New Algorithm for Chunks Based Transfer and Image Rotation CAPTCHA Validation

Ritika Sharma, Charu Shree, Manish Kumar

Arya institute of Engineering and Technology

Corresponding author: Ritika Sharma, Email: ritikas59@gmail.com

In the case of the Wireless Sensor Networks, the two main issues which are required to be highlighted, first is the authentication of the nodes, that is nodes which are participating in the communication process, need to verify their identity. Secondly, the data communications how we can save the nodes from get overloaded in the data communication process, when the communication channel is of low quality. The authentication password which we have generated with the combination of the photo based SHA-512 extract and the pattern generated using image CAPTCHA , are then tested with the various online tools for the examination of the strength of the pattern and simultaneously we test the patterns which are obtained from the base papers. The results are compared on the basis of the years required to crack the pattern as well as on the basis of entropy, and results shown that the proposed work perform better in all respects.

Keywords: Wireless Sensor Network,Security, SHA-512

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 765–778. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-72

1. Introduction

Wireless Sensor Network (WSN) that can be characterized as the wireless network which comprises many distributed arrangement of the sensor nodes that gather data from its encompassing condition and also the sensor nodes, process the data and screen them. The sensor nodes utilized in WSN speak with different nodes in wireless way. Sensor hub normally have low memory, low battery control, constrained computational capacity and low data transfer capacity. Sensor nodes are low power gadgets that straightforward calculations are performed on nearby data. The sensor nodes are low on expense as they can be utilized many. [1]

The fundamental capacity of sensor nodes in WSN are as:-

1. Nodes sense nature
2. Nodes preprocess the data and give stockpiling to data and data
3. Nodes speak with base station and others nodes

In WSN, sensor nodes are sent in condition that is just gotten to by remote or they are inaccessible. [1]

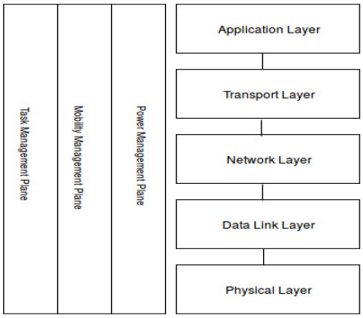

Fig 1 WSN Architecture Model [2]

In WSN, sensor nodes gathered data is the secret and profitable once in a while that is access by just approved clients. These sensor hubs are self sent in condition so they fit to self compose them after the arrangement. Sensor nodes in WSN are self sorted out, self continuing, great adaptability of network and capacity to remain in bad condition. The WSN is asset obliged as far as vitality, memory, calculation capacity and the scope of transmission. Structuring of conventions in WSN. Power the board is the primary issue for the originators. [1]

Wireless Sensor Network pursues the OSI engineering model which has five layers and three cross layers. In sensor network, there are five layers to be specific Application, Transport, Network, data Link layer and physical layer. These layers are utilized to achieve the network and make sensors cooperate. The three cross layers

are Task Management plane, Mobility Management Plane and power Management plane. [2]

WSN can be sent in condition in different ways like ad-hoc, Centralized and Distributed.

Customer verification is a mean of recognizing the customer and affirming that the customer is allowed to get to a few restricted organizations. Customer confirmation implies developing an association between the customer and some person. A person is the peculiarity property of a customer which ideally can't be produced or copied. Before long, characters are realized by things which customers know (passwords), have (secret keys or security tokens) or properties which they have (biometrics). [2]

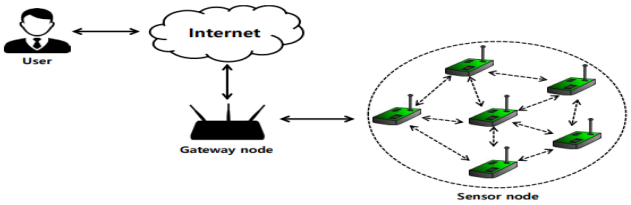

Fig 2: Authentication model in wireless sensor network.

1.1 Factors of Authentication

- Existing authentication techniques include three essential "factors":
- Something the client knows (e.g., secret phrase, PIN, pass phrases);
- Something the client has (e.g., keys, badges, ID, tokens, ATM card, brilliant card); and
- Something the client is (e.g., biometric trademark, for example, DNA, fingerprints, voice coordinate, quality, retinal output).

