust an incentive in trust-based steering choice. Furthermore, They present a doable trust factor gathering way to deal with guarantee the trust the executives framework were perfect with other security natives, for example, encryption and epitome.

In [26] Tan, S., Li, X., and Dong, Q. (2016), Author introduced to an effective reliability rot technique is additionally intended to determine the contention about rotting chronicled trust an incentive in the trust-based steering choice. They executed the proposed sifting algorithm and trust the executives framework by incorporating it into the upgraded connection state directing (OLSR) convention.

In [27] Li, W., and Song, H. (2016), creator actualized proposed assault safe trust the board conspire (ART) for VANETs that ready to identify and adapt to pernicious assaults and furthermore assessed the dependability of the two information and versatile hubs in VANETs.

In [28], In this paper displayed a trust-based appropriated the verification (TDA) technique that depends on a worldwide trust server and vehicle conduct for maintaining a strategic distance from impact assaults were proposed. This technique guarantees both between vehicular and intra-vehicular correspondence security in the system. Moreover, a channel state directing convention (CSRP) implied proposed to improve correspondence unwavering quality among the vehicles. Solid vehicles did distinguished by the locally available unit (OBU) vitality and the channel condition of the vehicle to convey consistent correspondence. Some Internet of Things (IoT) related works also reviewed for VANETs [29-32].

In this area present writing survey of the cryptography based and trust based steering answer for VANET. In next segment relative examination on different strategies and parameters to accomplish the exhibition of framework.

III. COMPARATIVE ANALYSIS

References	Year	Methodology	Performance Metrics	Index Terms
[23]	2014	new trusted directing	accomplished	geographic DTN

		convention in VANET dependent on GeoDTN+Nav by utilizing trust the executives model of Bayesian and the three entrepreneurial steering sending models,	great execution in the evacuation proportion of noxious hubs, right gathering proportion of parcel and the message payload	steering with pilot forecast; trust the executives; trust directing
[19]	2014	VANET-based Secure and Privacy-safeguarding Navigation (VSPN) plot and the vehicular system comprises of on board units (OBUs) introduced on vehicles, street side units (RSUs) along the streets, and confided in power (TA).	the course prompts reserve funds of up to 55% of the voyaging time contrasted and the disconnected guide information looking through methodology. This plan additionally gives a lower course blocking rate by and by. Note that our VSPN plan could apply to the circumstance where the course the looking	secure vehicular sensor network, anonymous credential, proxy re-encryption

			through procedure is finished by a focal server, which gathers and confirms speed information and street conditions from RSUs.	
[17]	2015	OPNET amusement gadget for the introduction of Data Gather based (DGRP) guiding show, collect a standard for the multifaceted design of the Vehicle Ad-Hoc framework zone similarly as apply the encryption on data or packages and after that strategy the five-mastermind come in this framework zone	DGRP (Data Gather Based outing show) has better execution in the term of interruption or delay and the total traffic sent and got. they coordinating traffic sent and got the amount of encoded packages and bit structure.	VANET, DGRP, OPNET 14.5 tool
[22]	2016	Propose the separating calculation and trust the executives system In the system, fluffy rationale is utilized to define loosely exact	Simulation results show that the proposed trust management system works well in detecting	Trust management, trust model, ad hoc networks, data plane security

		information, which is utilized to assess way trust esteem. Together with fluffy rationale, diagram hypothesis is received to assemble the novel trust model for computing hub trust esteem. A productive dependability rot strategy is additionally intended to determine the contention about rotting chronicled trust an incentive in the trust-based steering choice.	and resisting data plane attacks.	
[16]	2016	A keyed-Hash Message Authentication Code (HMAC), where the key pre-claimed in controlling the HMAC is common just between non-revoked On-Board Units (OBUs). In expansion, HMAC utilizes a creative probabilistic key sharing model, which engages non	The calculation multifaceted nature of EMAP is O(1), which is steady and autonomous of the quantity of repudiated testaments. At the end of the day, EMAP has the most reduced	Vehicular networks, message authentication, communication security.

		disavowed OBUs to resistance share and redesign a mystery key.	calculation multifaceted nature contrasted and the CRL checking procedures utilizing direct and twofold inquiry calculations. HMAC is demonstrated to be secure and proficient.	
[20]	2016	A proficient unknown bunch verification conspire (ABAH) to supplant the CRL checking process by computing the hash message validation code (HMAC).	The security and execution investigation is completed to show that ABAH is more productive as far as confirmation delay than the regular verification techniques utilizing CRLs. ABAH has preferable execution over the pen name	Certificate Revocation Lists (CRLs), hash message authentication code (HMAC).

			confirmation plans.	
[21]	2017	To epic directing convention named dependability assessment based steering convention (TERP). In our convention, the dependability of every individual is determined by the cloud contingent upon the property parameters transferred by the comparing vehicle.	TERP convention has a decent presentation as far as the parcel conveyance proportion, standardized steering overhead, and normal start to finish delay.	Trustworthiness Evaluation, Routing Protocol

IV. RESEARCH GAPS

From the above writing survey, we saw some examination holes so as to structure and study reveiw of trust based and cryptography based directing answers for vehicular impromptu systems. According to the advancement of research in this space, we recorded the examination issues.

