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

Innovative Authentication and Identity Validation Communication of WSN

Amita Pareek[1], Mr. Nitin Halkara[2]

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

[1,2] Department of Electronics (Digital Communication), Shekhawati Institute of Engineering and Technology, Sikar, Rajasthan

Abstract : A Wireless Sensor Network is composed of several wireless nodes that are dispersed and dedicated sensors that are physically positioned for monitoring the surrounding environment. Nowadays, wireless sensor networks are becoming part of almost every organization, whether it is the defense sector, banking, education, or other industries. In such an environment, we require data to be shared effectively and securely. The two main issues that need to be highlighted in Wireless Sensor Networks are the authentication of the nodes, i.e., the nodes that participate in the communication process need to verify their identities. Data communications security is the second issue to address. With the proposed concept, node authentication is performed by generating an authentication key based on the fingerprint SHA-256 code and the random image SHA-256 code of the node. As part of securing the data communication process, the secure authentication keys of the sender and receiver are used to create the communication key in conjunction with the concept of securing the data communication process. When compared with the previous research, the proposed concept has greater strength when validated using a variety of online and offline tools**.**

IndexTerms **– WSN ,Secure Communication, WSN Authentication.**

I. INTRODUCTION

The wireless sensor network (WSN) measures environmental conditions such as temperature, sound, pollution levels, humidity, and wind by using spatially dispersed and dedicated sensors. A WSN can monitor air quality in a nearby city or industrial level at a power plant.

Wireless sensor networks are used to monitor physical or environmental conditions, such as temperature and pressure. Modern WSNs are bi-directional, meaning they can collect data or enable control of sensors. The development of these networks was motivated by military applications such as battlefield surveillance. They've since become popular in the industrial and consumer sectors for applications like monitoring industrial processes and machine health. [1]

Each node in a Wireless Sensor Network is equipped with a radio transceiver and a microcontroller, as well as sensors to detect changes in its environment, power sources, and other factors. Although microscopic dimensions have not yet been realized, sensor nodes can range in size from a shoebox to (theoretically) the size of a grain. [2]

Sensor nodes can cost anything from a few dollars to more than a hundred dollars, depending on how complex they are. There are only so many things that the sensor node can have in order to be limited in size - energy, memory, computational speed, and communication bandwidth. There are a variety of topologies for wireless networks, from simple star networks to advanced multi-hop wireless mesh networks [2].

