International Journal For Technological Research In Engineering
Volume 6, Issue 12, August-2019 *ISSN (Online): 2347 - 4718*

NOVEL ALGORITHM FOR MUTUAL AUTHENTICATION USING FINGER PRINT AND PHOTO BASED KEY

Sushma Dagur[1], Yogesh Kumar Tiwari[2]
[1]M.Tech Scholar, [2]Assistant professor HOD (ECE specialization in Digital Communication),
[1,2]Chandravati Group of Institutions, Bharatpur.

Abstract: ***Wireless Sensor Network comprises of a few wireless nodes which are scattered and devoted sensors found physically to be utilized for observing of the encompassing natural conditions. The proposed work incorporates the plan to stack the unique finger impression/image of the customer , the dataset for the finger impression is taken for the unique finger impression reenactment of the enrolled customers. The customer when snap on the store photo get , pop will appear to pick the region where lives the record contrasting with the unique mark. By then the SHA 256 estimation will be incorporated for the age of the hash code which is related to the unique mark and furthermore make the mystery expression in association with the hash of the finger impression and the photograph which are utilized to create the private key utilizing the SHA 256 calculation, the outcome identified with security are very compelling.***

Keywords: WSN , Sensor Nodes, Mutual Authentication, Finger Print and photo

I. INTRODUCTION

In a wireless sensor network, a foe can without quite a bit of a stretch imbue messages. The recipient needs to guarantee that the information used in any fundamental initiative technique starts from the genuine source. Information authentication keeps unapproved parties from sharing in the network and genuine components should have the choice to recognize messages from unapproved substances and reject them. Measures for guaranteeing reliability are seen as critical to recognize message adjustment and to reject mixed message.[1] In the symmetric key cryptography, MACs are used to give authentication. The sender and the authority share a riddle key to process a message authentication code (MAC) of all conferred information. Exactly when a message with a correct MAC arrives, the recipient understands that it almost certainly been sent by the principal sender. In the open key cryptography, propelled imprints are used to seal a message as a technique for authentication. A propelled imprint is a numerical arrangement for demonstrating the validness of an automated message or a record. A genuine electronic imprint gives a recipient inspiration to acknowledge that the message was made by a known sender, and that it was not balanced in movement. Propelled imprint incorporates generously more estimation overhead in stamping, translating, checking and encoding exercises than frameworks used in symmetric cryptography [2].

Customer authentication is a mean of recognizing the customer and affirming that the customer is allowed to get to some constrained organizations. Customer authentication means working up an association between the customer and some character. A character is the peculiarity property of a customer which ideally can't be fabricated or copied. Before long, characters are completed by things which customers know (passwords), have (secret keys or security tokens) or properties which they have (biometrics). [3] In WSN, access to the assembled information will all things considered not be free since sending of WSNs starts a couple of costs of game plan. This infers the association workplaces will make the identified information open just to explicit people, generally the people who pay for getting the organization. For this circumstance, a WSN should undoubtedly perceive certified customers from the strange ones. In authentication, a customer sends his ID (e.g., name, IP address) and check of his character to a sensor with the objective that the sensor can pick whether the character is genuine and in reality has a spot with the customer of that name. Upon productive authentication, the sensor affirms the customer who is enabled access to the information.[3]

II. RELATED WORK

E. Yoon and K. Yoo,2011[4] Wireless sensor network (WSN) have been associated in different zones. Shared authentication is a huge organization in WSN. In 2010, Chen and Shih proposed a ground-breaking shared authentication (RMA) show for WSN. Regardless, this paper points out that Chen-Shih's RMA show has a couple of detriments: (1) customer emulate strikes by a malignant enrolled customer, (2) GW-center point emulate ambushes by a noxious selected customer, (3) sensor center point emulate attacks by a vindictive enrolled customer, (4) advantaged insider strikes, and (5) time synchronization issue.

Xin Liu, et.al 2013[5] With wireless sensor networks (WSNs) have been associated with various fields, its security issue has ended up being observable for whatever length of time that years. Hence it is critical to structure a sensible security authentication show for WSNs.

This paper proposes a one of a kind imprint based customer authentication show with one-time mystery key for WSNs. By differentiating and other pro's associated work, makers arrive at the assurance that their improved show has higher security and lower overhead execution than others.

