A HYBRID SHA-256-BASED SECURITY FRAMEWORK FOR RELIABLE NODE AUTHENTICATION AND DATA INTEGRITY IN WIRELESS SENSOR NETWORKS

Shagun[1], Mukesh Kumar Saini[2]

M.Tech Scholar[1], Assistant Professor[2,]

[1,2,3]Department of Electronic & Communication Engineering, Sobhasaria Group of Institutions

Abstract:

Wireless Sensor Networks (WSNs) consist of numerous wireless nodes that are distributed across physical locations to monitor environmental conditions. These networks are increasingly integrated into various sectors, such as defence, banking, and education. In such environments, efficient and secure data sharing is critical. Two key challenges in WSNs are node authentication and data communication security. This paper proposes a solution that addresses both issues. Node authentication is achieved through the generation of authentication keys based on the combination of fingerprint-derived SHA-256 codes and random image-based SHA-256 codes. To secure data communication, the proposed approach utilizes secure authentication keys for both the sender and receiver, which are then used to generate a communication key. The strength of the communication key is validated using various online and offline tools. Comparative results with previous research demonstrate that the proposed method offers superior key strength and enhanced security for WSNs.

Keywords: Wireless Sensor Networks (WSNs), security challenges, lightweight cryptography, secure routing protocols, intrusion detection systems, blockchain security.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have gained significant attention in recent years due to their diverse applications across multiple domains such as military defence, healthcare, industrial monitoring, agriculture, and environmental management. A WSN typically consists of numerous wireless nodes that collect and transmit environmental data to a central system for analysis. These nodes are often deployed in remote or hostile environments, making them vulnerable to various security threats. As the reliance on WSNs grows, ensuring the security and integrity of data transmission becomes paramount [1].

