JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

New Protocol Concept for WSN Security

[1] Ritika Sharma , [2] Charu Shree , [3] Dr. Manish Kumar Mukhija
[1] M. Tech Scholar, [2] Assistant professor, [3] Associate Professor
Department of Computer Science & Engineering
Arya Institute of Engineering & Technology , Jaipur ,India

Abstract : Wireless Sensor networks are going at a large pace , it is being part of business organizations, military department, health departments and more. With the advantage provided with the wireless networks related to communication, speed and more , it suffers from some security issues. In this paper we reviews about the WSN networks and work done in WSN , together with that we will propose a security related concept for enhancing the security parameters for the data communication in the wireless sensor networks.

IndexTerms **– Wireless Sensor Network ,Security , SHA-512**

I. INTRODUCTION

Lately a proficient plan of a Wireless Sensor Network has turned into a main area of examination. A Sensor is a gadget that reacts and recognizes some sort of contribution from both the physical or ecological conditions, like tension, heat, light, and so on The result of the sensor is by and large an electrical sign that is communicated to a regulator for additional handling. This article examines an outline of sorts of wireless sensor networks, order, kinds of assaults, sorts of portability and directing conventions.

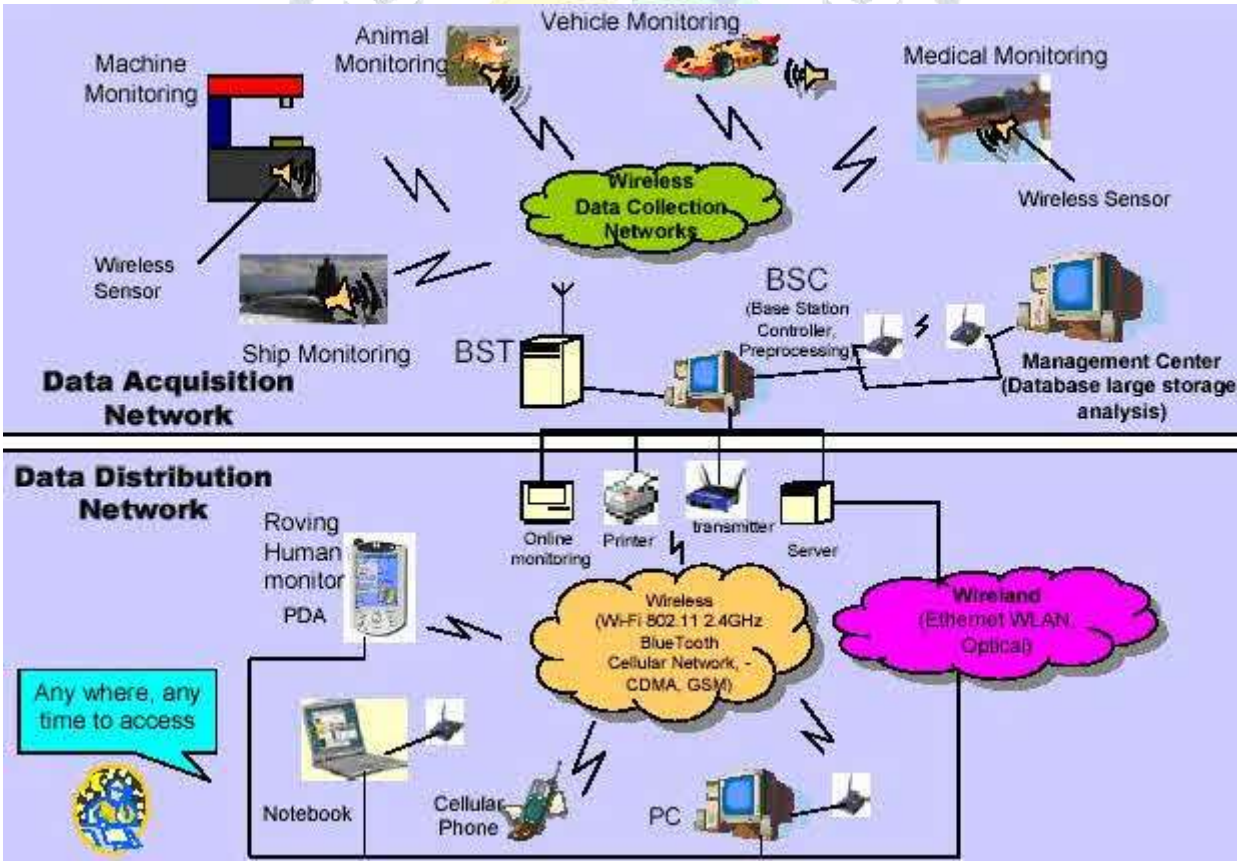

Fig 1. Wireless Sensor Network

A Wireless sensor network can be characterized as a network of gadgets that can impart the data assembled from an observed field through wireless connections. The information is sent through different nodes, and with an entryway, the information is associated with different networks like wireless Ethernet. WSN is a wireless network that comprises of base stations and quantities of nodes (wireless sensors). These networks are utilized to screen physical or ecological conditions like sound, strain, temperature, and co-operatively go information through the network to the principle area.

A few security arrangements had been proposed for WSNs; nonetheless, asset imperative of sensors makes a portion of these security arrangements ill suited for WSNs. This, accordingly, makes their reception in WSNs incomprehensible. This is because of insecurity of the geography of most WSNs. A portion of the WSNs, dissimilar to a few different networks, comprise of versatile nodes that discontinuously change the geography of the networks, accordingly making it unthinkable for such portable network to utilize existing convention produced for static nodes. Additionally, enormous volume of information is moved on the WSNs; this builds the traffic on the wireless correspondence framework of WSN. This large number of show that security and protection arrangements of WSN should in addition to the fact that lightweight be as far as the computational, correspondence, and energy overheads yet additionally support total and multi-jump to diminish the deals and broaden the life expectancy of the networks. In the mean time, the greater part of the current security arrangements don't have these presentation necessities.