2. Literature Survey

G. Yıldırım and Y. Tatar, 2018 [1] In this paper, first, the investigation and the need of the proposed framework are talked about. Then, at that point, the framework is reenacted in the OPNET Modeler stage to spread the word about correlations with well customary WSN asset sharing components. At long last, the actual examination trial of the framework is completed on an Open Stack-based cloud framework, and the accomplishment of the framework is shown.
P. Li, *et.al* 2019 [2] Wireless transmission technique in wireless sensor networks has advanced higher prerequisites for private assurance innovation. As per the parcel misfortune issue of private security calculation dependent on cut innovation, this paper proposes the data private insurance calculation with repetition component, which guarantees protection by protection homomorphism system and ensures

excess via conveying stowed away data.
Besides, it chooses the directing tree produced by CTP (Collection Tree Protocol) as steering way for data transmission. By isolating at the source hub, it adds the secret data and furthermore the protection homomorphism. Simultaneously, the data input tree is set up between the objective hub and the source hub. Furthermore, the objective hub promptly sends the parcel misfortune data and the encryption key by means of the data input tree to the source hub. Therefore, it works on the unwavering quality and protection of data transmission and guarantees the data excess.
M. U. H. Al Rasyid*et.al* 2015 [3] In the current review, the utilization of EMG can be extended by using WBAN that can send data through the network, so the consequences of the EMG sensor not really set in stone and dissected by a doctor or a specialist regardless of the distance separated with patients. Execution and observing of the EMG sensors in utilizing a Wireless Body Area Network, is extremely useful for patients through applications that can be gotten to by cell phones. The various sorts of gadgets are not an obstruction to the application can run on an assortment of gadgets with various screen sizes and details.
J. Nelson et al. 2021 [4] A coordinated printed circuit board radio wire was planned and executed to bring down cost. A safe entryway was executed to move data to a database for perception. The framework was approved by estimating the power utilization, radio wire return misfortune and parcel steering in the working climate. Five days of temperature, stickiness and CO2 data recorded from a sensor hub is introduced.
H. Wang, et.al 2011 [5] the automated idea of wireless sensor networks make them truly helpless against the malevolent assaults. Accordingly, how to finish secure data assortment under various conditions is the vital issue to wireless sensor networks. There have been a couple on-going examination endeavors about multipath steering for secure data assortment. In this paper, we utilize the transmission message when wireless sensor network instates to develop secure multipath directing for secure data assortment which will make minimal overhead the sensor hubs in the network. As per the reproduction results, the calculation in this paper contrasts and other ongoing investigates is better.
M. U. H. Al Rasyid et.al 2015 [6] The proposed work is carried out in Network Simulator 2 (NS2). The presentation of the convention CSMA/CA was assessed for WSN star geography. The reenactment results show that of unslotted CSMA/CA is better compared to opened CSMA/CA as far as the parcel achievement likelihood, energy utilization, and postponement. While opened CSMA/CA is better compared to unslotted CSMA/CA in term of throughput.
Fei Gao, et.al 2015 [7] How to expand lifetime of wireless sensor networks (WSNs) is as yet an open issue for analysts. In past years, there are two principle strategies were created for working on the lifetime of WSNs: One is to level energy utilization of networks, and another is to further develop energy productivity of hubs in networks.
In this paper, the creators proposed a multi-jump directing convention dependent on the LAR calculation and cross-layer system. In the proposition, the data both a hub's lingering energy and the separation from it to the following jump hub are considered with various balance weight factors. The consequences of examining and animating show that our proposition is effectively both on evening out the hubs energy utilization

and diminishing the network bundle misfortune rate. Additionally, the lifetime of networks has been prolonger than LAR.
F. Z. Glory et. al 2019 [8, 10] suggested the process of authentication of the user using the algorithm which generates the password using the random combination of the words and numbers. Password which generated is based on the dynamic inputs like the favorite name of the novel, the number of grandmother's children, secret dates etc
Shah ZamanNizamani et.al 2017 [9, 11] In this paper a text based client confirmation conspire is proposed which works on the security of printed secret phrase plot by altering the secret phrase input strategy and adding a secret key change layer. In the proposed conspire alphanumeric secret key characters are addressed by irregular decimal numbers which oppose online security assaults, for example, shoulder surfing and key lumberjack assaults [12].

