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 Approach of Biometric Based Security Implementation in WSN

Sonam Badjatya[1], Mr. Rajveer Singh[2]

M.Tech Research Scholar[1], Assistant professor[2]

[1] *Department of Electronics and Communication Engineering((With Specialization in Digital communication), Rajasthan College of Engineering for women, Jaipur*

Abstract : Information security might be the fundamental a piece of the IT for the affiliations which are of each and every size and kind. Information security is additionally also called Information security (IS) or PC security. Occasions of information security headways integrate fortifications, information cross section and data crash. A key data security development live is coding, any place handled information, programming or even the hardware, and cumbersome drives are disrupted and a while later delivered the indiscernible to the unapproved clients and software engineers. one among the premier regularly drilled strategies for practicing information security is that the usage of verification. The proposed work incorporates the plan to stack the fingerprints or the image of the client , the dataset which are for the fingerprints which are taken for the unique mark reenactment of the enrolled clients. The client when snap on the pile photo get , pop will appear to pick the region where experiences the record contrasting with the unique mark. By then the SHA 256 computation will be incorporated for the age of the hash code which is related to the finger impression and furthermore make the mystery expression in relationship with the hash of the finger impression and the photograph which are utilized to produce the confidential key utilizing the SHA 256 calculation and the idea of the confidential key which are of the shipper and beneficiary for creating the meeting with the novel exchange id, the made Session Key and Private Keys will additionally raise the level of safety. The result assessment when diverged from the base work , by using the different on the web and disengaged instruments of enlisting the mystery word quality , exhibits that the piece quality is almost extended in overabundance of various times the base work and moreover the entropy for the confidential keys one which is created is extended to the broad total.

***IndexTerms* - Wireless Sensor Network , Data Security, SHA.**

I. Introduction

Wireless sensor networks (WSNs) have the force of disseminated correspondence, figuring, and detecting highlights. They are described as foundation less, issue lenient and self-sorting out networks which give amazing chances to minimal expense, simple to-apply, quick and adaptable establishments in a climate for different applications. [1]

The wireless sensor and the sensor node design are given in the graph underneath −[1]

1.1 Attributes of WSN

The attributes of WSN are as per the following −

- Asset requirements − Nodes of WSN are more modest in size and get power from the batteries. It legitimizes that assistance given by the nodes like correspondence and calculation measure of memory is exceptionally restricted.
- Correspondence worldview − The information driven component of WSN makes sense of its information driven nature and legitimizes that the correspondence is confined to nodes. [1]
- Application explicit plan − WSN is application explicit for example the engineering of WSN depends on application.[2]
- Node disappointment and untrustworthy correspondence − Various variables like unforgiving working circumstances prompting flimsiness, unusualness, nodal portability, natural impedances makes normal WSN nodes to be mistake inclined.
- Adaptability and thickness − The quantity of nodes in WSNs might be huge and thickly conveyed to a more serious level in different applications. [2]