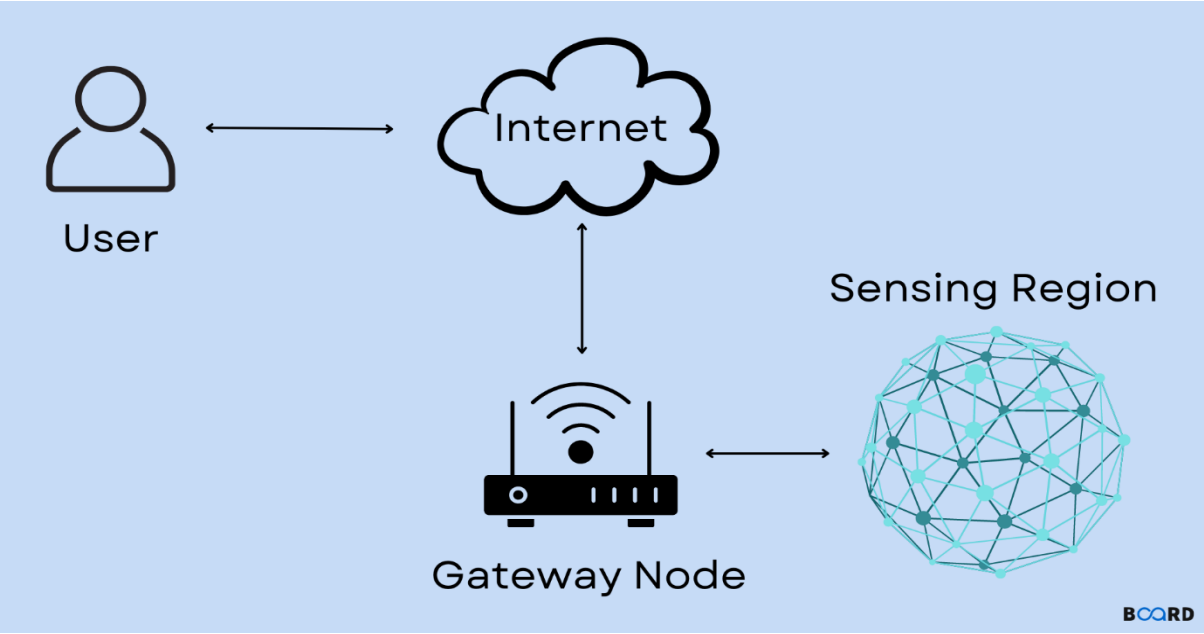

Figure 1. Wireless Sensor Networks

Two of the most critical challenges in WSNs are node authentication and secure data communication. Node authentication ensures that only legitimate nodes participate in the communication process, preventing unauthorized devices from infiltrating the network. Without effective authentication, the network becomes susceptible to attacks such as impersonation and unauthorized access. Additionally, securing data communication is essential to protect sensitive information from malicious interception, alteration, or eavesdropping during transmission [1].

Existing security protocols for WSNs often focus on one aspect, either node authentication or data security, but rarely address both issues simultaneously. This paper presents a comprehensive solution that combines secure node authentication with robust data communication security. The proposed method uses a novel approach for node authentication based on the generation of authentication keys derived from fingerprint-based and random image-based SHA-256 codes. These authentication keys are then utilized to form secure communication keys for data transmission [2].

The effectiveness of the proposed system is evaluated by comparing the strength of the generated communication keys with those from existing methods, using both online and offline security tools. The results show that the proposed method offers superior security, ensuring the integrity and confidentiality of both node authentication and data communication in WSNs [3].

2. LITERATURE REVIEW

R. Hu (2016) [4] highlighted that despite advancements in biometric technology, system-level issues in security systems, such as vulnerabilities in observation spaces and challenges in complex reconnaissance scenarios, need to be addressed. Issues like non-cross-over of sensors, reduced efficacy in poor lighting, and outdated traditional warning technologies remain obstacles to improving government-sponsored retirement programs' performance.

X. Wang et al. (2018) [5] discussed how large enterprises and public organizations use Managed Security Services (MSSs) to monitor and analyze cybersecurity data. They emphasized the importance of secure and controlled data sharing among MSS clients, despite privacy concerns. Their proposed solution focuses on enabling confidential, flexible, and cooperative data sharing while maintaining existing privileges and tasks.

T.T. Teoh et al. (2017) [6] utilized Hidden Markov Models (HMMs) for predicting cybersecurity attacks, highlighting the effectiveness of HMM's probabilistic nature in modeling complex security events and reducing false alarms in network security logs.

M. Elsayed and M. Zulkernine (2018) [7] addressed security risks in cloud-based scientific applications, which handle large datasets. Malicious, weak, or misconfigured applications were identified as top threats in big data security.

M. Kantarcioglu and F. Shaon (2019) [8] proposed the SECUREDL framework to ensure the protection of sensitive unstructured data, processed by AI and machine learning models. The framework includes features like access control, audit logs, data masking, and intrusion detection.

L. Ming et al. (2018) [9] presented a security model for Intelligent Transportation Systems (ITS), incorporating network security and transportation data elements. They tested the model using simulations with malicious nodes, showing significant performance impacts, including higher costs and longer travel times.

A.R. de la Concepcion et al. (2014) [10] developed a versatile solution for wireless sensor networks, ideal for transmitting large data over bandwidth-limited channels, with applications in sustainable agriculture.

F.Z. Glory et al. (2019) [11] introduced a user authentication algorithm that generates passwords based on dynamic inputs, such as favorite book titles or secret dates.

Shah Zaman Nizamani et al. (2017) [12] proposed a text-based client authentication scheme, enhancing security by altering the password input method and preventing online security attacks like shoulder surfing and keylogging.

