International Journal of Computer Science Trends and Technology (IJCST) – Volume 8 Issue 4, Jul-Aug

RESEARCH ARTICLE OPEN ACCESS

A Survey on Intelligent Transportation Security Systems

Mr. B. Subhash

Assistant Professor, Department of Computer Science and Engineering
Sasi Institute of Technology & Engineering
Tadepalligudem, Andhrapradesh, India

ABSTRACT

Enabling intelligence is an important part of the transportation system. Attacks on transport infrastructure are limited, but the risk of cyber-attacks increases if more vehicles are added, so the intelligent transport system (ITS) must be protected for separate vehicles and public transport. The security of this system is essential for safe and efficient transportation. Measures can be taken to eliminate system vulnerabilities, eliminate threats from outside the system, and reduce the risk of ITS attacks. The purpose of this study is to provide an overview of ITS security issues and the solutions applied to prevent and / or overcome ITS security breaches. We provide assistance on best practices for ITS protection and the implementation of security programs.
Keywords: Attacks, authorization, Intelligent Transportation Systems,biometrics, protection methods, and security.

I. INTRODUCTION

Communication and information knowledge play ansignificant role in visitor structures and traffic control[1]. Intelligence should be incorporated into the transportation and management systems of site visitors to develop the safety[2], efficiency and longevity of the transportation network, lessen congestion and improve driver practice[3]. The combination of intelligence, facts and communication technology leads to IT[4]. As this additional technology is auxiliary to the traffic and traffic control structures, the surface area is increased for an attack. This upsurges the need to protect him[5].

The idea of cyber security is applied in many areas[6]. Given the damage caused by these attacks, it is important to eliminate vulnerabilities in the structure, eliminate exterior threats to the system and lessen the risk of attacks on funds. [7] The document facilitates the review of security incidents and their responses regarding the security of intelligent transport structures. According to our review of the literature[8], limited research can be done on cyber security threats to ITS. This overview will look at the factors influencing the difficult ITS security situation and the answers to these problems[9]. There are many types of ITS security breach opportunities, and the general answer cannot be used for all general structures[10]. Our article will investigate solutions and learn the importance of the next solution step.

II. BACKGROUND

With the increase in the number and density of vehicles, technological advances have established a new way of controlling traffic[11]. ITS applies this technology to Progress Avenue Transportation. Information obtained from sensors and apparatus in cars and infrastructure[12]. These records can be used to improve modern transportation facilities[13].

The protection of roads and visitors, the efficiency of site visitors and the introduction of value-added applications all aim to improve the transport system[14]. The info is used to decrease the risk of vehicle injury and to limit the injury caused by inevitable accidents[15]. The packages used to improve traffic efficiency are intended to increase the flow of site visitors through support to reduce travel times and vehicle fears[17]. Value-added applications include infotainment systems[16], travel information, and Internet access[18]. ITS requires wireless communication between and among vehicles and the road infrastructure. ITS research can be very active and diverse in more than one department[19]. The technology used in vehicle and transport management is evolving and improving[20].

III. RATIONALE

ITS security is important as the latest technologies are developed and developed in the transport sector[21]. Due to the uncertainty of the technology, it will be easier for attackers to stop ITS. Different smart and traffic management methods use progressive ITS services for intelligent traffic networks[22]. IT is critical to building an intelligent city, and attacking such a system can create extreme conditions for city traffic[23]. IT is also an integral part of people's vehicles for security and luxury[24]. ITS has a wide range of applications and increases the importance of public transport[25]. These applications process and exchange facts to improve traffic based on the

environmental impact of the river, control of site visitors, and conveyance systems[26]. The skill is used in people's engines to connect info about a car to various vehicles in the nearby and distant infrastructure. This is because the age in the car has improved[27].

The creation of all of these technologies to ensure safety in public transport as well as in public transport is a growing number of important factors as the era for transport expands and evolves[28]. Most of the current research creates packages of intelligent traffic systems, not cybersecurity components[29]. There are limited assessments on the security of these ITS and system attacks[30]. More recent works evaluates the complex IT security situation in ITS. Our document compares unique security methods in ITS[31]. There is limited investigation into solutions and solutions related to cyber attacks to prevent such attacks on ITS[32].

