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

Dual Authentication of Node based on MAC Address and Biometric in WSN

Raja Manu[1], Ramesh Kumar[2]

[1] M.Tech Scholar, [2]Assistant Professor (HOD)

[1,2] Department of Computer Science and Engineering, K.K. University Nalanda (Bihar)

Abstract: Security is a major concern when transferring data over the internet because there are many risks, such as data breach, unauthorized access. The protocol presented in this article can help combat the communication hassle that often occurs with data. Each message is susceptible to a multitude of types of attacks, so it's necessary to verify that all data is transferred safely and securely to its destination. This is a protocol based on mutual authentication. The list of nodes permitted to access data is maintained by one node, while a monitoring node can monitor it. In communicating nodes, we've used the MAC address for an identifier and the finger print for identification- as we are assuming that the user will be operating on this node. The Monitoring Node allows to monitor the nodes in a network by checking their MAC address, fingerprint and digital certificate. The node can verify a connection despite changes of the session token. Data from every interaction with us is verified using a one-time password and cross verification of data. Together we generate new passwords every time, so that only the receiver can access their information.

Index Terms **– WSN , Node Authentication ,Data Security.**

I. INTRODUCTION

Wireless Sensor Networks (WSN) use a system of sensors to detect physical phenomena. Privacy is key factor with WSN, so its important to secure any data being collected and stored. One of the main challenges in WSNs is providing high-security requirements with constrained resources. Many parameters for high-security include node authentication, data confidentiality, anti-compromise, and resilience against traffic analysis. [1]

Data confidentiality in WSN is preventing access to unauthorized people obtaining data. Sensors should not relay on the data they take from the environment to their neighbors. When it comes to sensitive applications, like military, data collected on nodes can be very sensitive and may contain classified information. Furthermore, nodes in a wireless network have to transmit sensitive data using encryption in order to stay secure from malicious hackers. These networks are assured with low-energy encryption algorithms that safely transmit data and reduce bandwidth. [1]

Additionally, routing data must also be kept secret to prevent malicious nodes from exploiting it which can reduce the performance of the network. One way to maintain data confidentiality is with encryption using a secret key. [2] Low power algorithms that rely on secret keys are good for WSNs because they use less energy. If a malicious node is able to access the data, they will be able to alter it. Data integrity ensures that no one can alter the message that is being communicated during transmission. Though this protects data, it cannot prevent its misuse by unauthorized persons. [2]

Data security protects the data from getting taken by malicious nodes and altered by unauthorized persons; however, it cannot stop the data from being altered by either a malignant node or by transmission. [3] To ensure integrity of the messages, use an authentication code or a cyclic code to prevent alterations in the data through both these mechanisms. Data is only confidential if malicious nodes cannot gain access to the data. [4] Data integrity ensures that the message will not be altered during transmission, even if a malignant node disrupts the message or data is disrupted during transmission. For maximum security, MAC codes should be used to authenticate messages and verify data integrity. [4]

A vital feature of WSNs is a means to trade data without errors and tampering. One such technique is key-based authentication, used by most wireless communication systems. Authentication mechanisms allow nodes to verify other nodes' identity. If there is no authentication, a malicious node can masquerade as a different node and eavesdrop on data or disrupt the operation of other nodes. To trust two communicating nodes, one key can be used for both sender and receiver to verify messages. [5]