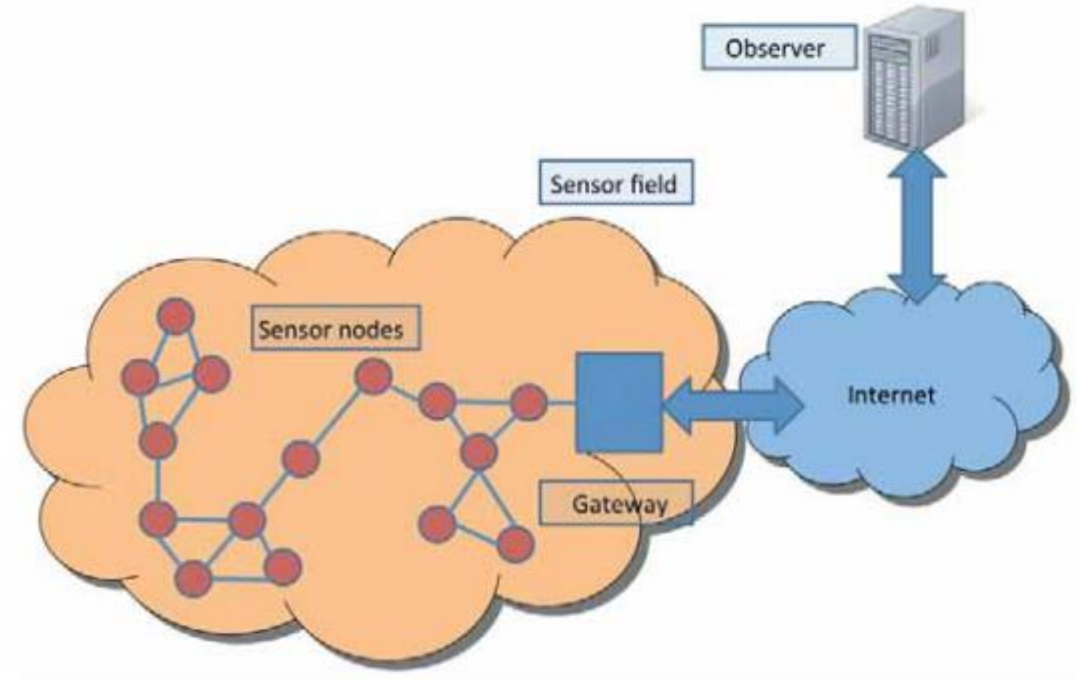


Fig 1.1 WSN

- Dynamic Topologies − Nodes are allowed to travel haphazardly at various velocities in couple of utilizations and here and there might neglect to work, to add or to supplant. So there can be different network geography.

- Correspondence models − WSNs utilize different correspondence models − Flat/progressive/disseminated WSNs; or homogeneous/heterogeneous WSNs. [2]

1.2 Working Environment

The WSNs are for the most part conveyed in remote and dangerous areas for unattended activities in view of their capacity to endure brutal natural circumstances. [3]

1.2.1 Prerequisites of WSN

The prerequisites of WSN are made sense of beneath:

- Adaptability − The engineering of WSN isn't fixed. Maybe it shifts from one application to another which legitimizes that the conventions and calculations have the qualities of self-association. [4]

- Adaptation to internal failure − The nodes in WSNs have the capacity to support the capacities completed in the network even in circumstances like restricted battery power, obstruction from outside sources, disappointment pace of nodes, unforgiving natural circumstances. [4]

- Lifetime − The two central point that ought to be thought about are load adjusting and energy saving. These two variables can improve the lifetime of the WSN design as far as might be feasible. [4]

- Adaptability − The quantity of nodes in a WSN network can be enormous. Likewise WSN engineering and conventions ought to be planned. [5]

- Ongoing − The Various capacities like detecting, handling and correspondence of WSN are utilized in different true issues so ought to follow rigid time. [5]

- Security − For instance in medical services information and military information, the information presented by WSN network are private which are delicate in nature. So security is obvious in such structures. [5]

- Creation cost − The expense of nodes in WSN network must be low as once the nodes run out of the energy it must be supplanted by fresher nodes.[5]

- Sending − In enormous scope WSNs, there is arbitrary organization of nodes whose support and substitutions are not for all intents and purposes conceivable. So there is an immense prerequisite of re-arrangement and once again programming. [6]

- Reliability − One can depend on WSN as the structural plan is strong that prompts secure assortment of information and solid conveyance with no misfortune. [6]

II. Literature Review

F. Z. Greatness et. al 2019 [7] proposed the course of check of the client using the appraisal which makes the mysterious explanation using the conflicting mix of the words and numbers. Secret word which passed on relies upon serious areas of strength for the of data like the most loved name of the novel, how much grandmother's young people, secret dates, etc.