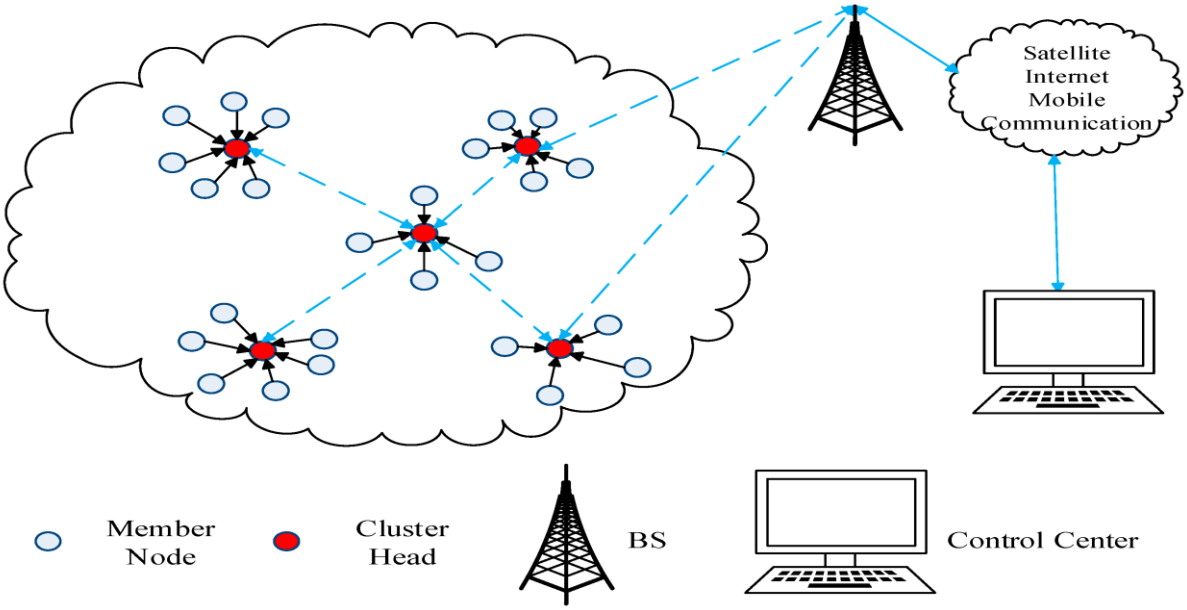

Fig 1. Wireless Sensor Network

II. LITERATURE SURVEY

F. Z. Glory et. al. 2019 [3] proposed that a password be generated by a random combination of words and numbers as a method of authentication. A password is generated based on dynamic inputs such as the novel's favorite name, the number of grandmother's children, secret dates, etc.

Shah Zaman Nizamani et.al 2017 [4] A text-based client confirmation conspire is proposed, which alters the secret phrase input strategy and adds a secret key change layer to the security of printed secret phrase plots. By using irregular decimal numbers to address alphanumeric secret key characters, the conspire opposes online security attacks, such as shoulder surfing and key lumberjacks.

R. Menaka, et. al ,2020 [5] Current systems employ a variety of security measures, such as training data, to protect against attacks. However, these measures are insufficient because they are vulnerable to compromises. One way to overcome this problem is by using iterative isolating computation in conjunction with weighted information aggregation. This makes the system more robust and less likely to take on too much damage in an attack.

Y. Al-Aali and S. Boussakta, 2020 [5] Lightweight cryptography: another part of cryptography focused on giving security to gadgets like wireless sensor networks (WSN), Radio-Frequency Identification (RFIDs), and other inserted frameworks. The elements considered in lightweight cryptography are circuit region, memory necessities, handling time, idleness, power, and energy utilization. This paper presents a conversation on common lightweight square codes for various performance levels, strength, pattern schemes, constraints, and applications including the NIST cycle 1 and 2 applicants.

A. J. Chinchawade and O. S. Lamba, 2020 [6] Internet of Everything (IOE) could be replacing Internet of Things in the coming years. IOE includes a multitude of devices and sensors that are IoT related, individuals, communications between machines and devices through the Internet. While they share an Internet connection, they can have several purposes such as IoT sensors in buildings, medical care properties and even homes. Programmers use IOE to send large scale attacks with alarming consequences that may be difficult to stop without the proper security measures. This paper focuses on some of the security threats and authentication mechanisms in the IOE frameworks.

M. H. Zaki et al 2017 [7] proposed a text-based secret phrase validation plot, but it is powerless against many forms of attacks. These include shoulder surfing, power animal attacks, and other related types of assaults, such as word reference attacks. Many practical based secret phrase confirmation plans exist, yet they are also costly in time and overall engagement for a business. In this paper, a safe example key based secret phrase validation plan that provides greater security using multiple example keys is proposed. This consists of client demands to input an enrollment number from the lattice into the design, register key qualities and guide values to the secret key and imitate qualities to the final secret word to spoof attackers. From that point onward, the client enters their graphical secret words in this design with already provided key qualities and adds fake digits to their final grouped word; this facilitates shoulder surfing protection because of high intricacy involved in deducing the key over 3 different levels: first from design then from key and finally from sham qualities. This mix creates a powerful procedure that does not burden human memory and enhances protection for those who do not have very little idea about passwords / passphrases in general - thereby providing them with increased safety from malicious aggressors.

III. PROPOSED WORK

The WSN Security model which we have proposed works in the two main segments, first the concept works for the authentication of the nodes and second it works for the validation of the communication process. On the basis of the concept which is taken, we have divided the whole process into four algorithms.

3.1 Node Authentication -Registration Process

In this section we will discuss about the node registration in WSN so that the valid nodes can be authenticated, for the registration process we have to follow the following steps:

Step 1: Read UserName for Node and Email ID of User Handling Node.

Step 2: Get the Fingerprint Image for the User Node Identification.

Step 3: Get the Random Photo from User for Image Validation.

Step 4: Process Fingerprint Image using SHA-256 and store in FigImgSHA.

Step 5: Process Photo using SHA-256 and store in PhotoFileSHA.

Step 6: Store the details in the database.

Step 7: Stop

3.2 Node Authentication -Login Process

In this section we will discuss about the node login in WSN so that the validation of the incoming node can be performed, for this we have to follow the following steps:

Step 1: Read UserName for Node.