3. Proposed Work

The proposed concept working in the modules of the user authentication and data file sharing in Wireless Sensor Networks for transfer data from one node to another node based on advanced Chunks based transfer and image rotation CAPTCHA validation algorithm.

3.1 Algorithms

Algorithm In our methodology, at first, we take input information from the user who is asking for a password. The input information consists of image. In our methodology, the number of input image rotation is kind of arbitrary. On the other hand, the number of input texts has some base-analogy. If we take only two texts as input, our system will use these two texts for password generation. Then if somehow the adversary can know or detect the input texts he can surely think that both these two texts are used in the password. So from the security perspective, we have increased the number of image to five where it can ensure some randomness for password generation. Now, think about the case if the number of input texts increases from five to ten for password generation. We can say that this input will be much secured as it will have more randomness than using five input images. Even if the adversary knows all the ten texts prompted to the system, he can never know the chosen ones from them by our generator for generating passwords. But from the user's perspective, inputting this large number of images can make the process slow and complicated and also can annoy the users. So we have picked the number "5" for images.

1: Begin Procedure
2: data 4— five Images and two numbers
3:N 4— number of demanded passwords (from 1 to 10)
4: specialchars 4— { @ , $, !, # , % , & , (,), 0, 3, 8, < , |}
5: punctuation 4 - {,*,+ ,-,:," ,/,\,~ ,? ,[,],{ ,} ,$,!,# ,% ,& ,(,),_ ,< ,|}
6: while N > 0 do
7: stringl 4— randomly selected from five Images
8: string2 4— randomly selected from four Images
9: Number 4— randomly selected from two numbers

10: stringl 4— capitalize (stringl) some letters randomly
11: string2 4— capitalize (string2) some letters randomly
12: Final_string 4— merge stringl and string2 randomly
13: Alphabets 4— {a, s, i, r, x, q, c, j, o, e, b, k, 1}
14: Final_string 4— Final_string. replace(Alphabets, specialchars)
15: Final_string 4— randomly insert Number in the final string
16: either in the middle, or in the beginning or in the end of it
17: Final_string 4— randomly append one special character from
18: punctuation at the end of the Final string
19: C = len (Finaljstring)
20: if C < 8 then
21: Final_string 4— append (8 - C) special characters randomly
22: print Final_string
23: end if
24: N 4— N — 1
25: end while
26: End Procedure

3.1.1 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: Image Based Captcha

And we have these angles

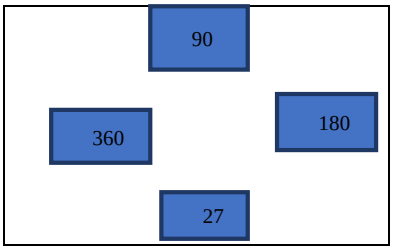

Fig. 4: Rotation Angles

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 [13].The fig. 5 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

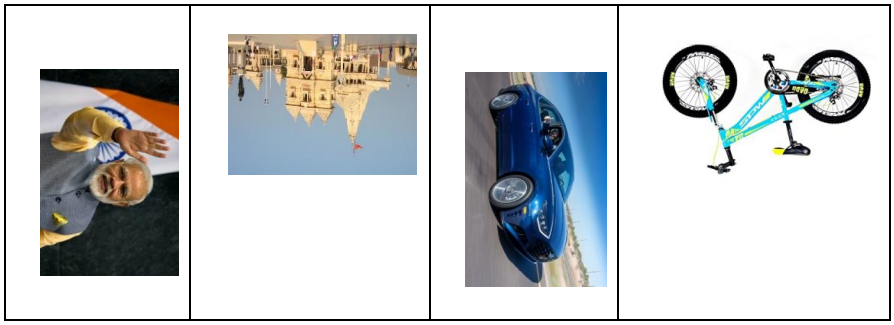

Fig. 5: sample for Rotate CAPTCHA

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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.2 Processing of SHA 512

SHA-512 is a function of cryptographic algorithm SHA-2, which is an evolution of famous SHA-1.SHA-512 is very close to Sha-256 except that it used 1024 bits "blocks", and accept as input a 2^128 bits maximum length string. SHA-512 also has others algorithmic modifications in comparison with Sha-256.