H. H. Kim, et.al 2015 [6] The headway of mechanized correspondence time fuses the two contraptions and applications running on different stages. Focal points applications are required for a guard correspondence ensuring affirmation and trust organizations to the customers.

This paper demonstrates an authentication and session-key establishment show that enabling shared authentication strategy between included components in the WSNs.
This arrangement gives express security standards, for instance, information decency, message characterization and session key establishment to ensure security and insurance of the two information and network. To plot the likelihood of the work to genuine shows, makers emulate the session key establishment computation using Scyther gadget for WiMAX show measures. A wide examination exhibits that the proposed arrangement achieves efficiency and can be safeguard to authentic wireless correspondence applications. Finally, a presentation appraisal and assessment exhibits that their proposed framework is lightweight and adaptable to various sorts of attacks.

N. Badetia and M. Hussain,2017 [7] Radio sign are used to move information between at any rate two physical contraptions in wireless networks. These devices are overall called as "nodes" of the network. In wireless impromptu networks, nodes don't depend upon any per-existing system. In these correspondences depends upon the capacity of the nodes to make a multi-bounce radio network. Security is an important stress in every correspondence system.
Every center in the network must be confirmed for strong correspondence. There are various authentication part like quality based imprint, character based imprint, etc. A huge bit of these segments are either untrustworthy or complex. Makers have proposed a disseminated instrument for authentication of nodes in wireless sensor networks. Tokens are used for authentication of nodes. The sensor nodes are coherently organized as twofold tree with base station confining the root center point. A token is made by the parent center point for its child center. By then this token is used further by the adolescent nodes for common authentication of the sensor nodes. The proposed show is fundamental and secure. The security assessment by AVISPA instrument has shown it to be shielded and free from all potential security strikes.

III. PROPOSED WORK

The proposed work involves the generation of session key in the following manner.
Step 1 : Read Finger Print.
Step 2: Read Photo.
Step 3: Apply SHA 256 algorithm on Finger Print to get the pattern.
Step 4: Apply SHA 256 algorithm on Photo to get the pattern.
Step 5: Generate the Key using the extracts of the SHA of finger print and Photo

IV. IMPLEMENTATION

The implementation of the proposed work is done in the matlab and the database which is used for the storage of the data is MS ACESS.
The connection with the MSACESS is done using the DSN concept of the Microsoft Windows.

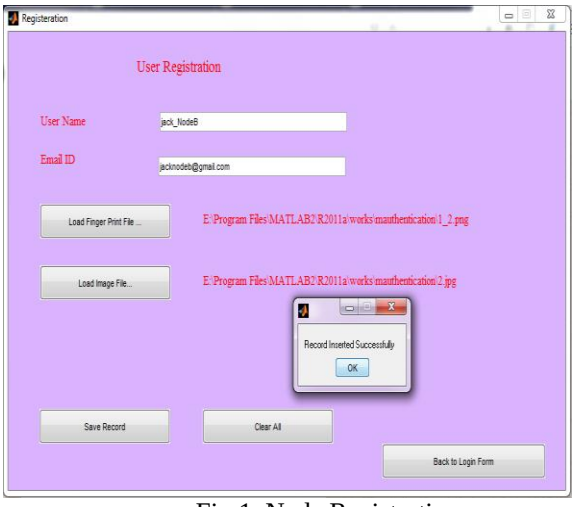

Fig 1. Node Registration

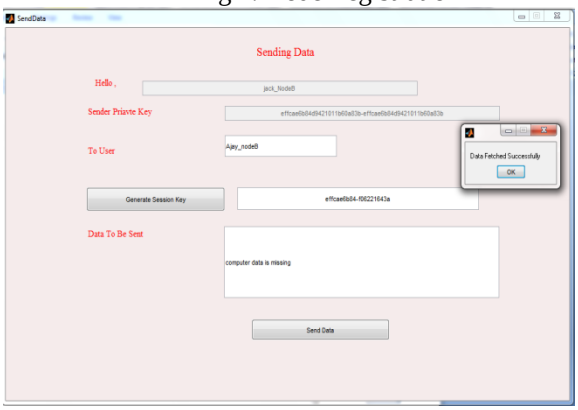

Fig 2. Data Transfer

The resultant OTP is tested using the various tools for checking the stability of OTP and result shown in table 1.