II. Related Work in Security

K. Fukuda et al 2018 [1] A genuine wireless limit change sensor network (PhyC-SN) uses the repeat change of identifying information and sees the whole recognizing information from the recognized repeat range. For long life sensor hub, the event driven sensor decides to send the recognizing information according to the particular proportion of changing concerning the distinguishing information. Regardless, the information division is hard for the PhyC-SN with event driven sensor. This paper proposes the send control and the information parcel for PhyC-SN with event driven sensor. The Gaussian probability model for expecting the future distinguishing information is used for surveying the difficulty of information segment. The effect of proposed procedure is evaluated by virtual experience.

L. Zhang et.al. 2016 [2] For heterogeneous wireless sensor networks energy costs, network information transmission, network life cycle and various issues, the introduction of fundamental investigation procedures for complex network theory.

P. Harichandan et.a.. 2013 [3] Wireless sensor hubs are shipped off collect important information from the field yet their limit on battery power drives us to contemplate energy compelling controlling shows with the objective that they can work over the course of longer time periods. We focus on the potential gains of having various chains in a network with each chain's most noteworthy hub (called the aggregator) assembling the information from the hubs under it and imparting it to the sink. In the proposed plot, a chain in each locale fills in as PEGASIS.

J. S. Ho, 2019 [4] Wireless networks of sensors, shows, and splendid contraptions on the body offer solid capacities for prosperity noticing, human-machine interfaces, and other emerging creative applications. Existing procedures for wireless interconnection, regardless, are confined by challenges in radiative incident, impedance, and information shortcoming natural for the radiation of radio-waves into the including space. In this show, we portray a powerful and secure method for managing interconnect wireless sensor networks by confining radio-waves on dressing planned with conductive materials. We show how these material models, named metamaterial materials, can overhaul wireless transmission (counting Bluetooth and Wi-Fi) from business contraptions (cells) by numerous huge degrees and enable wireless power move to sensors on the body.

Z. Yong, et.al. 2008 [5] This short paper presents sensible estimations for diminishing disappointment in reliability partition organization subject to geographical stateless controlling, which has exceptional likely applications in tremendous extension wireless sensor networks (WSN). Taking into account available estimation, the paper presents a mathematical formalization to productive appreciation the multipath reiteration issue of WSN. With the information past one leap and the pile changing part, the information retransmission and constancy detachment reassignments are lessened. The blueprint and amusement display the proposed computations feasibility and the ability to give unfaltering quality division organization.