IV. SECURITY CHALLENGES

It is significant to select risk participants for intelligent transport systems. Information from other countries, criminal gangs, hacktivists, cyber terrorists, insiders, dishonest operators and natural bugs have been labelled as the potential for attackers for ITS[33]. Nation states use spyware and malware software tools that are specifically designed to obtain information about their purposes[34]. This type of attack is aimed at stealing intellectual property a competitive advantage. For example, the country's ITS infrastructure could be threatened by another country throughout the war[35]. Hacking groups and resources may be under the direct control of the country or may be transferred to third parties to support potential failures[36]. Criminal gangs use unique systems to hack ITS and generate illegal sales. It wants to use the infrastructure of ITS to draw attention to political objectives and to achieve these objectives[37]. Highway bulletin boards can be hacked to promote political issues. Cyber terrorists attacked items to destroy, destroy and spread terror. Insiders attack the employer who currently owns or participates in it, while insiders attack the public-non-activities[38].

There are multiple motives behind this attack. Innocent operators to avoid traffic, destructive competitors to attack IT to avoid fines and costs[39]. Natural disruptions are also a threat to ITS. Natural disasters can lead to mechanical failures that destroy IT infrastructure. Most cyber attacks are motivated by money[40]. HIS structures are unique in that they look beautiful and have a great impact when they attack structures. This form can be the main motivator[41]. Their targets are ransom, record robbery, war record, equipment theft, theft, or revenge, and terrorism[42]. Facts can be obtained through physical, wireless or network attacks. Attacks can be initiated by one or two vectors. Encrypted facts and systems are attacked during a lethal ransom attack. Decryption keys will not be issued without a ransom[43]. The attacker can gain access to the accompanying vehicle and deactivate the operation until a ransom is paid[44]. The safety of this vehicle may be compromised[45]. Stolen statistics can be used to expand targets. The states of the country and their dishonest rivals are the most aggressive type of thieves. Personal gain is plunder[46]. Rejecting service attacks on infrastructure involves information warfare. This can lead to system failure and road crashes. It can also be used to post political views, protests and rallies[47]. This can ruin the reputation of the employer and lead to financial loss. Sending a fake car message (V2V) can cause road accidents. This attack can cause V2V write poisoning. Map hacking can also be used to compromise local transmitters, GPS receivers, and spoof GPS signals[48]. The system of games and thefts involves the theft of goods from the passenger compartment or the theft of the entire vehicle. They are used to avoid paying system fees and costs for the services of a telecom operator[49]. Autonomous vehicles can be hacked to indicate remote areas where valuables, automotive components, whole vehicles or theft are possible. Payment operators can avoid using ITS[50].

Mobile infrared transmitters (MRT) can gently transfer visitors to a computer-controlled site using a remote activator[51]. An enemy vehicle can be hacked to stop the competition and make cars inaccessible. There may be a situation where free cars want to free a compromised car that receives too much attention[52]. Orders of fake securities can be charged to suspicious customers. Revenge and terrorism are another model used to attack ITS and is one of the most serious and deadly attack vectors[53]. Driving in the car can be stolen and used as a weapon. It is very difficult to predict and protect against these attack methods[54]. Through flow control mechanisms, traffic can be stopped, ITS security structures can be disabled, roadside alarm structures can be implemented and strategic resources can be left online, jeopardizing the organization's operations and personal staff[55]. Hacking ITS systems The ITS gadget is commonly used as an access point to the ITS environment. An attack on an ITS gadget offers access to an ITS environment connected to the Internet or VPN[56]. Getting the right to deep community access requires little effort. Attacks can be excluded from the community when an attacker gains access to the network[57]. Physical attacks are easy because the ITS road infrastructure is open. It can be physically connected to open doors. The device can be retrieved by pressing by entering brute force or credentials[58]. The topology can be monitored by scanning a protected or closed network. Deleting documents can detect your device or machine[59].

