ZKG INTERNATIONAL ISSN: 2366-1313

INTEGRITY VERIFICATION AND DATA SECURITY IN WIRELESS SENSOR NETWORK

[1]Mr. T. Layaraja,[2]Punna Aishwarya,[3]P.Sampath,[4]V.Suraksha

[1]Assistant Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

Layaraaja@gmail.com

[2, 3, 4, BTech] Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

aishwaryapunna2002@gmail.com,psk630200@gmail.com,velpulasuraksha01102002@gmail.com

ABSTRACT:

In recent years, wireless sensor networks (WSNs) have become a useful tool for environmental monitoring and information collection due to their strong sensory ability. Whereas WSNs utilize wireless communication and is usually deployed in an outdoors environment, which make them vulnerable to be attacked and then lead to the privacy disclosure of the monitored environment. SUM, as one common query among the queries of WSNs, is important to acquire a high-level understanding of the monitored environment and establish the basis for other advanced queries. In addition, now-days WSNs are using everywhere such as road traffic monitoring, CCTV home monitoring and many more. They are small and tiny devices which sense the data from its environment and report to the centralized server for remote monitoring using Internet of Things (IoT) network connections. But sometimes malicious attackers can intrude or intercept network connection to alter messages and these altered messages will report to centralized server which many take wrong decision based on received data. To tackle such problem, this project implementing the data integrity verification using chaotic technique and data security using holomorphic encryption. In proposed technique, the system will send a verification hash code along with encrypted message to the receiver. Next, receiver will decrypt the received message and then it will re-generate the verification hash code. Finally, the verification will be successful if this received, and the generated hash code matches

ISSN: 2366-1313

Keywords: Integrity verification, Data security, Wireless sensor network.

I INTRODUCTION

Wireless Sensor Network (WSN) is a special kind of wireless network consisting of sensor nodes to monitor a physical or environmental variables, such as sound, pressure, and temperature, etc. Nodes in WSN are very constrict units in detail of power, storing, and processing time due to small size constraint. Moreover, WSN sensor nodes operate with a small DC energy source that makes sensor nodes energy constrained. Sensor nodes communicate in self-organized fashion after being deployed in a wireless environment.

WSNs have a great impact on the development of streaming applications, such as financial analysis services, real-time transaction logs, automated systems controlling, home appliances, and scientific workflow systems. Moreover, sensors vary from the internal environments, such as body sensors to external environment, cameras positioning, and battle field monitoring. Data in sensor networks is produced at source node and processed by multiple intermediate sensor nodes until the data reaches a destination node. The destination nodes further communicate to the gateway also known as a base station (BS). The trustworthiness and reliability of sensory data are of paramount importance as the data is used in making critical decisions at BS. Data provenance can be used to assess the trust and reliability of the data at the BS and provide the important attributes to transmitted sensory data [8].

II. LITERATURE SURVEY

1.An efficient data aggregation protocol concentrated on data integrity in wireless sensor networks

https://www.researchgate.net/publication/258391486_An_Efficient_Data_Aggregation_Protocol_Concentrated_on_Data_Integrity_in_Wireless_Sensor_Networks

Wireless sensor networks consist of a great number of sensor nodes with strictly limited computation capability, storage, communication resources, and battery power. Because they are deployed in remote and hostile environments and hence are vulnerable to physical attacks, sensor networks face many practical challenges. Data confidentiality, data integrity, source authentication, and availability are all major security concerns. In this paper, we focus on the very problem of preserving data integrity and propose an Efficient Integrity-

ISSN: 2366-1313

Preserving Data Aggregation Protocol (EIPDAP) to guarantee the integrity of aggregation result through aggregation in sensor networks. In EIPDAP, base station can immediately verify the integrity of aggregation result after receiving the aggregation result and corresponding authentication information. However, to check integrity, most existing protocols need an additional phase which will consume a lot of energy and cause network delay. Compared with other related schemes, EIPDAP reduces the communication overhead per node to, where is the degree of the aggregation tree for the network. To the best of our knowledge, EIPDAP has the most optimal upper bound on solving the integrity-preserving data aggregation problem.