Y. Meng et.al. for [6] In a standard checking system, physiological limits like Electrocardiography (ECG), Electromyography (EMG), and Electroencephalography (EEG) from various sensors set definitively on human body are noticed for giving continuous analysis to the patient and clinical staffs. In this paper, creators research the show the extent that structure power outage probability of proposed methodology in relationships with direct transmission, standard support and network coding-based sensor joint effort. Diversion results check the accuracy of the assessment and display that accommodating correspondence scheme subject to network coding in WBAN channel gives preferred execution took a gander at over other two plans.

F. X. Li et.al 2015 [7] This paper presents a wireless sensor network for assessing the hidden sufficiency of metropolitan expressway ranges. Sensor information were assembled on two pre-zeroed in on box point of support ranges (PSBB) with eight wireless sensor hubs. The wireless sensor had the choice to assemble 100 Accelerometer information tests each second without losing any wireless sensor information. Application writing computer programs was made to change the model information into repeat region. Sensor information from every one of the eight wireless sensor hubs have shown the tantamount zenith frequencies with various fundamental endeavors on a comparative augmentation. The apex repeat part was surprising to each highway expansion. The sign to fuss extent in repeat region is more vital than seven to one. By differentiating the real wireless sensor information and the conjectures from a restricted part length model, a theory of surveying the essential strength of the platform was presented.

R. Hu, 2016 [8] Seeing (perception) yet not cognizance (defenseless security execution)" is ordinary issue in most security structures. Yet actually basic headway has been cultivated in biometric ID development, the progression of single advances doesn't radically chip away at the overall show or tackle the structure level issues of government retirement assistant. At this point regardless overhauls of single advancement, the going with structure level specific bottlenecks ought to be settled to chip away at the overall show of government upheld retirement: 1. Weak sides of acumen exist in perception space of due to the non-get over of observation sensors, 2. The display of single distinctive verification advancement reduces distinctly in complex surveillance circumstances, for instance, powerless lighting conditions or cover, 3. Customary reprobation developments become invalid due to the multi-stage non-fixed progression component of muddled events.

Three hardships recorded above eagerly relate to three legitimate issues in the examination development of enormous visual information on three levels: recognizing information, ID advancement and model affirmation. Our survey centers around (1) exploiting the absolute arranging part between genuine space and multivariate distinguishing spaces to fill-in the weak sides of identifying information, (2) exploring the reciprocal arrangement of multi-secluded things in multivariate recognizing spaces to deal with the logical show from single ID development, (3) focusing on the spatial-brief progression instrument in the entire lifecycle of baffling events to expand plan affirmation from neighborhood presence. The security space is the real space with broad guarded limit, which consolidates unavoidable identifying, reliable distinctive confirmation, invading example examination and pushing toward hazard notice at whatever point, at any region, for any thing and for any lead.

Intending to create the theory of safety space, this audit is detached into three levels: information getting and perceptional estimation, scene examination and advancement assumption, resource booking and structure applications. Then, it is furthermore confined into five tasks: (1) task 1: visual article affirmation and enormous information based ID, (2) task 2: situational experience with social affairs and multi-scale irritated, (3) task 3: semantic examination of scenes and complementary computation in multivariate spaces, (4) task 4: significant scale visual recuperation and security peril assessment, (5) task 5: Warning game plan of the security space and its applications. Task 1 looks at to the essential level since identifying and recognizing confirmation of articles is the justification for assessment.

Task 2 and 3 connect with the second level since bundle lead, events, scene and their advancement are crucial for the conjecture and alerted of safety events. Task 4 and 5 connect with the third level of this audit to cultivate the prevalent show handling stage, to lead system appraisal and application show. Tremendous visual information contains immense high-layered recognizing information, proposing the jumbled relationship among social articles. In all honesty, in the domain of information, the spatial-common association between the tremendous information objects is more key than the causal relationship, and these private and certain associations make the essential convictions out of the enormous information social examination. Simply the assessment of individuals, get-togethers and scenes in enormous visual information rely upon the middle part of government retirement assistant examination, that is" social plan and social activities", can it maintains the fundamental exchange of metropolitan security structure from assessment in this manner to see early.