G. Wei and K. Wu, 2019 [8] Because wireless sensor association (WSN) centers have the constraints of low accumulating assets, slight enlisting power and less electric power, the paper proposes a matching free certificateless security affirmation plot for WSN considering ECC assessment. The plan perceives shared approval, key cognizance and meeting key update of centers in the association utilizing ECC point increment calculation and AES symmetric encryption assessment. Basing on this, creators investigate the precision and security, it shows that the course of action has two-get-together affirmation, forward security, amazing forward security, known-key security, taking steps to key spillage cover and other security credits. At last, producers make the authentic assessment of the introduction of the game plan, and a brief time frame later creators execute the multiplication on the supporting of OMNET++ basing on the language of C++. Separating and different plans, their course of action has less energy use and execution time, which can determine the issues of WSN better.

R. Maidhili and G. Karthik, 2018 [9] Wireless sensor networks (WSN) consolidates many loads with sensor center points. All the sensor center points in the social event joins and dnamically broadcast the most recent perceived information in the association. Because of the scattered quality and sending nature of WSNs, they are nearly utilized in each of the industrious applications for which multi client approval is necessitous which can at any rate incite copy assaults (Attacker center go most likely as genuine center point and sends misdirecting transmission messages in the association).

An Identity based plan nearby sink center point is proposed to give a defended transmission approval and limits the transmission rates and assessment considering ECC (Elliptical Curve Cryptography). At first the sink center point produces public and confidential keys considering center point ID utilizing ECC and dissipates the confidential key to the center in the association and public key to the client. The client encodes and broadcast the control message utilizing the public key to underwrite its approval while the center unscrambles the transmission message utilizing its confidential key given by the sink. Tolerating that the engraving gets embraced the center point and the client will support one another, else the association will be denied which can forestall imitate assault. In the assault situation, expecting the aggressor articulates to be a genuine client and sends counterfeit transmission messages, the attacker is dug due to the befuddle that happens while the engraving is avowed. This affirmation plot gives high security and disorders the assailant from the association. WSN consumes high energy during information transmission. To improvise the energy ampleness this task takes advantage of low energy utilization MAC shows. An energy-helpful information course of action is done in WSNs by arranging IEEE 802.15.4/ZigBee guidelines in MAC layer. The standard objective of the proposed work is to perform conveyed after check, to thwart asset consuming assaults through affirmation and to diminish the energy wastage nearby security in WSN correspondence.

E. H. Teguig, et. al 2017 [10] In wireless sensor networks, guaranteeing got trades during plan pondering targets, for example, ideal use of assets ought to be examined truly. Ordinarily, starting trades require the evaluation of a mystery key involving ECDH with power demand or executing ECDSA assessments for signature suggesting huge computations and two or three transmissions between sensor center points. In this paper, producers propose another part for public keys the board utilizing an elliptic bends cryptosystem where the goal is to redesign drugs by diminishing all around the estimation of scalar duplications. Subsequently, public keys trade instrument permits a lacking correspondence by sending basically the abscise and the LSB of the ordinate of the elliptic bend point adding up to 161 pieces rather than 320 pieces. To show benefits of their obligation, creators view at its showcases to the degree that execution time and execution to ECDH, ECDSA and ECIES by performing genuine tests on a TMote Sky sensor.

G. Choi and I. Lee, 2017 [11] Today, wireless sensor networks are generally utilized considering the climb of the Internet of Things. These networks convey in uncovered conditions and as such they are helpless against clear impedance by aggressors. Also, by its certifiable nature, the Wireless Sensor Network climate is restricted in its ability to oversee maybe delicate data by virtue of light security structure. Consequently, this study has been supposed to draw in the work environment of secretive client confirmation and meeting key scattering in the transmission of delicate information much more safely through correspondence planning with sensors. It also gives client indefinite quality on the association with the objective that the personality of the carrier or beneficiary can't be avowed, and proposes major areas of strength for an against refusal of-association assaults and caricaturizing assaults.

S. Pirbhulal, et. al 2016 [12] Wireless Body Sensor Networks (WBSNs) are broadly utilized for clinical advantages seeing applications. Inferable from the meaning of secret and security, the transmissions of clinical data in WBSNs ought to be genuinely shielded. This examination intends to develop an Intel Galileo based WBSN stage. The physiological properties, for example, (Electrocardiogram) ECG got from human body can be utilized as unambiguous way for substance indisputable pieces of check (EIs) to confirm information in WBSNs. In this paper utilizing Matlab programming, creators besides analyzed the demonstration of some of really evolved padded vault based information affirmation methodology for part ID in WBSNs.