3. PROPOSED WORK

Algorithm 1 WSN Security Model Algorithm

Node Authentication - Registration Process
Read UserName for Node and Email ID of User Handling Node.
Get the Fingerprint Image for the User Node Identification.
Get the Random Photo from User for Image Validation.
Process Fingerprint Image using SHA-256 and store in FigImgSHA.
Process Photo using SHA-256 and store in PhotoFileSHA.
Store the details in the database.
End of Registration
Node Authentication - Login Process
Read UserName for Node.
Get the Fingerprint Image for the User Node Identification.
Get the Random Photo from User for Image Validation.
Process Fingerprint Image using SHA-256 and store in FigImgSHA.
Process Photo using SHA-256 and store in PhotoFileSHA.
Fetch the Details on basis of UserName.
if Details Verified **then**
    Access Granted
else
    Access Denied
end if
End of Login
Data Communication: Sender End
Access the Authentication Key of Sender and store in SHASender.
Select the Receiver from the list of valid nodes.
Access the Authentication Key of Receiver and store in SHAReceiver.
Extract fixed characters from SHASender (1:35) and SHAReceiver (1:35) and store in KEYDataCom.
Generate Communication Unique AutoGenerate ID.
Read Message for Communication.
Store all details in the database.
End of Sender Process
Data Communication: Receiver End
Get the Communication ID, and KEYDataCom (Communication Key).
Fetch Details from the Database.
if Details Corresponds to Receiver **then**
    Message Accessed
else
    Stop
end if
End of Receiver Process

.

4. IMPLEMENTATION AND RESULT ANALYSIS

The hardware infrastructure for the Wireless Sensor Network (WSN) security model consists of various components designed to support both the sensor node operations and secure communication within the network. Each wireless sensor node typically includes a microcontroller, such as an ARM-based processor, that controls the node's functionality. The sensor nodes are equipped with environmental sensors to collect data (e.g., temperature, humidity, motion) and communication modules like ZigBee, Wi-Fi, or Bluetooth for wireless communication. A power supply, such as a battery or energy harvesting system, powers the sensor nodes. Additionally, biometric devices such as fingerprint scanners and cameras are used to capture user identification details, which play a key role in the authentication process. A centralized or distributed database infrastructure is employed to store node registration details, authentication credentials, and secure communication keys, while user interface devices (e.g., computers or smartphones) facilitate the management and monitoring of the WSN.

On the software side, the WSN security model is designed to handle critical tasks such as node authentication, secure data communication, and data management. The node authentication process involves capturing fingerprint images and random photos from the user, followed by processing these images using the SHA-256 hashing algorithm. This ensures the secure storage and validation of node identities. Secure communication is achieved through the generation of unique communication keys derived from the authentication keys of both the sender and the receiver. These keys are used to encrypt transmitted data, ensuring confidentiality and integrity. The software also includes a database management system (DBMS), either relational or NoSQL, which stores

authentication data and communication keys, facilitating secure login and message validation processes. Security mechanisms, such as SHA-256 hashing, are integral to maintaining the system's integrity, ensuring that both the authentication and communication processes remain secure. Furthermore, a user interface is provided for administrators to manage nodes, initiate communication, and monitor the security status of the network. Simulation and evaluation tools are also employed to assess the strength of communication keys and evaluate the overall security of the system, testing its resilience against potential attacks.