2.New improved two-phase interleaved converter with clamp circuit and diode capacitor cell.

https://www.researchgate.net/publication/339581060_New_Improved_Two-Phase_Interleaved_Converter_with_Clamp_Circuit_and_Diode_Capacitor_cell

This paper introduces a new improved two-phase DC-DC interleaved converter with clamp circuit and diode capacitor cell with coupled inductor for DC micro grid. 3 The key focus of this research is to amend voltage gain and to cut down the stress of the switches. The diode capacitor arrangement with coupled inductor used to attain twice the voltage gain. The capacitors are connected end to end at the output to dismiss the voltage ripple. The gain of the modified converter is improved by secondary winding of coupled inductor. The leakage energy of the inductance is recycled and voltage spikes of power switches during turn off operation are suppressed by clamp circuit. The theoretical analysis of the modified converter is verified through simulation. A prototype of 150W is constructed to demonstrate the efficient operation of the converter.

3. Smart methodology for performance improvement of energy sources for home applicationhttps://www.sciencedirect.com/science/article/abs/pii/S0141933119306325

The integrated solar and wind serves as a major contributor's for clean electrification in many nations. In this technical era energy crisis is primary issue due to depletion of nonconventional resources. Solar and wind available are charge less. The hybrid energy can be installed for domestic or commercial purpose, it is required to meet impetration of

ISSN: 2366-1313

power. To meliorate the pursuance of the hybrid energy, installed the continuous real time monitoring becomes necessary. IoT helps in monitoring the system by providing the detailed values of different parameters of plant over a dedicated IP address. This helps to maintain the plant over long distances by getting to know the values and thus maintain it to the desired levels. IoT helps in communicating the performance of the power generated and helps controlling the switch over between the energy sources available. A framework for energy source integrated with IoT is proposed to have fly back converter in continuous conduction mode along with multilevel inverter to decline the stress of current and escalate the power efficiency. The proposed venture not only helps in monitoring, controlling energy flow without any manual interference and power interruption, but also increases the productivity for the consumer and is highly reliable. In order to affirm the suggested venture a prototype module is made and executed.

4. Energy evaluation of data aggregation and authentication protocol (DAA) in wireless sensor networks.

https://www.researchgate.net/publication/268191003_Energy_Evaluation_of_Data_Aggregation_and_Authentication_Protocol_DAA_in_Wireless_Sensor_Networks

While security is an important feature in wireless sensor networks, but the energy constraints of sensor nodes should also be considered. In this work, the energy expenditure of such authentication protocol has been investigated respect to TelosB energy consumption behavior. Data Aggregation and Authentication protocol (DAA) integrates false data detection with data aggregation and confidentiality. DAA computes several Message Authentication Codes (MACs) and performs data aggregation along the path. Furthermore, integrity verification is carried out from source to destination. To evaluate precisely the energy efficiency of the scheme in the real world, a test bed implementation of DAA protocol is compared in terms of energy consumption with another authentication protocol. It is shown when the network is under attack and the amount of false data is high, DAA greatly outperforms traditional authentication techniques.

5.A secure data aggregation approach in hierarchical wireless sensor networks.

ISSN: 2366-1313

https://dl.acm.org/doi/10.1145/2857546.2857637

As wireless sensor networks (WSNs) are employed in many applications, security of these networks must be ensured. Considering the limited resources of nodes in WSNs, it is a critical challenge. Meanwhile, the deployed nodes are separated and they need to cooperatively transmit the sensed data to the base station. To reduce the amount of sending data, an aggregation approach can be applied along the path from sensors node to the sink. However, usually the carried information contains confidential data. Therefore, a security aggregation approach is required.

III SYSTEM ANALYSIS

EXISTING SYSTEM

The existing system for WSN security is vulnerable to attacks because it uses wireless communication and is deployed in outdoor environments. These factors make it difficult to secure the data collected by WSNs.

Limitations of Existing system

➢ High-Energy Consumption

➢ Scalability Issues

➢ Vulnerability to side-channel attacks

➢ Limited data integrity verification

PROPOSED SYSTEM

The proposed system, SUM, is more secure than the existing system because it uses a query-based approach. This means that SUM does not need to collect all of the data from the WSN in order to answer queries. Instead, SUM can query the WSN for specific pieces of data. This makes it more difficult for attackers to compromise the data collected by WSNs. This project implementing the Integrity Verification using Chaotic Technique and Data Security using Holomorphic Encryption.