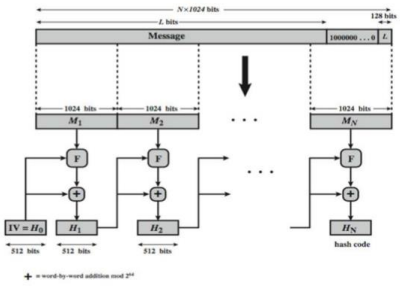

Fig. 6: Processing of SHA 512 for single 1024 Bit Block

4. Implementation and Result Analysis

The implementation of the network is simulation in VS 2010

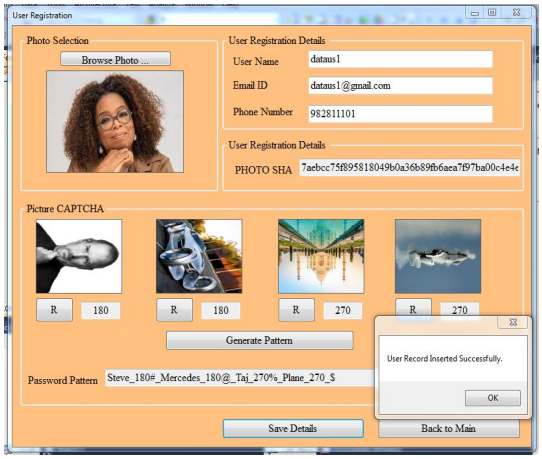

Fig.7: User Registration

The fig.7 shows that in order to simulate the user interaction, the users are required to be created. The user 1 is dataus1, and the process of first user creation is explained. In this process, first the user photo is required to be selected, the SHA-512 will get generated for the photo [14, 15]. The second phase is the image captcha, in which images are displayed and we will click on them to rotate then, as then click on the generate button, which will generate the pattern based on the rotation of the images and after that save the details [16].

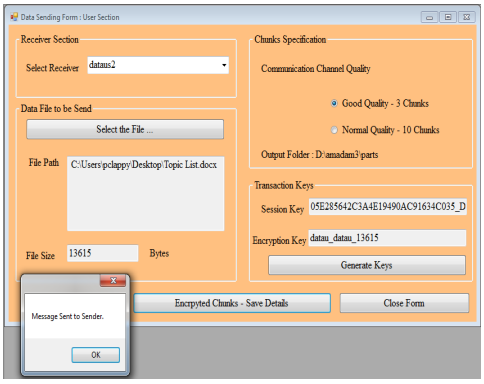

Fig. 8: Data Sending

In the send section, we will click on the Send Data in order to communicate with the receiving node. In this we will have to first select the file which is containing the data, which we want to send. After the specification of the receiver, the receiver name can be

selected for the combo box, which contains the user names fetched from the database table.

The second step is for the specification channel quality and which can be good or normal , the channel quality will able to determine the number of chunks in which the main file , which is to be send to the receiver.

Now, the session key and encryption key will be generated and the basis for the First 5 character extracted from the sender name, next the 5 character extracted from the receiver name, size of file.

E.g Sender is :demoXuser
Receiver is :Kapiljpr
demoXu_Kapilj_11189

4.1 Result Analysis

4.1.1 Comparison on Basis of Paper 1

F. Z. Glory, A. UlAftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based on User Inputs," 2019
Base Paper Password Pattern
{urAn29iRfan-

Proposed Password Pattern
dcec96dc8825e96bd0512d9fae6a28ae73f_Steve_90#_Mercedes_180@_Taj_90%_Plane_180_$
Thus, the results on the basis of the time period required are summarized in the table 4.1.

Table 4.1: Result Analysis on Basis of Time Period Comparison with Paper 1

Website/Tool	Base Result	Proposed Result
Password Monster Tool	0.000005 trillion years	10 thousand trillion trilliontrilliontrilliontrilliontrilliontrillion years
Thycotic.com Password Checker Tool	1.86E-67 quattuorvigintillions years	341,714,432 quadragintillion years
How Secure is My Password Checker Tool	4.6E-68 quattuorvigintillions years	85 million quadragintillion years

The results on the basis of the time period required are summarized in the table 4.2.