Step 2: Get the Fingerprint Image for the User Node Identification.

Step 3: Get the Random Photo from User for Image Validation.

Step 4: Process Fingerprint Image using SHA-256 and store in FigImgSHA.

Step 5: Process Photo using SHA-256 and store in PhotoFileSHA.

Step 6: Fetch the Details on basis of UserName.

Step 7: If Details Verified then Access Granted Else Access Denied.

Step 8: Stop

3.3 Data Communication: Sender End

Now, in the case of communication data from sender node to the receiver node. The sender will initiate the communication process by following the steps given below:

Step 1: Access the Authentication Key of Sender and store in SHASender.

Step 2: Select the Receiver from the list of valid nodes.

Step 3: Access the Authentication Key of Sender and store in SHAReceiver.

Step 4: Extract fixed characters from SHASender (1:35) and SHAReceiver (1:35) and store in KEYDataCom.

Step 5: Generate Communication Unique AutoGenerate ID.

Step 6: Read Message for Communication

Step 7: Store all details in the database.

Step 8: Stop.

3.4 Data Communication: Receiver End

Now, when at the receiver end, to access the data following the steps given below:

Step 1: Get the Communication ID, and KEYDataCom (Communication Key)

Step 2: Fetch Details from the Database.

Step 3: If Details Corresponds to Receiver, then Message Accessed Else Stop.

Step 4: Stop.