The overall inspiration driving this audit is to create the immense information assessment system in security space, understanding the brilliant gigantic visual information structure which maintains information examination of hundred billions of component information, billions of picture information, an enormous number of visual distinguishing terminals. The ordinary achievements on the notification and security structure for tremendous spaces can show up at the worldwide driving level. Considering the achievements over, the endeavor plans to encourage 10 smart colossal information examination aftereffects of 3 classes, and the ordinary benefits of industrialization progression can show up at 100 billion, which propels the upstream and downstream industry to recognize money related benefits 3 billion. Similarly we attempt to transform into the generally driving industry in the field of huge security information examination.

X. Wang et.al. 2018 [9] Large endeavors and relationship from both private and public regions typically re-fitting a phase plan, as a part of the Managed Security Services (MSSs), from outcast providers (MSSPs) to screen and look at their information containing network wellbeing information. Splitting such information between these colossal components is acknowledged to additionally foster their ampleness and usefulness at taking care of cybercrimes, through superior examination and encounters. In any case, MSS stage customers as of now are not skilled or not ready to split information between themselves because of different reasons, including insurance and protection worries, regardless, when they are using a comparative MSS stage. Thusly any proposed framework or technique to address such a test need to ensure that sharing is refined in a strong and controlled way. In this paper, we propose another designing and use case driven designs to engage secret, versatile and agreeable information splitting between such affiliations using a comparable MSS stage. MSS stage is an amazing environment where different accomplices, including supported MSSP workforce and customers' own customers, approach a comparable stage anyway with different sorts of honors and endeavors. Consequently we truly make every effort to chip away at the accommodation of the stage supporting sharing while simultaneously keeping the current honors and endeavors impeccable. As an innovative and leading undertaking to address the trial of information participating in the MSS stage, we want to ask further work to follow with the objective that grouped and helpful partaking over the long haul happens among MSS stage customers.

T. T. Teoh et.al. 2017 [10] Authors acknowledge the properties of HMM being perceptive, probabilistic, and its ability to show different typically happening states structure a respectable reason to exhibit advanced security information. It is therefore the motivation of this work to give the fundamental delayed consequences of our undertakings to predict security attacks using HMM. An enormous network datasets tending to advanced insurance attacks have been used in this work to develop an expert structure. The characteristics of assailant's IP areas can be removed from our joined datasets to deliver quantifiable information. The computerized security ace gives the substantialness of every characteristic and designs a scoring structure by clarifying the log history. We applied HMM to perceive a computerized insurance attack, questionable and no attack by introductory breaking the information into 3 bundle using Fuzzy K mean (FKM), then, truly name a little information (Analyst Intuition) ultimately use HMM

state-based procedure. Subsequently, our outcomes are incredibly elevating as difference with finding characteristic in a network assurance log, which all around results in making colossal proportion of fake area.
M. Elsayed and M. Zulkernine, 2018 [11] Cloud figuring is connecting new advancements for colossal information. At the heart, cloud logical applications become the most-publicized uprising. Cloud intelligent applications enjoy astounding benefits for tremendous information dealing with, simplifying it, fast, adaptable and functional; however, they present various security possibilities. Security breaks due to threatening, frail, or misconfigured logical applications are seen as the top security threats to gigantic information.

M. Kantarcioglu and F. Shaon, 2019 [12] Progressively affiliations are gathering ever more noteworthy extents of data to fabricate complex data assessment, AI and AI models. Furthermore, the data required for building such models might be unstructured (e.g., text, picture, and video).

Along these lines such data might be dealt with in various data the board structures going from social informational indexes to extra ground breaking NoSQL informational collections uncommonly created for dealing with unstructured data. Moreover, data researchers are intelligently utilizing programming tongues, for example, Python, R, and so on to oversee data utilizing many existing libraries. Some of the time, the made code will be in this way executed by the NoSQL framework on the put away data. These overhauls display the need for a data security and confirmation strategy that can dependably ensure data put away in a wide extent of data the bosses frameworks and keep up with security approaches whether or not delicate data is managed utilizing a data expert submitted complex program. In this paper, we present our vision for building such a reaction for ensuring huge data. In particular, our proposed SECUREDL structure licenses relationship to 1) keep up with plans that control acceptance to touchy data, 2) keep major review logs regularly for data association and legitimate consistence, 3) clean and redact delicate data on-the-fly ward on the data affectability and AI model necessities, 4) perceive possibly unapproved or inquisitive authorization to delicate data, 5) therefore make quality set up access control frameworks based in regards to data affectability and data type.