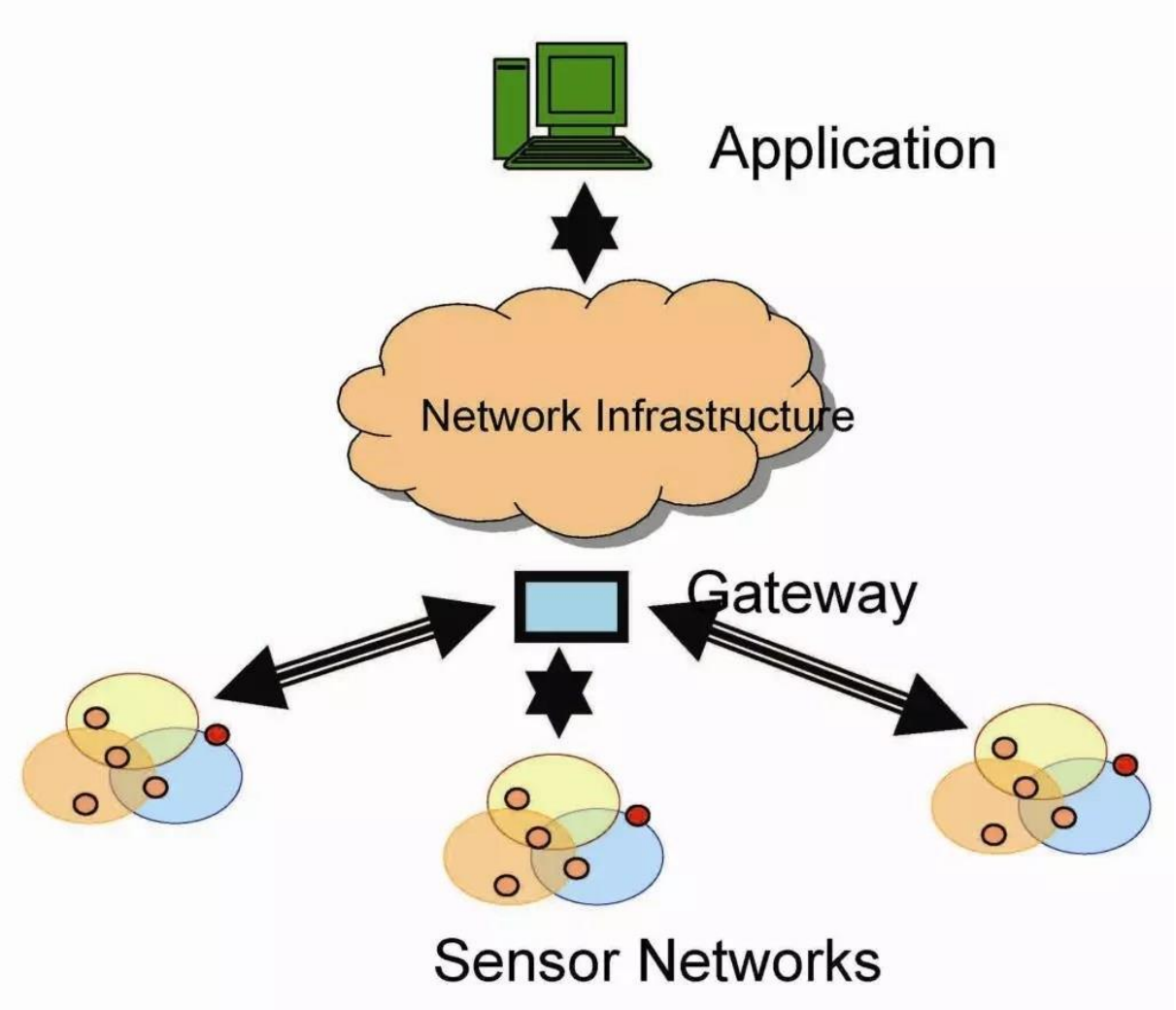

Fig 1. WSN Networks

Sensor networks are made up of sensors that cooperate with one another to monitor scenarios in a variety of settings. Intelligent systems can be integrated with devices and sensors in order to increase security. With sensors and actuators, the environment can be made more comfortable and safer. Accuracy and robustness problems are resolved by the sensor fusion, but reducing cost and consumption is a way to further resolve this issue. Some people have suggested using active devices on the human instead of using sensor, in order to detect and track human activities.[6]

II. LITERATURE REVIEW

Sachin Malhotra,Munesh C. Trivedi ,2017 [7] Cybersecurity is a major concern of the government and people around the world. The number of incidents reported is rising and people are always looking for ways to make their information more secure. To do this, an authentication instrument has been proposed that makes sure that alterations in data and pantomime techniques cannot compromise or disrupt operations.

Y. K. Alapati and S. Ravichandran, 2019 [26]The proposed strategy of secure mobile ad hoc networks, recognizes and tracks courses among trusted hubs and updates them regularly due to a dynamic topology. The results show that the proposed strategy takes a better course guiding approach when contrasted to existing techniques.