III. PROPOSED WORK

3.1 Registration Phase

I. Algorithm for Node A and Ticket Server S Interaction

Step 1: Whenever a node want to authenticate itself. Initially, it requires its authentication ticket from the Ticket Server. The sensor node A will request the ticket Server S for ticket initiating the request.

$$A \rightarrow S:\{ID_a,\{N_a\}_{Kas}\}$$

Step 2: The request message has ID of node A ID_a and Nonce encrypted with secret key Kas which is shared with ticket server S, using the finger print and photo.

Step 3: The Ticket Server decrypt the received request with Shared Secret Key (Kas) and verify the freshness of nonce to generated a ticket for node A. The ticket of node A is denoted by $Ticket_a$ which contains the ID of node A (ID_a) ,ID of Ticket Server S (ID_s), Time stamp for sensor node A (TS_a) and Life time (L_a) for the validity of ticket for sensor node A which are encrypted with private key of ticket server KR_s.

$$Ticket_a=\{Id_a,Id_s,TS_a,L_a\}_{KRs}$$

II. Algorithm for Node B and Ticket Server S Interaction

Note: The Sensor node B also requires its authentication ticket from Ticket Server S by following above steps. The ticket of sensor node B is:

$$Ticket_b=\{Id_b,Id_s,TS_b,\ L_b\}_{KRs}$$

The ticket of sensor node B is denoted by $Ticket_b$, which contains the ID of node B (ID_b) ,ID of Ticket Server S (ID_s), Time stamp for sensor node B (TS_b) and Life time (L_b) for the validity of ticket for sensor node B which are encrypted with private key of ticket server KR_s.

3.2 Authentication Phase

I. Algorithm for Node A to node B Interaction

Step 1: Sensor Node A authenticates itself and sends its identity (ID_a) and authentication ticket ($Ticket_a$) to sensor node B.

$A \rightarrow B$: $\{Id_a$, $Ticket_a\}$

Step 2: The transaction ID is acts as the ID and the generation of the key using the SHA code of the private key of the user 1 and the private key of the user 2

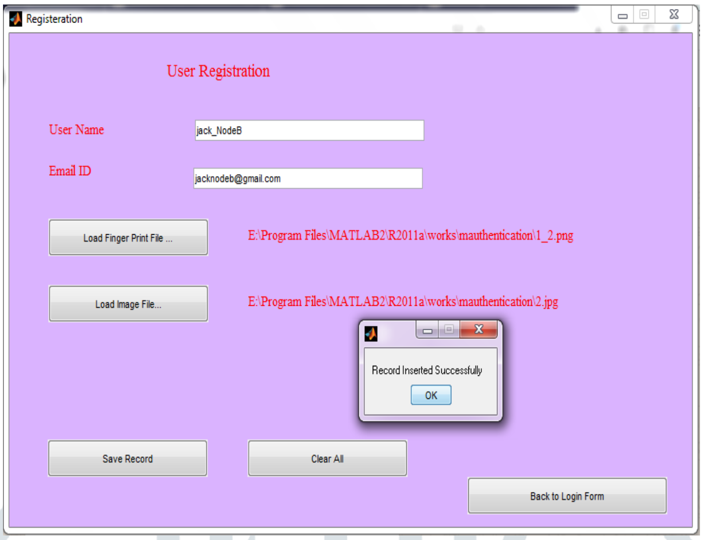
$B \rightarrow A$: $\{Id_b$, $Ticket_b\}$

Step 3: Sensor node A receives the ticket and identity of node B and decrypted with private key of ticket server KRs. If, successful, then node B is authenticated or it is a legitimate node.

Hence sensor node A and sensor node B is mutually authenticated.

IV. Implementation and Result Analysis

Implementation is performed using the MATLAB.