L. Ming, et.al. 2018 [14] Modern vehicles in Intelligent Transportation Systems (ITS) can talk with each other similarly as roadside establishment units (RSUs) to construct transportation viability and road prosperity.

For example, there are strategies to alert drivers early with regards to traffic episodes and to help them with avoiding blockage. Threats to these structures, of course, can limit the upsides of these advancements. Getting ITS itself is a critical concern in ITS arrangement and execution. In this paper, we give a security model of ITS which widens the praiseworthy layered network security model with transportation security and information security, and gives a reference for arranging ITS designs. Considering this security model, we also present a gathering of ITS risks for insurance. Finally a proof-of-thought model with malignant hubs in an ITS structure is in like manner given to display the impact of attacks. We examined the risk of toxic hubs and their effects to laborers, for example, extending cost costs, travel distances, and travel times, etc Test results from reenactments subject to Veins shows the perils will accomplish 43.40% more complete expense charges, 39.45% longer travel distances, and 63.10% more travel times.

A. R. de la Concepcion et.al 2014 [15] The paper presents a flexible response for the affirmation of uniquely named wireless sensor networks sensible to move gigantic measures of information over narrowband channels. The electromagnetic front-end is expressly expected to stay aware of radiation efficiency regardless, when implanted in media with unpredictable dissipative characteristics. The use of tight band channels, similarly as the probability to lessen the carrier down to 180 MHz (impeccably with authoritative endorsements), empowers obstacles, lower signal affectability, and non-view consideration. For this enormous number of reasons, the stage is being applied to improvements, to assemble a strong and insignificant cost instrument, which works with doable cultivation.

F. Z. Brilliance et. al 2019 [16] recommended the course of validation of the client utilizing the calculation which creates the secret key utilizing the arbitrary mix of the words and numbers. Secret key which created depends on the powerful sources of info like the most loved name of the novel, the quantity of grandma's youngsters, secret dates and so on

Shah Zaman Nizamani et.al 2017 [17] In this paper a text based customer affirmation scheme is proposed which chips away at the security of printed secret expression plot by modifying the mystery expression input procedure and adding a mystery key change layer. In the proposed plot alphanumeric mystery key characters are tended to by sporadic decimal numbers which go against online security attacks, for instance, shoulder surfing and key logger attacks.

III. SOLUTION SUGGESTED

For the purpose of the security enhancement we have proposed a new concept of WSN Data Security. The proposed concept working in the modules of the user authentication and data file sharing,

3.1 Algorithms for the User Registration

Step 1: Read the user details like user name, email id, phone number
Step 2: Select the File Related with the User Photo.
Step 3: Display the Rotation Captcha to User.

Fig 3.1 Image Based Captcha

And we have these angles

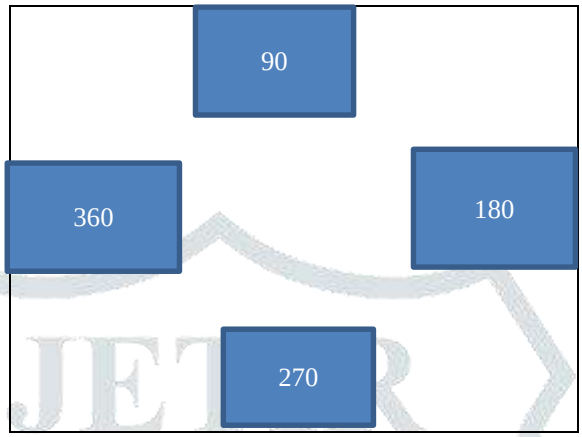

Fig 3.2 Rotation Angles

Now, we rotate these images as by clicking over the image , whenever when we will click over the image the image will get rotate by an angle of 90 degree. The fig 3.3 shows the status after the rotation of the images and the pattern will be formed as per the rotation angle of each of the image