The firmware can be connected to restore credentials and configuration. Human attacks in the middle intercept data about the use of open cables or cables and can send false records to internal servers. The tool can be modified to remove loan or compromise data. Malicious software can be installed from a removable storage device[60]. Wrong commands can be sent to internal servers and the controller. The corporate community can be accessed using the enhanced tool and ITS as an access factor you can rely on. Software vulnerabilities could be exploited. In

addition, devices can be hacked or manipulated due to abuse of authority by operators. Wireless attacks pose a major risk to IT security for ITS infrastructure. You can send messages with speakers, receive Wi-Fi transmissions, transmit and connect malicious firmware, wireless transmissions and vehicle protection systems can be blocked electronically, "middle type" attacks can be intercepted and control In fact, vulnerabilities can be exploited and Wi-Fi can be used to access the controller network bus (CAN) and the built-in diagnostic, information and control unit. Telematics. The CAN bus can be compromised by remote hijacking, and harmful applications can be installed for the third day of birth. Network attacks are possible due to the fact that ITS facilities are open on the Internet and are detected when they enter the IoT, which makes them susceptible to cyber attacks. Incorrect device configurations are identified and abused. Software and hardware vulnerabilities are exploited. The device can be detected remotely and misused. Malware and / or adware can be connected to systems. Targeted attacks are possible, which can be sponsored by the government and continuous advanced threats. Malicious firmware can be downloaded and installed. Distributed courier denial of service (DDoS) attacks can be launched on ITS infrastructure and back-end servers that can be detected on the Internet. Harmful scriptures can be introduced as advertisements. Risks to ITS may include online scripts on websites (XSS) where malicious script is posted to the community. Structured Query Language (SQL) injection is one of the most common hacking techniques on the Internet. Session involves the use of a legitimate PC session[61].

Call servers that enter the wrong IP address include DNS hijacking and hijacking. Eliminates malware infiltration of frequently used websites in the community. Hash attacks occur when a user's credentials are stolen and reused in a face-to-face community to go to the device to verify that the session is valid. Passport attacks are used to move around the gadget. Incorrect notifications can be sent to the controller and backend server. Its device tools can be built based on input elements in the company community. Trusted operators can abuse their power and compromise systems or equipment. The computers of third party contractors will be hijacked and gain access to the corporate community. Vehicles ad hoc networks (WANET) attacks that affect road safety. Sibyl attacks are the most dangerous attacks and it is very difficult to get out. This includes high performance cars with more than one identity. The data obtained from this vehicle does not determine whether the mileage belongs to the car. Attackers use these to build communities according to their objectives. DDOS attacks can cause the system to send more than it should handle and prevent the system from overheating. A blank black attack involves sending packets of recordings by attackers[62].

The attacker rejects the packets of statistics and misrepresents communication in the community. A Wormhole Attack Two or more uncompromising cars are concerned about fake ads and many routing requests for marketing and they understand the minimum distance to the vacation spot. Contains documents created or transmitted by false information attack to other VANET vehicles. With the help of an attacking vehicle you can create false facts and send them to the van. Fake Area Information Fake Area Information is an attack transmitted by vehicles. Security packages and systems are not compromised as automobile area data may respond incorrectly. This happens in lost statistical packets as the packets of records are transferred to Phantom Motors. Censor fraud is required to simulate errors using conditions. In-car sensors can be deceived by attackers. A replay attack occurs when messages are collected and transmitted at a later date to mislead other cars on the network, but the message is not legitimate or genuine. This type of attack recreates and exploits what happened when a particular message was sent.

Passive evacuation attacks occur when a network is monitored by attackers to tune the movement of the vehicle or listen for messages on the motors. Attacking machines intercept messages and test messages. The information used in attack tasks is motors and communication styles. The attacks on him are even more obvious. The risk of such attacks can be assessed by assessing using selected vectors of cybernetic conversations. Electronic jamming of Wi-Fi broadcasts, DDoS attacks on open cyber infrastructure, exploitation of vulnerabilities, Credential Brute Force attacks and sensational attacks all threaten its programs and structures. The previous five vectors can threaten ITS, DDoS attacks, vulnerabilities, and violent pressure attacks commonly used in attacks against the deployment of various systems and programs. Electronic jamming is more accurate for its applications and systems. Sensational attacks are risky, but difficult to execute because gadgets or structures are not available to attackers. To properly compromise gadgets or systems, cybercriminals need the expertise and information of experts. The most serious threat to his gadgets and systems comes from the cyberzot community, wireless attacks and physical attacks.