- The steering issues in VANET far reaching dissected and incorporated the VANET bunch model with Security demonstrating utilizing keyed-Hash Message Authentication code procedure, while security requirements come up short on the system a completely fledged VANET model.
- Vehicles are not impeccable because of high parcels misfortune rate correspondence among. Vehicular specially appointed systems are imparting between one another as well as getting data and sending or accepting information to association units.
- Because of the hub of vehicular specially appointed systems have the qualities of high versatility and experience transitory, a trust the executives between the hubs in the steering procedure turns out to be progressively troublesome.
- The verification and protection saving, our plan satisfies all other vital security necessities. To secure the protection of the drivers, the inquiry (goal) and the driver who issues the a question is destined to be unlinkable to any gathering includingthe confided in power.
- In vehicular impromptu systems (VANETs), Large correspondence sources, extra room, and checking time are required for CRLs that reason the security revelation.
- Due to the qualities, for example, receptiveness and dynamic topology, specially appointed systems experience the ill effects of different assaults on the information plane. Much more terrible, a few assaults can subvert or sidestep the regularly get personality based security systems.

V. CONCLUSION AND FUTURE WORK.

Soon, it is normal that Vehicular specially appointed systems will send in various nations. The security of such systems is fundamental since individuals' lives might be in question because of it. In this paper, we have examined this issue has specific prerequisites. We likewise portray various sorts of dangers that are conceivable in vehicular specially appointed systems. We likewise survey the writing on a few security issues explicitly identified with VANETs. These security issues make a potential hindrance to send VANETs. This paper displayed a survey of trust based and cryptography based steering answers for vehicular impromptu systems exhaustive security convention and furthermore talked about a structure that covers all security parts of

VANET. We displayed the examination and relative investigation of late examinations. The result of this paper guarantees the different research holes recognized from the writing survey.