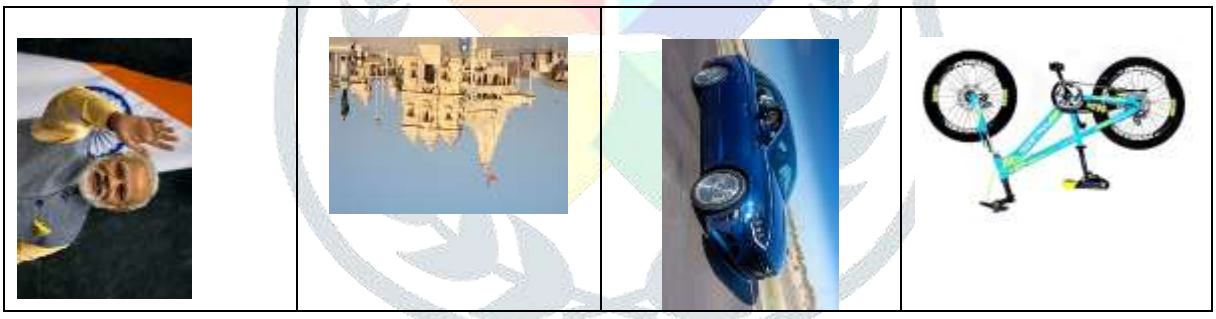

Fig 3.3 Rotate CAPTCHA

This is the sample,

Pic1_180_Pic2_270_pic3_90_pic3_270

Pic1 , Pic2 are the simulated names and the actual names will depends on the image used in the implementation.
Step 4 :Together with that we will form the hash using the SHA-512 algorithm for the user photo given in the previous steps and two step validation concept will be used on which is the image based SHA Pattern extract as well as pattern which is formed using the CAPTCHA concept.
Step 5: We will then store all the details in the database.

3.2 Algorithms for the User Login

Step 1: Read the user details like user name
Step 2: Specify the image and First part HASH.
Step 3: Display the Rotation Captcha to User.
Step 4: If all this validation is OK then the user prompted for the second part which is the CAPTCHA validation.
Step 5: After all the details are validated then the user is allowed to login in the system.

3.3 Algorithm for the File Sharing Sender End

Step 1 : Select the Username to whom the file is to be send.
Step 2: Internally the SHAFirst Part of User name (Sender) and SHA Second Part of Username (Receiver) are fetched to form the session key.
Step 3: Select the Document file to be shared.
Step 4: Fetch the File Size and the data speed of communication
(a) Normal Channel Chunks of 500KB
(b) Good Channel Chunks of 1 MB

Step 5: Specify the Encryption Key which is formed as First 5 character of sender name, 5 character of receiver name, size of file.
E.g Sender is :demoXuser
Receiver is :Kapiljpr
demoXu_Kapilj_11189
(Size of file in bytes)
Step 6: The File is divided into chunks and encrypted
Sep 7: Details will stored in the file.

3.4 Algorithm for the File Sharing Receiver End

Step 1: Enter Session Key and Encryption Key
Step 2: Specify location of Chunks.
Step 3: Chunks decrypted and joined in original file.
Step 4: File then accessed by the user.

IV. CONCLUSION

One of the difficulties in WSNs is to give high-security necessities obliged assets. The security necessities in WSNs are included node confirmation, information secrecy, hostile to think twice about flexibility against traffic investigation. So , it is important to focus on these issues and via our proposed algorithm we are trying to propose a concept for security enhancement. In the further research we will like to implement its simulation model.