R. Seetharaman et. al 2019 [27] This enact improves security of Ad Hoc On Demand Distance Vector protocols for peer-to-peer networks by utilizing encryption and decrypting measures. The proposed framework utilizes proactive and responsive measures for information transmission.

Z. Cui et al.,2020 [28] Technology is continuously evolving, and security is a main topic of concern. Blockchain technology with decentralization features provides better security than other alternatives. A blockchain authentication scheme for IoT in proposed that not only has the same level of security as trusted third parties, but also eliminates single points of fails. Node identity authentication relies on trusted "third parties" which are prone to single point failures in many different environments. The node's capability determines what type it is; base station, cluster head or ordinary node. In IoT nodes are arranged hierarchically according to each node's capacity rather than location like in the traditional network structure. With this infrastructure, there can be hybrid blockchain models and node identity authentication. The analysis proves with its performance and security, it is a better alternative than other options.

III. PROPOSED CONCEPT

3.1 Entry of New Node

- Read the user's MAC Address and Fingerprint to verify identity
- Next, create a fingerprint. Generate the hash code for the fingerprint using SHA-256 and store it in FPSHA.
- To create a hash code, use the SHA-256 algorithm to encode the MAC address and store it in MASHA.
- The next step of your workflow is saving the digital signature, by using 10 characters from SHAFIG and extracting 10 characters from MASHA
- Verify in database, if not present then save the details of the new node.

3.2 Data Communication Concept

- Generation of 10 random numbers which will range from 0-9 and store DIG10RND
- Take the first 20 characters of the SHA-256 hash and store them in the USR1SHA string variable.
- To generate the hash code for authentication, use SHA-256 on the destination MAC address and then string the first 20 characters together to create USR2SHA.
- To for SKEY combine all DIG10RND, USR1SHA, USR2SHA

IV. IMPLEMENTATION AND RESULT ANALYSIS

The implementation of the concept is done using the database Microsoft Access and MATLAB.