Proposed system Advantages:

- Reduced energy consumption
- Enhanced scalability
- Improved data integrity
- Privacy protection
- Lightweight infrastructure

IV IMPLEMENTATION

Architecture:

ISSN: 2366-1313

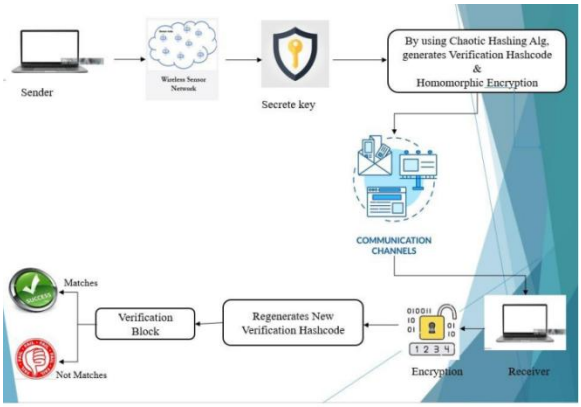


Fig-1. Architectures of the system model

MODULES:

To implement this project, we have designed following modules.

▪ Sender Module: Sender will select source and destination from simulation and then generate secret key and then calculate integrity code and then encrypt message and sent to receiver.

▪ Receiver Module: Receiver will receive message with Integrity code and then decrypted message and then regenerate Integrity code from decrypted message and if received and regenerated signature or integrity code matches then verification is successful.

▪ Network Simulation: We create a simulation module environment to generate WSN nodes and test data transmission between nodes for verification purpose.

▪ Testing and Evaluation: Here, we conduct through testing to ensure system correctness robustness and security to different scenarios. ▪ User Interface: We design user-friendly interface for sender and receiver to facilitate easy interaction with the system and monitor verification.

▪ Acknowledgement: We implement a feedback mechanism for the receiver to acknowledge verification result back to the sender.

Now-a-days wireless sensor networks are using everywhere for monitoring such as road traffic monitoring, CCTV home monitoring and many more. WSN are small tiny devices which sense data from its environment and report to centralized server for monitoring using IOT network connections. Sometime some malicious attackers can intrude or intercept network connection to alter messages and this altered message will report to centralized server which many take wrong decision based on received data. To overcome from such issues many encryption technologies were introduced which are based public or private keys and if this key exposed then data will be exposed to attacker. To tackle such problem, we are adding data Integrity Verification using chaotic technique and

ISSN: 2366-1313

data security using Holomorphic encryption. In propose technique we are sending Verification Hash code along with encrypted message and receiver will receive message and then decrypt the message and then regenerate Verification Hash code and if received and generated Hash code matched then verification will be successful. To generate Verification code we are taking sensor MESSAGE & Secret Key as Input and then convert and pad message to BINARY and then split binary data into blocks and then convert those blocks to 512 randomized hash code and in below screen we are showing code for Chaotic Hash code Integrity Algorithm.

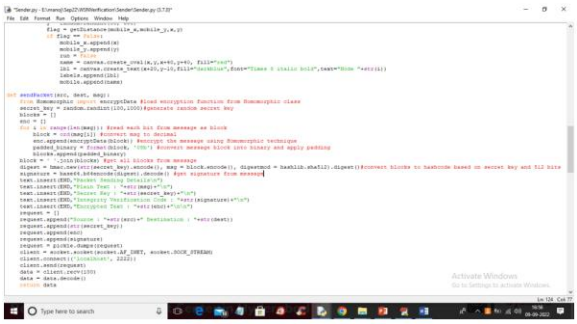


Fig-2: Red color comments to know about Integrity Code and homomorphic Encryption

Chaotic Technique

This project implementing the data integrity verification using chaotic technique and data security using homomorphic encryption. In proposed technique, the system will send a verification hash code along with encrypted message to the receiver. Next, receiver will decrypt the received message and then it will regenerate the verification hash code. Finally, the verification will be successful if this received, and the generated hash code matches.