REFERENCES

1. K. Fukuda *et al*., "Transmit control and data separation in physical wireless parameter conversion sensor networks with event driven sensors," *2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, 2018, pp. 12-14.
2. L. Zhang, J. Qu and J. Fan, "Topology Evolution Based on the Complex Networks of Heterogeneous Wireless Sensor Network," *2016 9th International Symposium on Computational Intelligence and Design (ISCID)*, 2016, pp. 317-320.
3. P. Harichandan, A. Jaiswal and S. Kumar, "Multiple Aggregator Multiple Chain routing protocol for heterogeneous wireless sensor networks," *2013 INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND COMMUNICATION (ICSC)*, 2013, pp. 127-131.
4. J. S. Ho, "Wireless Body Sensor Networks with Metamaterial Textiles," *2019 8th Asia-Pacific Conference on Antennas and Propagation (APCAP)*, 2019, pp. 89-89.
5. Z. Yong, M. Jianfeng, D. Lihua, P. Liaojun and G. Yuanbo, "Adaptive Algorithms to Mitigate Inefficiency in Reliability Differentiation Mechanisms for Wireless Sensor Networks," *2008 The 4th International Conference on Mobile Ad-hoc and Sensor Networks*, 2008, pp. 208-211.
6. Y. Meng, T. Qin and J. Xing, "Sensor Cooperation Based on Network Coding in Wireless Body Area Networks," *2014 International Conference on Wireless Communication and Sensor Network*, 2014, pp. 358-361.
7. F. X. Li, A. A. Islam, A. S. Jaroo, H. Hamid, J. Jalali and M. Sammartino, "Urban highway bridge structure health assessments using wireless sensor network," *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, 2015, pp. 75-77.
8. R. Hu, "Key Technology for Big Visual Data Analysis in Security Space and Its Applications," *2016 International Conference on Advanced Cloud and Big Data (CBD)*, 2016, pp. 333-333.
9. X. Wang, I. Herwono, F. D. Cerbo, P. Kearney and M. Shackleton, "Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services," *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1-7.
10. T. T. Teoh, Y. Y. Nguwi, Y. Elovici, N. M. Cheung and W. L. Ng, "Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data," *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 2017, pp. 2080-2083.
11. X. Wang, I. Herwono, F. D. Cerbo, P. Kearney and M. Shackleton, "Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services," *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1-7.

12. T. T. Teoh, Y. Y. Nguwi, Y. Elovici, N. M. Cheung and W. L. Ng, "Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data," *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 2017, pp. 2080-2083.
13. M. Elsayed and M. Zulkernine, "Towards Security Monitoring for Cloud Analytic Applications," *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, 2018, pp. 69-78.
14. M. Kantarcioglu and F. Shaon, "Securing Big Data in the Age of AI," *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2019, pp. 218-220.
15. L. Ming, G. Zhao, M. Huang, X. Kuang, H. Li and M. Zhang, "Security Analysis of Intelligent Transportation Systems Based on Simulation Data," *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, 2018, pp. 184-187.
16. A.R. de la Concepcion, R. Stefanelli and D. Trinchero, "Adaptive wireless sensor networks for high-definition monitoring in sustainable agriculture," *2014 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, 2014, pp. 67-69.
17. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2019.
18. Shah Zaman Nizamani, Syed Raheel Hassan, Tariq Jamil Khanzada and Mohd Zalisham Jali, “A Text based Authentication Scheme for Improving Security of Textual Passwords” International Journal of Advanced Computer Science and Applications(ijacsa), 8(7), 2017.
19. Lata B T Vidya Rao Sivasankari H Tejaswi V Shaila K Venugopal KR et al. "SEAD: Source Encrypted Authentic Data for Wireless Sensor Networks" International Journal of Engineering Research and Development vol. 11 no. 03 pp. 01-16 March 2015 ISBN 227 8–067X.
20. Christine Salamacha Sterling Smoot and Kathlene Farris "C4ISRT in an Operational Context" John Hopkins APL Technical Digest vol. 21 no. 3 2000.
21. Tarek Azzabi and Hassene Farhat "A Survey On Wireless Sensor Networks Security Issues And Military Specificities" International Conference on Advanced Systemsand Electric Technologies (IC_ASET) 2017.
22. S.R. BoselinPrabhu M. Pradeep and E. Gajendran "Military Applications of Wireless Sensor Network System" A Multidisciplinary Journal of Scientific Research & Education vol. 2 no. 12 December 2016.
23. Jitender Grover and Shikha Sharma "Security Issues in Wireless Sensor Network - A Review" 5th International Conference on Reliability Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions) pp. 7-9 Sep. 2016.
24. Prerna Mahajan and Abhishek Sachdeva "A Study of Encryption Algorithms AES DES and RSA for Security" Global Journal of Computer Science and Technology Network Web & Security vol. 13 no. 15 2013.
25. AL. Jeeva V. Palanisamy and K. Kanagaram "Comparative Analysis of Performance Efficiency And Security Measures of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) vol. 2 no. 3 pp. 3033-3037 May-Jun 2012 ISBN 2248–9622.
26. Rajat Gupta Pallavi Singh Kaushal Sultania and Archit Gupta "Security for Wireless Sensor Networks in Military Operations" Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT) 2013.
27. Sattar J Aboud "An efficient method for attack RSA scheme" IEEE 2009.
28. Khirod Chandra Sahoo and Umesh Chandra PatiG "IoT Based Intrusion Detection System Using PIR Sensor" 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT) May 19–20 2017.
29. B. Ayyappan and P. Mohan Kumar "Vehicular Ad Hoc Networks (VANET): Architecture methodologies and design issues" IEEE Conf Publication pp. 177-180 2016.
30. P Priyanka and B Ayyappan "Wireless sensor networks - technologies protocols applications and simulators: A survey" JCPS Journal 2015.
31. Monika Bhalla Brijesh Kumar and Nitin Pandey "Security Protocols for Wireless Sensor Networks" in ICGCloT - International Conf on Green Computing and Internet of Things IEEE 2015.
32. Perrig Adrian Szewczyk Robert Culler David and J.D. Tygar "SPINS: Security protocols for sensor networks" 7th Annual ACM International Conf on Mobile Computing and Networks-MobiCom July 2001.
33. M. Luk G. Mezzour V. GLigor and A. Perrigo "MiniSec: A Secure Sensor Network Communication Architecture" IEEE International conf on Information Processing in Sensor Networks 2007.
34. C. Karlof D. Wagner and N. Sastry "Tiny Sec: a link layer security architecture for wireless sensor networks" Second International conference on embedded networked sensor systems pp. 162-175 2004.
35. Fadi Aloul and Mokhtar Aboelaze "Current and Future Trends in Sensor Networks: A Survey" IEEE-2005.