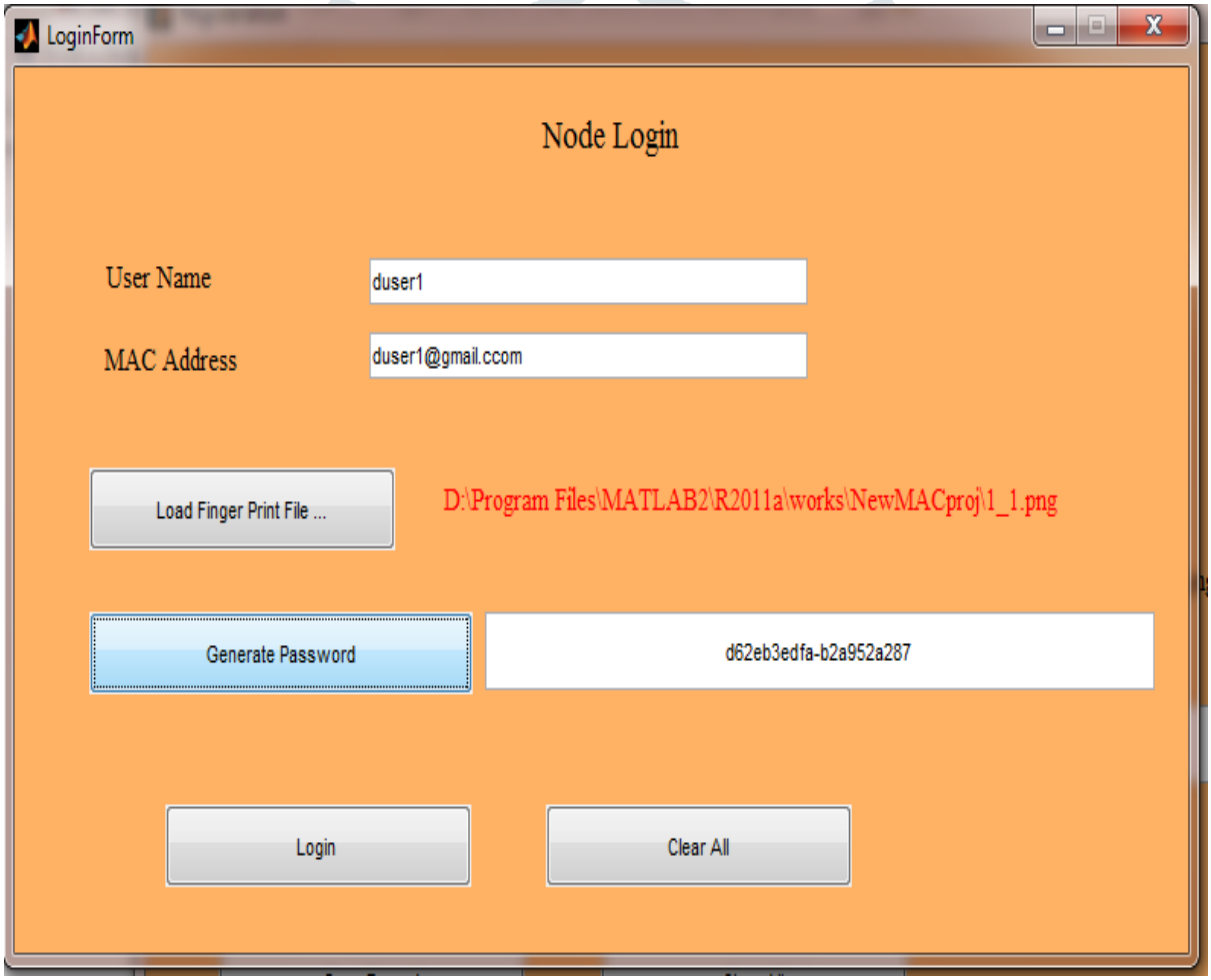

Fig 2. Login Process

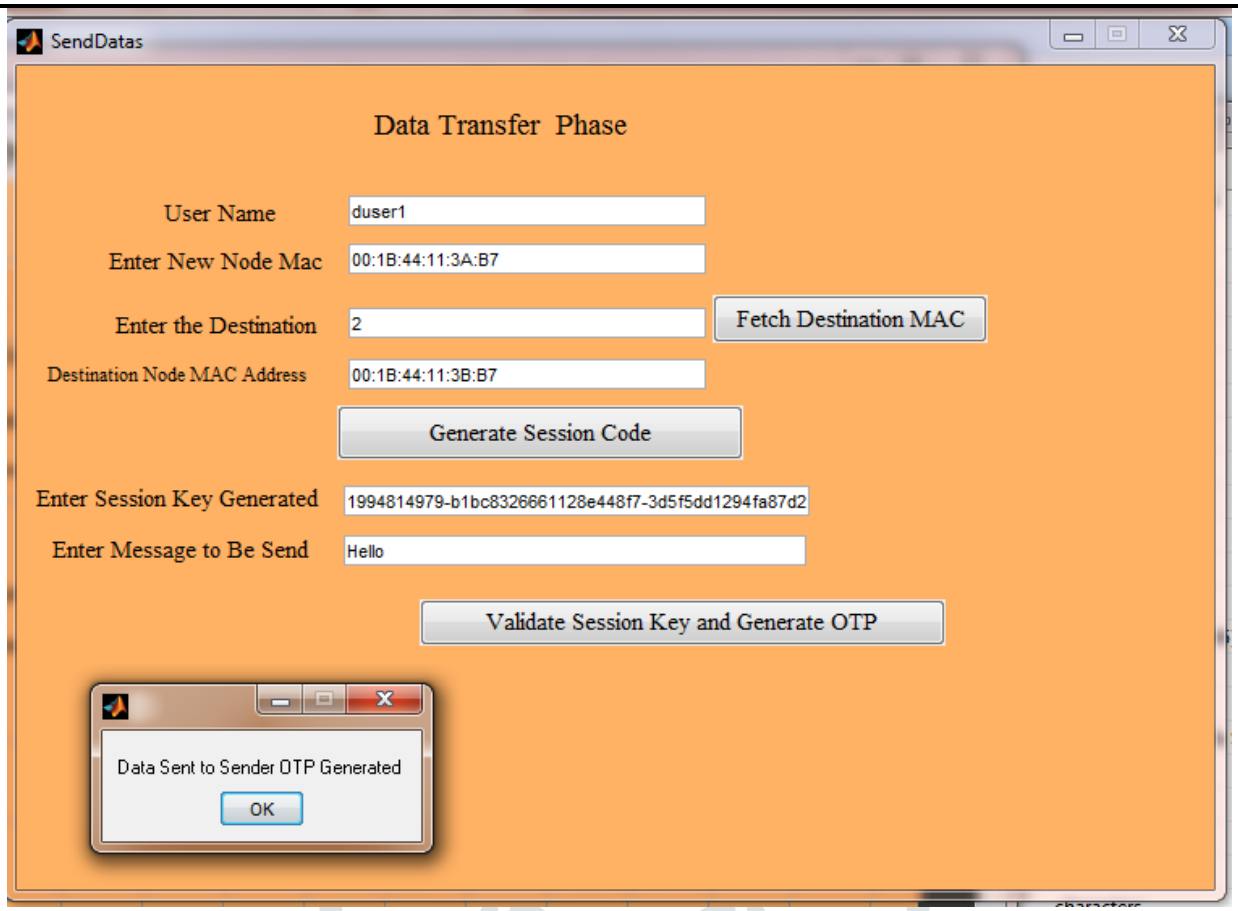

Fig 3. Communication Process

Result Analysis using tools

Base: 4112-df53ca268240ca76670-924645b3e345a600bfa1

Proposed: 1994814979-b1bc8326661128e448f7-3d5f5dd1294fa87d200a

Table 4.5 Result from Test Tool-1(Rumkin)