Table 4.2: Result Analysis on Basis of Entropy Comparison with Paper 1

Website/Tool	**Base Result**	**Proposed Result**
Rumkin Tool	60.9 bits	377.5 bits
Password.Blue Tool	43 bits	240 bits

4.1.2 Comparison on Basis of Paper

The paper 2 which we have taken for analysis or comparison of strength is, Shah ZamanNizamani, Syed Raheel Hassan, Tariq JamilKhanzada and MohdZalishamJali, "A Text based Authentication Scheme for Improving Security of Textual Passwords", 2017

Base Paper Password Pattern

g m x F G P X)>

Proposed Password Pattern

dcec96dc8825e96bd0512d9fae6a28ae73f_Steve_90#_Mercedes_180@_Taj_90%_Plane_180_$

Thus, the results on the basis of the time period required are summarized in the table 4.3.

Table 4.3: Result Analysis on Basis of Time Period Comparison with Paper

Website/Tool	**Base Result**	**Proposed Result**
Password Monster Tool	1 billion trillion years	10 thousand trillion trilliontrilliontrilliontrilliontrilliontrillion years
Thycotic.com Password Checker Tool	2.0E-60 quattuorvigintillions years	341,714,432 quad ragintillion years
How Secure is My Password Checker Tool	6.0E-61 quattuorvigintillions years	85 million quadragintillion years

The results on the basis of the time period required are summarized in the table 4.4.

Table 4.4: Result Analysis on Basis of Entropy Comparison with Paper 2

Website/Tool	**Base Result**	**Proposed Result**
Rumkin Tool	79.7 bits	377.5 bits
Password.Blue Tool	56 bits	240 bits

4.1.3 Mathematical Justification

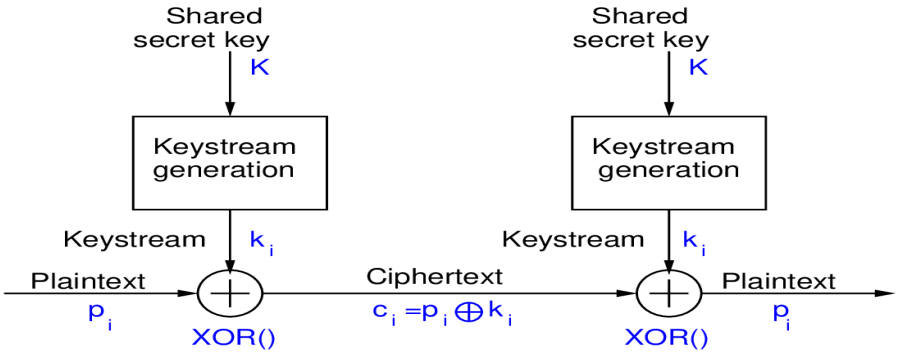

Fig. 9: Mathematical model in proposed work

5. Conclusion

Wireless Sensor Networks are today becoming the part of each and almost every organization, whether we are talking about defense, banking, education and more. In such an environment, we require the data should be shared effectively and securely. In the case of the Wireless Sensor Networks, the two main issues which are required to be highlighted, first is the authentication of the nodes, that is nodes which are participating in the communication process, need to verify their identity. Secondly, the data communications how we can save the nodes from get overloaded in the data communication process, when the communication channel is of low quality. The authentication password which we have generated with the combination of the photo based SHA-512 extract and the pattern generated using image CAPTCHA , are then tested with the various online tools for the examination of the strength of the pattern and simultaneously we test the patterns which are obtained from the base papers. The results are compared on the basis of the years required to crack the pattern as
well as on the basis of entropy, and results shown that the proposed work perform better in all respects.

6. Future Scope

Later on, we further prefer to reach out in the field of the retina based passwords, video based passwords and more aspects in the Wireless Sensor Networks and security in data communication

.

References

[1] G. Yıldırım and Y. Tatar, "Simplified Agent-Based Resource Sharing Approach for WSN-WSN Interaction in IoT/CPS Projects," in *IEEE Access*, vol. 6, pp. 78077-78091, 2018.

[2] P. Li, C. Xu, H. Xu, L. Dong and R. Wang, "Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks," in *China Communications*, vol. 16, no. 5, pp. 158-170, May 2019.