36. Feng Rui and Hu Xiangdong "Message Broadcast Authentication in uTESLA Based on Double Filtering Mechanism" International Conference on Internet Technology and Applications (iT AP) pp. 1 4-18 Aug. 2011.
37. V. Bapat P Kale V. Shinde N. Deshpande and A. Shaligram "WSN application for crop protection to divert animal intrusions in the agricultural land" Computers and electronics in agriculture vol. 133 pp. 88-96 2017.
38. A. Rani and K. Sanjeet "A survey of security in wireless sensor networks" 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) 2017.
39. Y. Zhang "The authentication scheme of WSN based on certificateless cryptography" morden computer vol. 2013 no. 15 pp. 8-12.
40. S. S. Al-Riyami and K. G. Paterson "Certificateless public key cryptography" International conference on the theory and application of cryptology and information security 2003.
41. A. Mnif O. Cheikhrouhou and M. B. Jemaa "An ID-based user authentication scheme for Wireless Sensor Networks using ECC" ICM 2011 Proceeding. IEEE 2011.
42. Y. M. Tseng S. S. Huang T. T. Tsai and J. H Ke "List-free ID-based mutual authentication and key agreement protocol for multiserver architectures" IEEE Transactions on Emerging Topics in Computing vol. 4 no. 1 pp. 102-112 2015.
43. Q. Xie D. S. Wong G. Wang X. Tan K. Chen and L. Fang "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model" IEEE Transactions on Information Forensics and Security vol. 12 no. 6 pp. 1382-1392 2017.
44. Y. Lu L. Li and H. Peng "A lightweight ID based authentication and key agreement protocol for multiserver architecture" International Journal of Distributed Sensor Networks vol. 11 no. 3 pp. 635890 2015.
45. G. Yang and H. B. Cheng "An efficient key agreement scheme for wireless sensor networks" Acta Electronica Sinica vol. 2008 no. 07 pp. 1389-1395.
46. H. M. Yang Y. X. Zhang and Y. Z. Zhou "Certificateless two-party authenticated key agreement protocol based on bilinear pairings" Journal of Tsinghua University (Science and Technology) vol. 52 no. 09 pp. 1293-1297 2012.

.