REFERENCES

1. Yu, R.; Zhang, Y.; Gjessing, S.; Xia, W. Toward cloud-based vehicular networks with efficient resource management. IEEE Netw. 2013, 27, 48–55.
2. Kong, Q.; Lu, R.; Zhu, H.; Alamer, A.; Lin, X. A Secure and Privacy-Preserving Incentive Framework for Vehicular Cloud on the Road. In Proceedings of the Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
3. Ahmed, Z.E.; Saeed, R.A.; Mukherjee, A. Challenges and Opportunities in Vehicular Cloud Computing. In Vehicular Cloud Computing for Traffic Management and System; Grover, J., Vinod, P., Eds.; IGI Global: Hershey, PA, USA, 2018; pp. 57–74. ISBN 13 9781522539810.
4. Olariu, S.; Eltoweissy, M.; Younis, M. Towards autonomous vehicular clouds. EAI Endorsed Trans. Mob. Commun. Appl. 2011, 11, e2.
5. Alamer, A.; Deng, Y.; Lin, X. Secure and privacy-preserving task announcement in vehicular cloud. In Proceedings of the International Conference onWireless Communications and Signal Processing, Nanjing, China, 11–13 October 2017; pp. 1–6.
6. Lim, K. Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-Based Architecture for Vehicular Cloud. Ph.D. Thesis, University of Kentucky, Lexington, KY, USA, 2016.
7. Yan, G.; Wen, D.; Olariu, S.; Weigle, M.C. Security challenges in vehicular cloud computing. IEEE Trans. Intell. Transp. Syst. 2013, 14, 284–294.
8. Sensors 2018, 18, 2896 27 of 28 8. Rajeshwari, P. A Survey on Security challenges in Vehicular cloud computing. Int. J. Sci. Res. Educ. 2016, 4, 4848–4853.
9. Ahmad, I.; Noor, R.M.; Ali, I.; Qureshi, M.A. The Role of Vehicular Cloud Computing in Road Traffic Management: A Survey. In Proceedings of the International Conference on Future Intelligent Vehicular Technologies, Islamabad, Pakistan, 17–19 October 2017; pp. 123–131.
10. Sookhak, M.; Gani, A.; Buyya, R. A survey on vehicular cloud computing. J. Netw. Comput. Appl. 2014, 40, 325–344.
11. Wan, J.; Zhang, D.; Zhao, S.; Yang, L. Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions. Commun. Mag. IEEE 2014, 52, 106–113.
12. Chi, W.D.; Ru, L.I.; Fan, P.F. Research on the Checkpoint Server Selection Strategy Based on the Mobile Prediction in Autonomous Vehicular Cloud. In Proceedings of the International Conference on Service Science, Technology and Engineering, Suzhou, China, 14–15 May 2016; pp. 262–267.
13. Hussain, R.; Son, J.; Eun, H.; Kim, S.; Oh, H. Rethinking Vehicular Communications: Merging VANET with cloud computing. In Proceedings of the IEEE International Conference on Cloud Computing Technology and Science, Bristol, UK, 2–5 December 2013; pp. 606–609.
14. Al-Riyami, S.S.; Paterson, K.G. Certificateless Public Key Cryptography; Springer: Berlin, Germany, 2003; pp. 452–473.
15. Diffie, W.; Hellman, M.E. New directions in cryptography. IEEE Trans. Inf. Theor. 1976, 22, 644–654.
16. Dhanya and Dr.L.Pavithira "A Secure Cluster based VANET Modelling System with keyed Hash Message Authentication Code",International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 23 Issue 5 –SEPTEMBER 2016.
17. Alhan, A., & Chawla, M. (2015). Analysis of Encryption Dgrp-Data Gather Routing Protocol Based on Opnet in VANETs. 2015 International Conference on Computational Intelligence and Communication Networks (CICN). doi:10.1109/cicn.2015.207
18. Yeh, L.-Y., Chen, Y.-C., & Huang, J.-L. (2011). ABACS: An Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, 29(3), 630–643. doi:10.1109/jsac.2011.110312
19. Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, V. O. K. (2014). VSPN: VANET-Based Secure and Privacy-Preserving Navigation. IEEE Transactions on Computers, 63(2), 510–524. doi:10.1109/tc.2012.188
20. Jiang, S., Zhu, X., & Wang, L. (2016). An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs. IEEE Transactions on Intelligent Transportation Systems, 17(8), 2193–2204. doi:10.1109/tits.2016.2517603
21. Shen, J., Wang, C., Castiglione, A., Liu, D., & Esposito, C. (2017). Trustworthiness Evaluation-based Routing Protocol for Incompletely Predictable Vehicular Ad hoc Networks. IEEE Transactions on Big Data, 1–1. doi:10.1109/tbdata.2017.2710347

22. Huang, Z., Ruj, S., Cavenaghi, M.A. *et al.* A social network approach to trust management in VANETs. *Peer-to-Peer Netw. Appl.* **7,** 229–242 (2014). https://doi.org/10.1007/s12083-012-0136-8
23. Wu, Q., Liu, Q., Zhang, L., & Zhang, Z. (2014). A trusted routing protocol based on GeoDTN+Nav in VANET. China Communications, 11(14), 166–174. doi:10.1109/cc.2014.7085617
24. Yan, G., Olariu, S., & Weigle, M. (2009). Providing location security in Vehicular Ad Hoc networks. IEEE Wireless Communications, 16(6), 48–55. doi:10.1109/mwc.2009.5361178
25. Sun, C., Liu, J., Jie, Y., Ma, Y., & Ma, J. (2018). Ridra: A Rigorous Decentralized Randomized Authentication in VANETs. IEEE Access, 1–1. doi:10.1109/access.2018.2868417
26. Tan, S., Li, X., & Dong, Q. (2016). A Trust Management System for Securing Data Plane of Ad-Hoc Networks. IEEE Transactions on Vehicular Technology, 65(9), 7579–7592. doi:10.1109/tvt.2015.2495325
27. Li, W., & Song, H. (2016). ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 960–969. doi:10.1109/tits.2015.2494017
28. King Saud University, Deanship of Scientific Research, Community College Research Unit" Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs " date of current
29. Mahajan, H.B., Badarla, A. & Junnarkar, A.A. (2020). CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02502-0.
30. Mahajan, H.B., & Badarla, A. (2018). Application of Internet of Things for Smart Precision Farming: Solutions and Challenges. International Journal of Advanced Science and Technology, Vol. Dec. 2018, PP. 37-45.
31. Mahajan, H.B., & Badarla, A. (2019). Experimental Analysis of Recent Clustering Algorithms for Wireless Sensor Network: Application of IoT based Smart Precision Farming. Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 9. 10.5373/JARDCS/V11I9/20193162.
32. Mahajan, H.B., & Badarla, A. (2020). Detecting HTTP Vulnerabilities in IoT-based Precision Farming Connected with Cloud Environment using Artificial Intelligence. International Journal of Advanced Science and Technology, Vol. 29, No. 3, pp. 214 - 226.