Table 1: Summary of ITS Attacks and their Outcomes

Type of Attack	**Description of Attack**	**Outcome of the Attack**
DDoS Attacks	Vehicle to Vehicle message; Electronic Jammin	Chaos on Roadways; Service not available to legitimate users
Revenge and Terrorism	Hacking ITS to get the attacker access to the systems	Driving functions are cooperated and used as weapon
System gaming and theft	Hacking the autonomous vehicle	Avoid paying fees and tolls. Stealing goods from vehicle
Physical Attacks	Brute force; Reconnaissance and Man in the Middle attacks	Compromised or Tampered ITS device

Wireless Network Attacks	Sniffs wireless; Jamming of vehicle security systems; A man in the central of an attack	Gain access of CAN and on-board diagnostics, infotainment and telematics.
Wired Network Attacks	DNS Spoofing and hijacking; Malware; Spyware; SQL Injection and CSS attacks	Targeted state-sponsored attacks that pose a continuous threat.
VANET Attack	Sybil attacks; Black-hole attacks; Wormhole attacks	Fake location data is transmitted by vehicles; Compromises security-related applications and systems.

V. OPEN ISSUES AND RECOMMENDATION

The inclusion suggestion of organizing ITS systems can be extreme in light of a reluctance to work together and change realities. This will be expected to reputational costs, pressures from rivalry, and misfortunes that may results from digital wrongdoing. Data probably won't be to be had for sharing because of the reality fundamental frameworks or degree might not have been applied. Another strategic answers is imperative essentialness isn't given to digital security and therefore, spending is deficient.

The viability of countermeasures for cyber security isn't estimated precisely. There is an absence of understanding and comprehension of digital security that is viable and that which isn't ground-breaking. Eliminating of heritage ITS structures with new related structures is a moderate procedure. At the point when discussion and data exchange isn't incredible, security is debilitated. Information on the scope of digital dangers and having the option to make sure about ITS might be hard. Cyber security might be done, however in the event that there is restricted aptitude on an approach to utilize the product, it isn't generally as viable as it could be.

Countermeasures can be a powerful way to forestall and fathom cyber attacks, in any case if there might be protection from insurance selection the ITS is at extended risk as assaults are advancing and infiltrating the ITS air. Extra examination is needed to survey the viability of biometrics for moderating digital ambushes and first-rate rehearses for utilizing biometrics in Quite a while biological systems. An increasingly all-encompassing appraisal of ITS is expected to explore dangers at early degrees of improvement of car mechanization structures. Exploration wants to be drawn nearer from a repercussion of points of view, being equipped for accept a broad assortment of potential dangers. Adjusting the security, comfort and capacity of insurance vectors wishes to be assessed to be utilized inside the ITS air.

VI. CONCLUSION

Its ecosystem is constantly evolving and the threats to that system are evolving as ever. Many updates can be made in many areas. Improve security that primarily requires prevention and attack. The current method of using the ITS ecosystem has several shortcomings, which need to be addressed in the previous section. Further research is needed to evaluate exactly what responses to various ITS structures and applications in general. More research on co-operative structures is needed to identify cyber threats and develop strategies to prevent them. Biometric schemes are essential for ITS cyber security decisions.

REFERENCES

[1]. Krishnaraj,N.,Ezhilarasu,p., Dharun, V.S.," Smart Phone Application For Automatic Public Transportation Though Providing Intelligent Bus Status Information To The Users" International Journal of Applied Engineering Research (IJAER), Vol 59, pp.163-167, Jun -2015,

[2]. Chi-Hua Chen, "A Cell Probe-based Method for Vehicle Speed Estimation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103-A, no. 1, pp. 265-267, January 2020.

[3]. G.S.S.S.S.V.Krishna Mohan and Komanapalli Venkata Lakshmi Narayana, "Auto Tuning Smith-Predictive Control of Delayed Processes Based on Model Reference Adaptive Controller", Jour of Adv Research in Dynamical & Control Systems,Vol. 12, 04-Special Issue, p.p.1224-1230, 2020.

[4]. J.Sangeetha,T.Jayasankar," A Novel Whispered Speaker Identification System Based on Extreme Learning Machine", International Journal of Speech Technology, Springer,(2018) ,21 (1), pp.157–165.

[5]. Dr.N.Krishnaraj, Kiranmai Bellam, "Improved Distributed Frameworks to Incorporate Big Data through Deep Learning", Journal of Advanced Research in Dynamical & Control Systems, Vol. 12, 03-Special Issue, 2020.pp:332-338.