	Base Key Score	Proposed Key Score
Entropy	146 bits	161 bits
Length	45	52

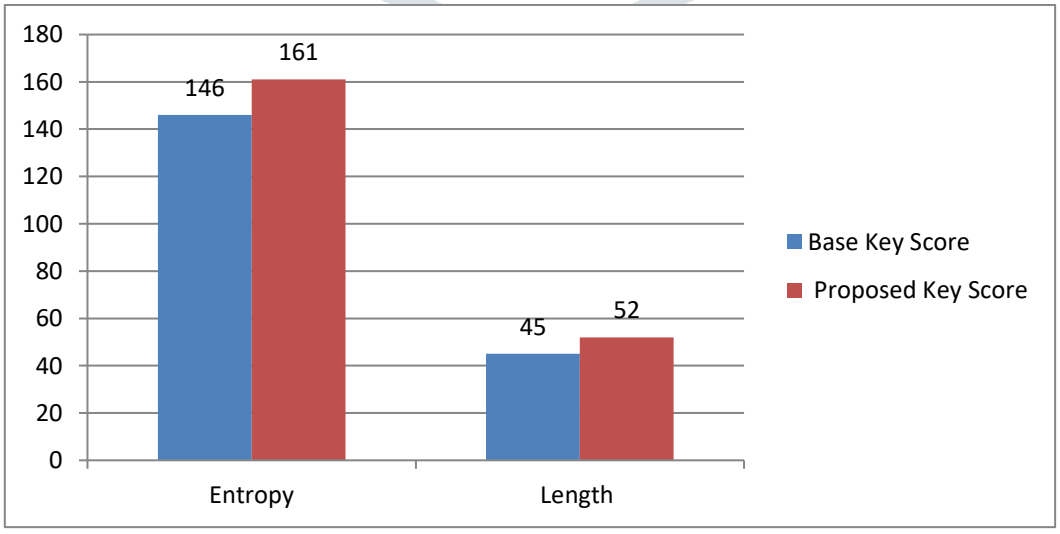

Fig 4 Graph for Test-1

Table 2. Result from Test-2

	Base Key Score	Proposed Key Score
Entropy	181.3 bits	209 bits

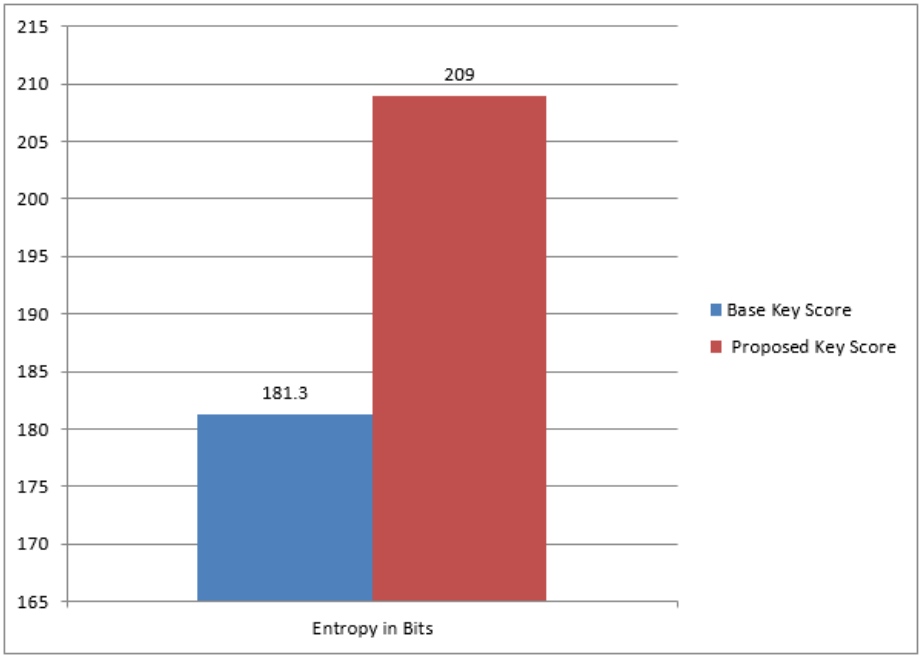

Fig 5 Graph for Test-2

V. CONCLUSION

The list of nodes permitted to access data is maintained by one node, while a monitoring node can monitor it. In communicating nodes, we've used the MAC address for an identifier and the finger print for identification- as we are assuming that the user will be operating on this node. The Monitoring Node allows to monitor the nodes in a network by checking their MAC address, fingerprint and digital certificate. The node can verify a connection despite changes of the session token. Data from every interaction with us is verified using a one-time password and cross verification of data. Together we generate new passwords every time, so that only the receiver can access their information.

REFERENCES

1. K. Gomathi and B. Parvathavarthini, "An efficient cluster based key management scheme for MANET with authentication," *Trendz in Information Sciences & Computing(TISC2010)*, Chennai, 2010, pp. 202-205.
2. L. Licai, Y. Lihua, G. Yunchuan and F. Bingxing, "Bargaining-Based Dynamic Decision for Cooperative Authentication in MANETs," *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, 2014, pp. 212-220.
3. P. Yadav and M. Hussain, "A secure AODV routing protocol with node authentication," *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, 2017, pp. 489-493.
4. H. Yang and S. Yoo, "Authentication Techniques for Improving the Reliability of the Nodes in the MANET," *2014 International Conference on IT Convergence and Security (ICITCS)*, Beijing, 2014, pp. 1-3.
5. Y. P. Singare and M. Tembhurkar, "Design of an efficient initial access authentication over MANET," *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, Pune, 2015, pp. 1614-1619.
6. U. Amin and M. A. Shah, "A Novel Authentication and Security Protocol for Wireless Adhoc Networks," *2018 24th International Conference on Automation and Computing (ICAC)*, Newcastle upon Tyne, United Kingdom, 2018, pp. 1-5.
7. Sachin Malhotra,Munesh C. Trivedi,"Symmetric Key Based Authentication Mechanism for Secure Communication in MANETs",Intelligent Communication and Computational Technologies pp 171-180,2017.
8. Y. K. Alapati and S. Ravichandran, "Efficient Route Identification Method for Secure Packets Transfer in MANET," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019.
9. R. Seetharaman, L. H. Subramaniam and S. Ramanathan, "Mobile Ad Hoc Network for Security Enhancement," 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 2019.
10. Z. Cui et al., "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241-251, 1 March-April 2020