[3] M. U. H. Al Rasyid, D. Prasetyo, I. U. Nadhori and A. H. Alasiry, "Mobile monitoring of muscular strain sensor based on Wireless Body Area Network," *2015 International Electronics Symposium (IES)*, 2015, pp. 284-287.

[4] J. Nelson *et al*., "Wireless Sensor Network with Mesh Topology for Carbon Dioxide Monitoring in a Winery," *2021 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNeT)*, 2021, pp. 30-33.

[5] H. Wang, G. Yang, J. Xu, Z. Chen, L. Chen and Z. Yang, "A noval data collection approach for Wirelsee Sensor Networks," *2011 International Conference on Electrical and Control Engineering*, 2011, pp. 4287-4290.

[6] M. U. H. Al Rasyid, I. U. Nadhori, A. Sudarsono and R. Luberski, "Analysis of slotted and unslotted CSMA/CA Wireless Sensor Network for E-healthcare system," *2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*, 2014, pp. 53-57.

[7] FeiGao, Hongli Wen, Lifen Zhao and Yuebin Chen, "Design and optimization of a cross-layer routing protocol for multi-hop wireless sensor networks," *PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System*, 2013, pp. 5-8.

[8] 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.

[9] Shah ZamanNizamani, Syed Raheel Hassan, Tariq JamilKhanzada and MohdZalishamJali, "A Text based Authentication Scheme for Improving Security of Textual Passwords" International Journal of Advanced Computer Science and Applications (ijacsa), 8(7), 2017.

[10] H. Kim, J. Han and Y. Lee, "Scalable network joining mechanism in wireless sensor networks," *2012 IEEE Topical Conference on Wireless Sensors and Sensor Networks*, 2012, pp. 45-48.

[11] Y. Nishikawa *et al*., "Design of stable wireless sensor network for slope monitoring," *2018 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, 2018, pp. 8-11.

[12] 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.

[13] Maru U., Sujediya G., Saini Y. (2021), "Color Image Encryption and Compression Using DCT in Joint Process",*Proceedings of International Conference on Communication and Computational Technologies,* Algorithms for Intelligent Systems, Springer.

[14] TarekAzzabi and HasseneFarhat "A Survey On Wireless Sensor Networks Security Issues And Military Specificities" International Conference on Advanced Systemsand Electric Technologies (IC_ASET) 2017.

[15] 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.

[16] 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.

[17] PrernaMahajan 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.
[18] 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.
[19] Rajat Gupta Pallavi Singh KaushalSultania and Archit Gupta "Security for Wireless Sensor Networks in Military Operations" Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT) 2013.
[20] Sattar J Aboud "An efficient method for attack RSA scheme" IEEE 2009.
[21] 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.
[22] B.Ayyappan and P. Mohan Kumar "Vehicular Ad Hoc Networks (VANET): Architecture methodologies and design issues" IEEE Conf Publication pp. 177-180 2016.
[23] Kaur, R., Kumar, S., & Shree, C., "Outlining Systemof C Compiler Algorithm for Retargetable Coding in Network Processors." Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 04-Special Issue, 2018.
[24] Kaur, R., Upadhyay, S., Joshi, J., & Shree, C. (2019, February). Classified Optimum Real Time Recognition And Extraction Of Multiple Object Through Surveillance Monitoring System. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.
[25] P Priyanka and B Ayyappan "Wireless sensor networks - technologies protocols applications and simulators: A survey" JCPS Journal 2015.
[26] 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.
[27] 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.
[28] 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.
[29] 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.
[30] FadiAloul and MokhtarAboelaze "Current and Future Trends in Sensor Networks: A Survey" IEEE-2005.
[31] 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.
[32] 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.
[33] A. Rani and K. Sanjeet "A survey of security in wireless sensor networks" 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) 2017.
[34] Y. Zhang "The authentication scheme of WSN based on certificate less cryptography" modern computer vol. 2013 no. 15 pp. 8-12.
[35] Y. M. Tseng S. S. Huang T. T. Tsai and J. H Ke "List-free ID-based mutual authentication and key agreement protocol for multi server architectures" IEEE Transactions on Emerging Topics in Computing vol. 4 no. 1 pp. 102-112 2015.
[36] 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.