[6]. N.Krishnaraj, Mohamed Elhoseny, M.Thenmozhi,Mahmoud M.Selim , K.Shankar , "Deep Learning Model for real- time image compression in Internet of Underwater Things(IoUT)", Journal of Real-time Image Processing ,2019.

[7]. Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Khanna, A., & de Albuquerque, V. H. C. (2020). Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, 32(4), e5122.

[8]. GSSSSV.Krishna Mohan and Yarravarapu Srinivasa Rao, "An efficient design of finite impulse response — Fractional-order differentiator using shuffled frog leaping algorithm heuristic", International Journal of Wavelets, Multiresolution and Information Processing, World Scientific Publishing Company, Vol. 17, No. 2 March 2019.

[9]. N.Krishnaraj,M.G.Kavitha,T.Jayasankar,K.Vinoth Kumar , "A Glove based approach to recognize Indian Sign Languages", International Journal of Recent Technology and Engineering (IJRTE) Volume-7, Issue-6, March 2019, pp.1419-1425.

[10]. Dr.N.Krishnaraj ,Dr P Kiran Kumar, Mr K Subash Bhagahavn , "Conceptual Semantic Model for Web Document Clustering Using Term Frequency", EAI Endorsed Transactions on Energy Web and Information Technologies, Volume 5, Issue 20,2018,pp.1-4.

[11]. Chi-Hua Chen, Fangying Song, Feng-Jang Hwang, Ling Wu, "A Probability Density Function Generator Based on Neural Networks," *Physica A: Statistical Mechanics and its Applications*, vol. 541, Article ID 123344, March 2020.

[12]. G.S.S.S.S.V. Krishna Mohan & Yarravarapu Srinivasa Rao: "Optimal Order of the Differentiator Selection in Noise Removal of ECG Signals", International Journal of Recent Technology and Engineering (IJRTE),Volume-7, Issue-6, 260-267, March 2019.

[13]. N. Krishnaraj, P. Ezhilarasu, X Z Gao ,"Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data" , Current Signal Transduction Therapy Vol.11 (2),pp71-75,June 2016.

[14]. N. Krishnaraj, P. Ezhilarasu, S.Karthik , Manoj Prabhakar.J, ,"Enhancing Security in Mobile Devices through Multimodal biometrics" , Middle-East Journal of Scientific Research 23 (8) ,pp. 1598-1603,Jun 2016

[15]. Mingyang Pan, Yisai Liu, Jiayi Cao, Yu Li, Chao Li, Chi-Hua Chen, "Visual Recognition Based on Deep Learning for Navigation Mark Classification," *IEEE Access*, vol. 8, pp. 32767-32775, February 2020.

[16]. GSSSSV.Krishna Mohan and Yarravarapu Srinivasa Rao, "An efficient design of fractional order differentiator using hybrid Shuffled frog leaping algorithm for handling noisy electrocardiograms", International Journal of Computers and Applications,Feb 2019.

[17]. Shankar, K., Lakshmanaprabu, S. K., Khanna, A., Tanwar, S., Rodrigues, J. J., & Roy, N. R. (2019). Alzheimer detection using Group Grey Wolf Optimization based features with convolutional classifier. Computers & Electrical Engineering, 77, 230-243.

[18]. GSSSSV.Krishna Mohan and K.Venkata Lakshmi Narayana, "Design Of A Fractional Order PID For A Three Tank System", International Journal of Applied Engineering Research, Volume 10, Number 2 (2015) pp. 3133-3148, Research India Publications, April 2015.

[19]. Ling Wu, Qishan Zhang, Chi-Hua Chen, Kun Guo, Deqin Wang, "Deep Learning Techniques for Community Detection in Social Networks," *IEEE Access*, vol. 8, pp. 96016-96026, May 2020.

[20]. D.V.L.N.Sastry, B.Anil Kumar, P. Kameswara Rao, G.S.S.S.S.V.Krishna Mohan "Tuning Of Fractional Order PID Controller For Interacting Systems By Different Methods", i--manager's Journal on Instrumentation & amp; Control Engineering Vol.2 No.2 May July 2014.

[21]. A,Venkata Naga Vamsi, G.S.S.S.S.V.Krishna Mohan, S.S.S.Srikanth, "Simplified Thermocouple Interface For Hot Only Or Cold Only Measurement With Linearization Circuit", (IJERA) International Journal of Engineering Research and Applications, Vol. 2, Issue5, September-October 2012, pp.1663-1667.