OTP	Website/Tool	Result
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Password Meter	Extremely Strong
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Password Checker	Good
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924	Cryptool2	Entropy 3.452 Strength 171 Extreme Strong

V. CONCLUSION

The current circumstance of the information move required being secure and no unapproved individual will prepared to get to the noteworthy information. The proposed work incorporates the plan to stack the unique finger impression/image of the customer , the dataset for the unique finger impression is taken for the unique mark reenactment of the enrolled customers. The customer when snap on the pile photo get , pop will appear to pick the territory where lives the record contrasting with the unique finger impression. By then the SHA 256 estimation will be incorporated for the age of the hash code which is related to

the unique finger impression and furthermore make the mystery expression in association with the hash of the unique finger impression and the photograph which are utilized to produce the private key utilizing the SHA 256 calculation and the idea of the private key of the sender and recipient for creating the session with the one of a kind exchange id, the made Session Key and Private Keys will further raise the level of security. The result assessment when stood out from the base work , by using the distinctive on the web and separated instruments of enrolling the mystery word quality , shows that the bit quality is about extended in abundance of numerous occasions the base work and moreover the entropy for the private key which is delivered is extended to the broad aggregate.

REFERENCES

[1] AneeshM.Koya ,Deepthi P. P.,"Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", Computer Networks ,Elsevier,2018
[2] U. Jain and M. Hussain, "Simple, secure and dynamic protocol for mutual authentication of nodes in wireless sensor networks," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2017, pp. 1-7.
[3] C. Jiang, H. Li, Y. Huang and W. Lin, "Mutual authentication architecture in wireless sensor networks," 2010 Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia), Shanghai, 2010, pp. 291-294.
[4] E. Yoon and K. Yoo, "Cryptanalysis of robust mutual authentication protocol for wireless sensor networks," IEEE 10th International Conference on Cognitive Informatics and Cognitive Computing (ICCI-CC'11), Banff, AB, 2011, pp. 392-396.
[5] Xin Liu, Yongjun Shen, Shuxian Li and Fenglan Chen, "A fingerprint-based user authentication protocol with one-time password for wireless sensor networks," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Nangang, 2013, pp. 9-12.
[6] H. H. Kim, N. Bruce, M. Sain, S. Park and H. Lee, "Simulation and evaluation of the authentication and session-key establishment protocol in wireless sensor networks," 2015 IEEE Conference on Wireless Sensors (ICWiSe), Melaka, 2015, pp. 7-11.
[7] N. Badetia and M. Hussain, "Distributed mechanism for authentication of nodes in wireless sensor networks," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 471-474.
[8] L. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," 2008 IEEE International Symposium on Wireless Communication Systems, Reykjavik, 2008, pp. 608-612.
[9] H. Huang and K. Liu, "A New Dynamic Access Control in Wireless Sensor Networks," 2008 IEEE Asia-Pacific Services Computing Conference, Yilan, 2008, pp. 901-906.
[10] R. Nanda, S. Tiwari and P. V. Krishna, "Secure and efficient key management scheme for wireless sensor networks," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 58-61.
[11] Debiao He, N. Kumar and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, 2013, pp. 1-6.
[12] Y. S. Lee, H. J. Lee and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on Physical UnclonableFunction (PUF)," 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, 2013, pp. 1314-1318.
[13] B. Bettoumi and R. Bouallegue, "Evaluation of Authentication Based Elliptic Curve Cryptography in Wireless Sensor Networks in IoTContext," 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, 2018, pp. 1-5.
[14] C. Wang and J. Feng, "A Study of Mutual Authentication for P2P Trust Management," *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, 2010, pp. 474-477.
[15] T. Ma, Y. Jiang, H. Wen, B. Wu, X. Guo and Z. Chen, "Physical Layer Assist Mutual Authentication scheme for smart meter system," *2014 IEEE Conference on Communications and Network Security*, San Francisco, CA, 2014, pp. 494-495.
[16] X. Zhou, Y. Xiong, F. Miao and M. Li, "A new dynamic user authentication scheme using smart cards for wireless sensor network," *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering*, Wuhan, 2011, pp. 1-4.