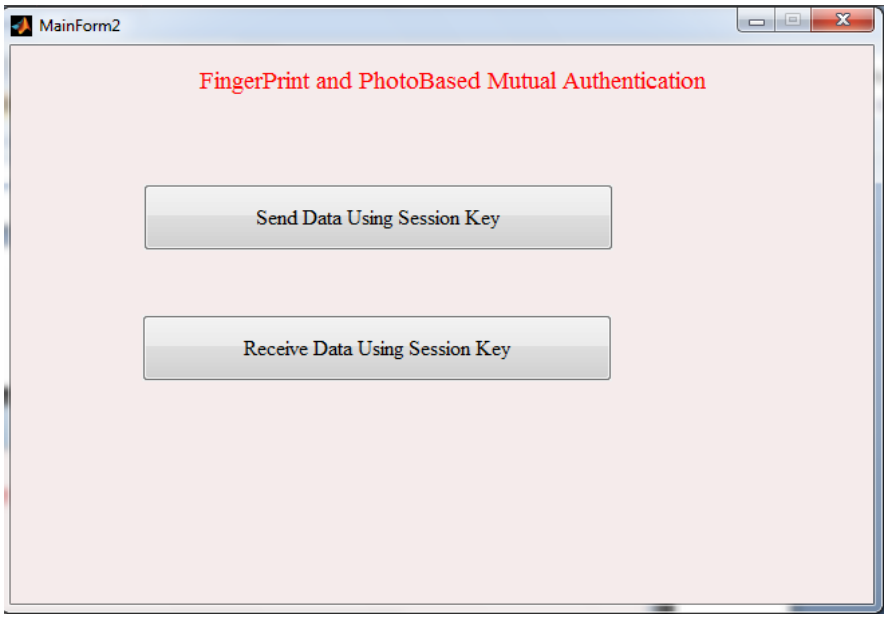

Figure 2. Implementation in Matlab

4.1 Results Analysis

One of the base papers for comparison, **F. Z. Glory et al., 2019, formed the pattern on the basis of the concept then proposed on their paper, the sample pattern according to their concept is taken as,**

"Base Paper Password Pattern

{urAn29iRfan-

Proposed Password Pattern"

f06221643a3a3b9070243d924-f06221643a3a3b9070243d924

Table 1. Result Analysis

Website/Tool	Base Result	Proposed Result
Password Monster Tool	0.000005 trillion years	4 billion trillion trillion trillion years
Delinea.com Password Checker Tool	186 million years	4.0E+63 million years
How Secure is My Password Checker Tool	46 million years	9.0E+62 millions years

5. CONCLUSION

In conclusion, the proposed WSN security model offers a comprehensive solution to address the critical challenges of node authentication and secure data communication within Wireless Sensor Networks. By incorporating advanced cryptographic techniques such as SHA-256 hashing for both fingerprint and image-based authentication, the model ensures that only legitimate nodes are allowed to participate in the network. Additionally, the use of secure communication keys for data transmission guarantees the confidentiality and integrity of the information exchanged between nodes. The integration of a centralized database for storing authentication data and communication keys further enhances the security of the network. The results obtained through the validation of the communication keys indicate that the proposed approach provides a higher level of security compared to existing methods. This model can be effectively applied to a wide range of applications, including defense, healthcare, and industrial monitoring, where secure and efficient data sharing is essential. Future work could explore the scalability of the system, its performance in large-scale networks, and the integration of additional security features to further strengthen the overall framework.

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. Fei Gao, 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. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. J. S. Ho, "Wireless Body Sensor Networks with Metamaterial Textiles," *2019 8th Asia-Pacific Conference on Antennas and Propagation (APCAP)*, 2019, pp. 89-89.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.

19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. Shah Zaman Nizamani, Syed Raheel Hassan, Tariq Jamil Khanzada 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.
26. R. Menaka, R. Dhanagopal and N. Archana, "An Efficient Approach for Secured Data Aggregation Against Security Attacks in WSN," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2020, pp. 239-245.
27. Y. Al-Aali and S. Boussakta, "Lightweight block ciphers for resource-constrained devices," *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 2020, pp. 1-6
28. A. J. Chinchawade and O. S. Lamba, "Authentication Schemes and Security Issues in Internet Of Everything (IOE) Systems," *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2020, pp. 342-345.
29. X. Liu and Z. Guo, "An Authentication Scheme with Computable Password for Wireless Sensor Networks," *2020 International Conference on Computer Communication and Network Security (CCNS)*, 2020, pp. 184-190
30. W. Tiberti, A. Carmenini, L. Pomante and D. Cassioli, "A Lightweight Blockchain-based Technique for Anti-Tampering in Wireless Sensor Networks," *2020 23rd Euromicro Conference on Digital System Design (DSD)*, 2020, pp. 577-582.
31. 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.
32. M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2017, pp. 171-174.