[22]. Chin-Ling Chen, Tsai-Tung Yang, Yong-Yuan Deng, Chi-Hua Chen, "A Secure IoT Medical Information Sharing and Emergency Notification System Based on Non-repudiation Mechanism," *Transactions on Emerging Telecommunications Technologies*, Accepted Manuscript.

[23]. D.V.L.N.Sastry, G.S.S.S.S.V.Krishna Mohan, M.S.R.Naidu, N.Mohana Rao, "An Implementation of different non-linear PID controllers on a single tank level control using Matlab", (IJCA) International Journal of Computer Applications (0975 – 8887) Volume 54– No.1, September 2012.

[24]. Hsu-Yang Kung, Chi-Hua Chen, Mei-Hsien Lin, Tai-Yang Wu, "Design of Seamless Handoff Control Based on Vehicular Streaming Communications," *Journal of Internet Technology*, vol. 20, no. 7, pp. 2083-2097, December 2019.

[25]. Dhanapal, R & Visalakshi, P 2016, Real Time Health Care Monitoring System for Driver Community Using Adhoc Sensor Network", Journal of Medical Imaging and Health Informatics, ISSN 2156-7018, vol. 6, no. 3, pp. 811-815.

[26]. Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter Tuning Deep Learning for Diabetic Retinopathy Fundus Image Classification. IEEE Access.

[27]. "Distributed Security Model for Remote Healthcare (DSM-RH) Services in Internet of Things Environment" Cyril Mathew, R. Dhanapal, P. Visalakshi, K. G. Parthiban, S. Karthik, Journal of Medical Imaging and Health Informatics, Volume 10, Number 1, January 2020, pp. 185-193(9).

[28]. Shankar, K., & Elhoseny, M. (2019). Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES. Journal of Universal Computer Science, 25(10), 1221-1239.

[29]. "Hybrid Dragonfly Optimization-Based Artificial Neural Network for the Recognition of Epilepsy" R. Dhanapal K. G. Parthiban, S. Vijayachitra, International Journal of Computational Intelligence Systems,Volume 12, Issue 2, 2019, Pages 1261 - 1269.

[30]. Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography. In Cybersecurity and secure information systems (pp. 193-204). Springer, Cham.

[31]. "A Cost-Aware Method for Tasks Allocation on the Internet of Things by Grouping the Submitted Tasks"R Dhanapal, T Akila, SS Hussain, D Mavaluru - Journal of Internet Technology, Volume 20 (2019) No.7,Pages 2055-2062.

[32]. Shankar, K. (2017). Prediction of most risk factors in hepatitis disease using apriori algorithm. Research Journal of Pharmaceutical Biological and Chemical Sciences, 8(5), 477-484.

[33]. "Real Time Health Care Monitoring System for Driver Community Using Adhoc Sensor Network" Dhanapal, R.; Visalakshi, P.Journal of Medical Imaging and Health Informatics, Volume 6, Number 3, June 2016, pp. 811-815(5)

[34]. Chi-Hua Chen, "An Arrival Time Prediction Method for Bus System," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4231-4232, October 2018.

[35]. "A Sector Based Energy Efficient Adaptive Routing Protocol for Large Scale MANET" R Dhanapal, P Visalakshi - Research Journal of Applied Sciences, Engineering and Technology,volume 9(7): pages 478-484,2015.

[36]. Elhoseny, M., Shankar, K., &Uthayakumar, J. (2019). Intelligent diagnostic prediction and classification system for chronic kidney disease. Scientific reports, 9(1), 1-14.

[37]. Dhanapal, R & Visalakshi, P 2016, "Optimizing Trust Based Secure Routing for Unified Efficient Resource Sharing for Large Scale MANET-TSRRS", Asian Journal of Information Technology, ISSN :1682-3915, vol. 15, no. 19, pp. 3756-3762.

[38]. Elhoseny, M., Bian, G. B., Lakshmanaprabu, S. K., Shankar, K., Singh, A. K., & Wu, W. (2019). Effective features to classify ovarian cancer data in internet of medical things. Computer Networks, 159, 147-156.

[39]. Dhanapal, R & Visalakshi, P 2015, "Efficient Clustering Protocol on Ant-Bee agent for Large Scale Manet", International Journal of Applied Engineering Research, ISSN 0973-4562, vol. 10, no. 52, pp. 349-361.