IV. Result Analysis and Implementation

The implementation is performed in Matlab and database is MS Access

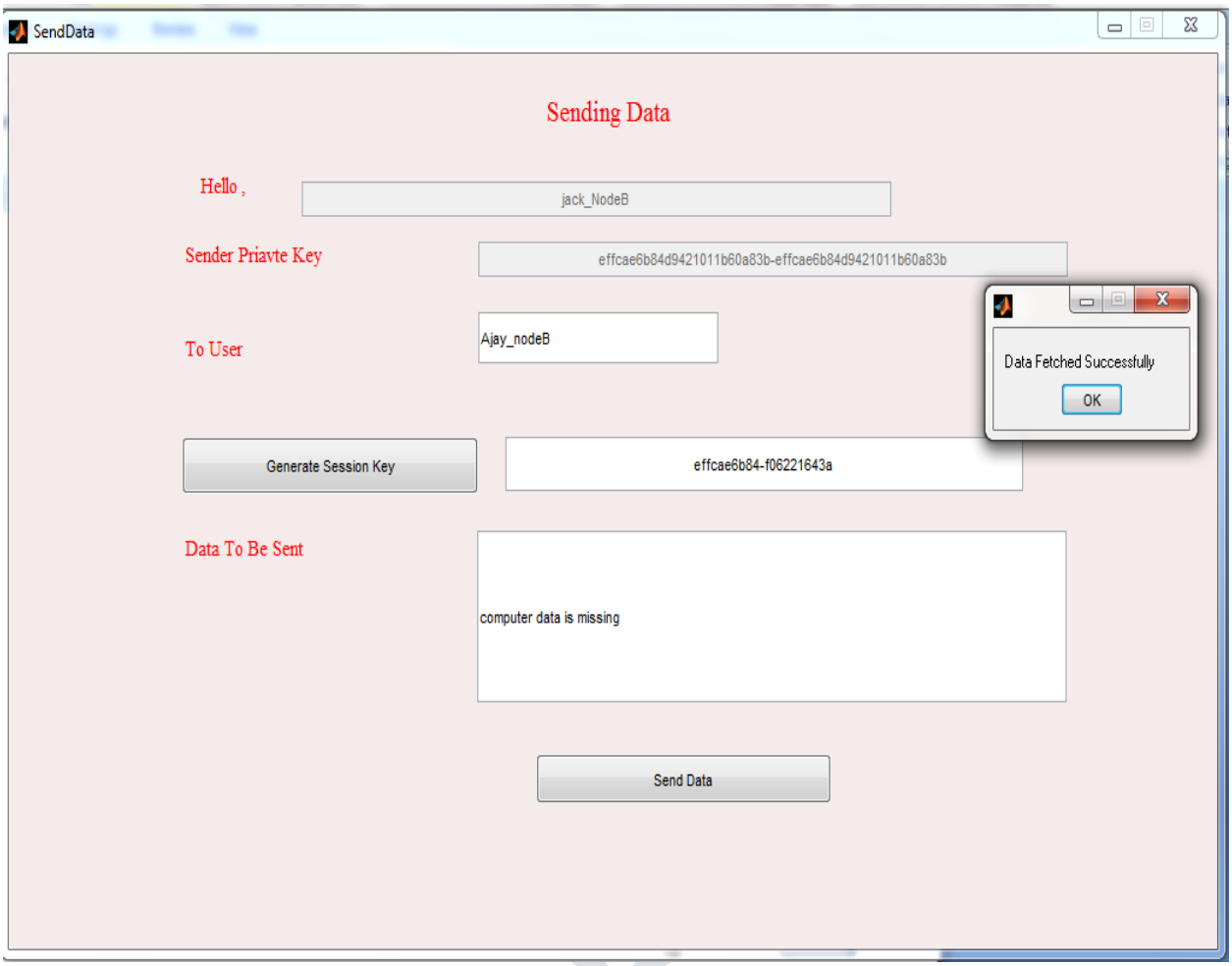

Fig 2. Implementation Form

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 on Basis of Time Period Comparison with Paper 1

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 million years

Table 2: Result Analysis on Basis of Entropy Comparison with Paper 1

Website/Tool	Base Result	Proposed Result
Cryptool2 Tool	83 bits	116 bits
Password. Blue Tool	43 bits	154 bits

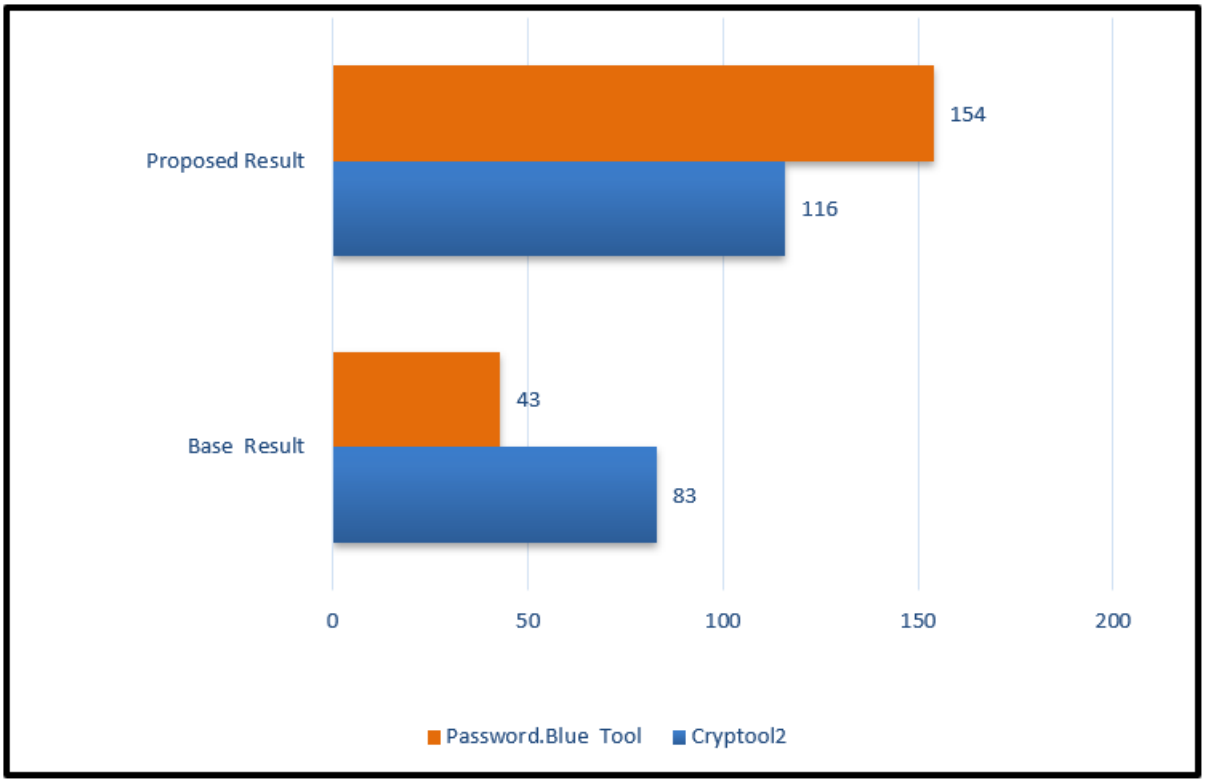

Fig 3. Result Analysis Paper 1

Another base paper, **Shah Zaman Nizamani, et al. 2017 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
g m x F G P X)>