User Name: jack_NodeB

Email ID: jacknodeb@gmail.com

E:\Program Files\MATLAB2\R2011a\works\mauthentication\1_2.png

E:\Program Files\MATLAB2\R2011a\works\mauthentication\2.jpg

Record Inserted Successfully

Fig 4.1 Implementation

Table 4.1 Test Result Analysis Table Proposed Work

OTP	Website/Tool	Result
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Password Blue	154 bits
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Rumkin	200.3 bits
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Password Monster	4 billion trillion trillion trillion years

Table 4.2 Test Result Analysis Table Base Work

OTP	Website/Tool	Result
@Six29ol!vEr_	Password Blue	36 bits
@Six29ol!vEr_	Rumkin	62.2 bits
@Six29ol!vEr_	Password Monster	35 Years

V. Conclusion

The information correspondence is the significant piece of the general working of the web or some other correspondence organization. Its on the regular schedule that we share the in the middle of between the clients. Be that as it may, the issue which we face on broad premise is the connection of as far as possible to a specific size which is permitted to be sent at a time. In the event that the size of the record is diminished to an impressive sum, more number of documents can be sent at a time. In the idea which we have proposed we have adopted the papers and strategies connected with Discrete Cosine Transformation and Singular Value Decomposition. In the algorithm of the image compression which we have proposed , we have joined the idea of the DCT and SVD to get the better compression proportion and these radios we have communicated in the outcome investigation and in the changed consolidated approach , we have obtain the improved outcomes.

REFERENCES

1. V. O. Nyangaresi, E. W. Abood, Z. A. Abduljabbar and M. A. Al Sibahe, "Energy Efficient WSN Sink-Cloud Server Authentication Protocol," *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, 2021, pp. 1-6.

2. A. Kore and S. Patil, "Reliable and Secure Data Transmission in Smart Healthcare Application of Internet of Things," *2021 IEEE Bombay Section Signature Conference (IBSSC)*, 2021, pp. 1-6.

3. A. A. Islam and K. A. Taher, "A Novel Authentication Mechanism for Securing Underwater Wireless Sensors from Sybil Attack," *2021 5th International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, 2021, pp. 1-6.

4. M. R. Mortada, A. Nasser, A. Mansour and K. C. Yao, "LIBRO: A Location Information Based Routing Protocol for Multi-Hop WSN Applications," *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1-6.

5. M. Alotaibi, "Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN," in *IEEE Access*, vol. 9, pp. 159187-159197, 2021.

6. A. Kumar and B. Kaur, "Improved Elliptic Curve Digital Signature Algorithm in Wireless Sensor Networks," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2021, pp. 1-5.

7. 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.

8. G. Wei and K. Wu, "Paring-free certificateless security authentication scheme for WSN based on ECC," *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*, 2019, pp. 1355-1360.

9. R. Maidhili and G. Karthik, "Energy Efficient and Secure Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks," *2018 International Conference on Computer Communication and Informatics (ICCCI)*, 2018, pp. 1-6.

10. E. H. Teguig, Y. Touati and A. Ali-Cherif, "ECC Based-Approach for Keys Authentication and Security in WSN," *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, 2017, pp. 1-4.

11. G. Choi and I. Lee, "A key distribution system for user authentication using pairing-based in a WSN," *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017, pp. 1-4.

12. S. Pirbhulal, H. Zhang, W. Wu and Y. -T. Zhang, "A comparative study of fuzzy vault based security methods for wirless body sensor networks," *2016 10th International Conference on Sensing Technology (ICST)*, 2016, pp. 1-6.

13. P. Joshi, M. Verma and P. R. Verma, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN," *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2015, pp. 527-532.

14. P. Zhou, M. Xiao and Z. Xia, "A Message Authentication Method for Wireless Sensor Networks Using Polynomial Interpolation," *2015 2nd International Symposium on Dependable Computing and Internet of Things (DCIT)*, 2015, pp. 151-153.

15. M. Sarvabhatla and C. S. Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN," *2014 Fourth International Conference of Emerging Applications of Information Technology*, 2014, pp. 367-372.

.