[40]. Elhoseny, M., & Shankar, K. (2020). Energy efficient optimal routing for communication in VANETs via clustering model. In Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks (pp. 1-14). Springer, Cham.

[41]. R. Meera, P.Anandan "A Review On Automatic Detection of Brain Tumor Using Computer Aided Diagnosis System Through MRI" The Energy Green, Intelligent in Computing & Communication Technologies in Journal of Energy Web and Information Technologies, Vol5, Issue20, 2018.

[42]. Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., &ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[43]. G. Keethana , P.Anandan "A Survey on Security Issues and Challenges in Mobile Ad-hoc Network" The Energy Green, Intelligent in Computing & Communication Technologies in Journal of Energy Web and Information Technologies,Vol5,Issue20,2018.

[44]. Mohanty, S. N., Lydia, E. L., Elhoseny, M., Al Otaibi, M. M. G., & Shankar, K. (2020). Deep learning with LSTM based distributed data mining model for energy efficient wireless sensor networks. Physical Communication, 101097.

[45]. K.Dhanasekaran , P.Anandan, A.Manju "A Computational Approach of Highly Secure Hash Algorithm For Color Image Steganography Using Edge Detection And Honey Encryption Algorithm" International Journal of Engineering & Technology, 7 PP. 239-242, 2018.

[46]. Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[47]. K.Vijayalakshmi,P.Anandan "A Multi Objective Tabu Particle Swarm Optimization for Effective Cluster Head Selection in WSN" Cluster Computing, Vol. 22,Issue5,12275–12282,2019.

[48]. Lydia, E. L., Raj, J. S., PandiSelvam, R., Elhoseny, M., & Shankar, K. (2019). Application of discrete transforms with selective coefficients for blind image watermarking. Transactions on Emerging Telecommunications Technologies, e3771.

[49]. B.Senthilraja, P.Anandan, A.Manju "The Survey to Implement Recent Reversible Watermarking Techniques In Medical Images And Other Applications" Journal of Advanced Research in Dynamical & Control Systems, Vol.10-Special Issue 03, May 2018.

[50]. Sivaram, A. M., Lydia, E. L., Pustokhina, I. V., Pustokhin, D. A., Elhoseny, M., Joshi, G. P., & Shankar, K. (2020). An Optimal Least Square Support Vector Machine Based Earnings Prediction of Blockchain Financial Products. IEEE Access.

[51]. P.Vinayagam, P.Anandan "A Review on Pixel Performance in CMOS Image Sensors" Journal of Advanced Research in Dynamical & Control Systems, 05-Special Issue, July 2017.

[52]. Elhoseny, M., Selim, M. M., & Shankar, K. (2020). Optimal Deep Learning based Convolution Neural Network for digital forensics Face Sketch Synthesis in internet of things (IoT). International Journal of Machine Learning and Cybernetics, 1-12.

[53]. P.Anandan, N.Mohankumar,V.Saranya "Characterization of Flicker noise in Dual Material Gate Silicon Nanowire Transistors" Journal of Nanoelectronics and Optoelectronics, 12, 72–75 (2017) (Impact Factor 0.369)

[54]. Chi-Hua Chen, Feng-Jang Hwang, Hsu-Yang Kung, "Travel Time Prediction System Based on Data Clustering for Waste Collection Vehicles," *IEICE Transactions on Information and Systems*, vol. E102-D, no. 7, pp.1374-1383, July 2019.

[55]. N.Mohankumar, A.Mohanbabu, S.Baskaran, P.Anandan, N.Anbuselvan and P.Bharathivikkiraman "Modeling of Sheet Carrier Density, DC and Transconductance of Novel InxAl1-XN/GaN-Based HEMT Structures" Advanced Materials Research Vol. 1105 (2015) pp 99-104.

[56]. Lakshmanaprabu, S. K., Shankar, K., Ilayaraja, M., Nasir, A. W., Vijayakumar, V., &Chilamkurti, N. (2019). Random forest for big data classification in the internet of things using optimal features. International journal of machine learning and cybernetics, 10(10), 2609-2618.

[57]. Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 102, 1027-1037.

[58]. Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[59]. Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., &Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[60]. Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems. IEEE Access, 8, 107112-107123.

[61]. Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[62]. Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.