Proposed Password Pattern
f06221643a3a3b9070243d924-f06221643a3a3b9070243d924

Table 3: Result Analysis on Basis of Time Period Comparison with Paper 2

Website/Tool	Base Result	Proposed Result
Password Monster Tool	1 billion trillion years	4 billion trillion trillion trillion years
Delinea.comPassword Checker Tool	2000000000 million	4.0E+63 million years
How Secure is My Password Checker Tool	6 hundred trillion years	9.0E+62 million years

Table 4: Result Analysis on Basis of Entropy Comparison with Paper 2

Website/Tool	Base Result	Proposed Result
Cryptool 2	76 bits	116 bits
Password. Blue Tool	56 bits	154 bits

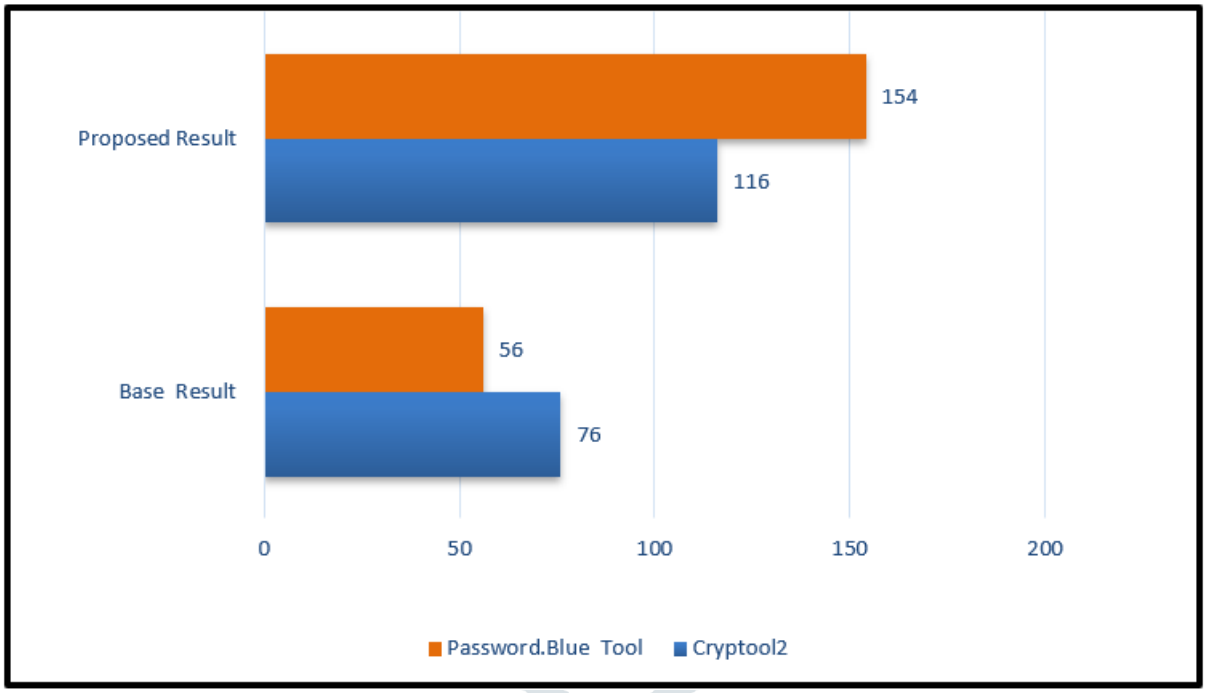

Fig 4. Result Analysis Paper 2

V. CONCLUSION

The proposed concept allows node authentication to take place. The verification process includes the generation of the key by using a fingerprint that has been determined with SHA-256 and an image hash which has been obtained with SHA-256 as well. This is combined with securing the data communication process, in order for two nodes to communicate, validating the keys either online or offline are done to ensure there isn't any tampering performance. It is shown through various methods of validating that when compared against prior research, this proposed method has greater strength to it.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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

7. 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.
8. 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.
9. 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
10. 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.
11. 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.