Chaos-based encryption algorithms offer many advantages over conventional cryptographic algorithms, such as speed, high security, affordable overheads for computation, and procedure power. Chaotic techniques are a class of mathematical algorithms used for cryptography and data encryption. They are based on chaotic systems, which are deterministic systems that exhibit seemingly random and unpredictable behavior. Chaotic techniques use the inherent randomness of chaotic systems to generate cryptographic keys or encrypt data. The basic idea behind chaotic techniques is to use a chaotic system to generate a sequence of numbers that can be used as a cryptographic key or to encrypt data. The sequence of numbers generated by a chaotic system can be highly unpredictable, which makes it difficult for an attacker to guess the key or decrypt the data.

ISSN: 2366-1313

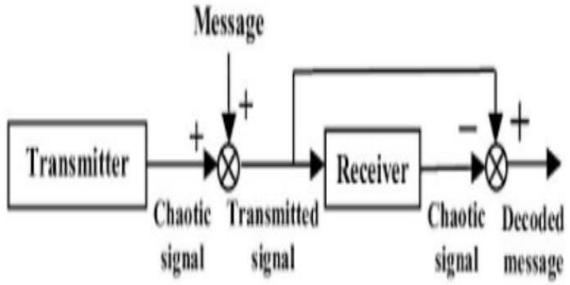


Fig-3: Chaotic Technique

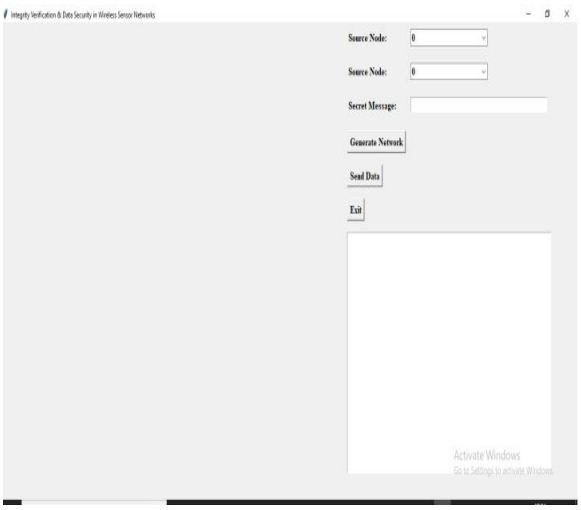
Homomorphic Encryption

Homomorphic encryption is a type of encryption that allows computation to be performed on encrypted data without first decrypting it. In other words, it allows operations to be performed on encrypted data while keeping the data encrypted throughout the computation process. The result of the computation is also encrypted, and can only be decrypted by the authorized user with the appropriate decryption key. Homomorphic encryption is useful in situations where data privacy and security are critical concerns. It allows sensitive data to be stored and processed securely, without the need for decryption and encryption at each step of the computation process. There are two main types of homomorphic encryption: fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE). FHE allows for any computation to be performed on encrypted data, while PHE allows for only a limited set of computations to be performed on encrypted data.

Fig-4: Homomorphic Encryption

V RESULT AND DISCUSSION

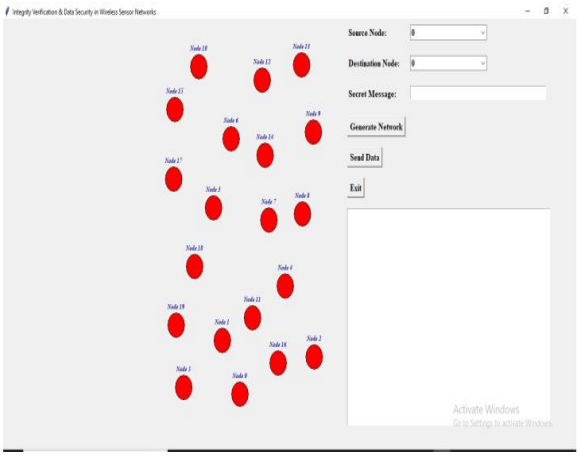
WSN network:



ISSN: 2366-1313

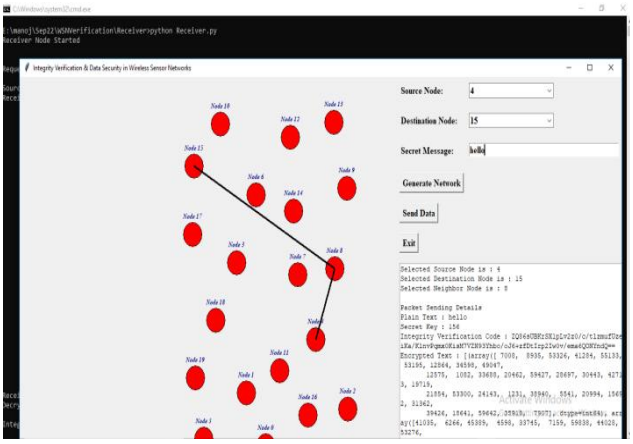
In above screen first click on 'Generate Network' button to create WSN network and get below output.

WSN Nodes:



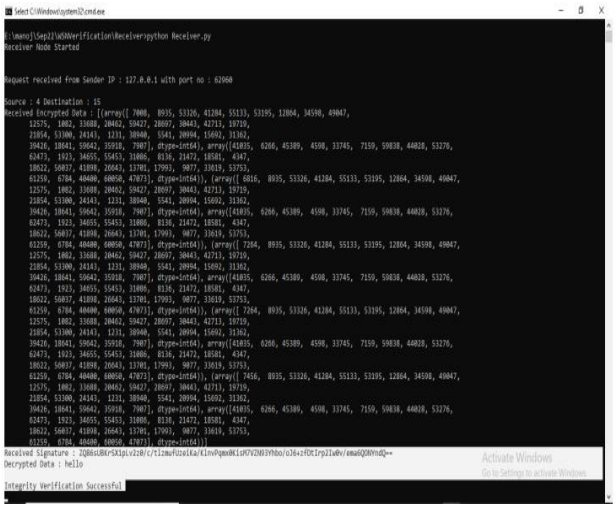
In above screen all red colour circles are the WSN nodes and now select any source and destination from source and destination drop down box and then enter some message in text field and then press 'Send Data' button to encrypt and send data to destination.

Data Transmission from Source and Destination:



In above screen source node 4 sending data to destination 15 by using neighbour node as 8 and in text area we can see all messages like Plain message, secret key, encrypted data and generated integrity code and then in below receiver screen will get decrypted data.

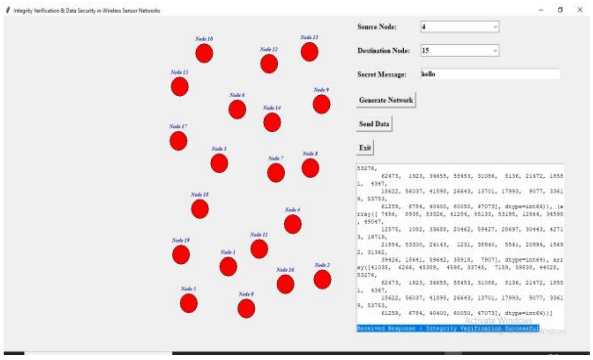
Acknowledgement in Sender Application:



In above receiver screen we can see received signature, decrypted message and verification successful and will get acknowledgement in sender application like below screen

Acknowledgement in Receiver Application:

ISSN: 2366-1313



VI CONCLUSION

Towards making several attacks never hurt the cloud storage, in this paper, we propose a public data verification scheme that ensures efficient verification and resists the malicious attacks. Unlike traditional solutions, the proposed scheme introduces symmetric encryptions to protect data privacy that is critical and suitable for practical use.

FUTURE ENHANCEMENT

Furthermore, real experimental results make the proposed scheme substantially more convincing.

VII REFERENCES

1. L. Zhu et al. An efficient data aggregation protocol concentrated on data integrity in wireless sensor networks. Int. J. Distrib. Sens. Netw. (2013)
2. M. Kavitha et al. New improved two-phase interleaved converter with clamp circuit and diode capacitor cell. Microprocess. Microsyst. (2020)
3. P. Sivagami et al. Smart methodology for performance improvement of energy sources for home application. MicroprocessMicrosyst. (2020)
4. S.P.T Prathima et al. ADA: authenticated data aggregation in wireless sensor networks. Int. J. Comput. Appl. (June 2017)
5. S. Naeimi et al. Energy evaluation of data aggregation and authentication protocol (DAA) in wireless sensor networks. IEEE (2012)
6. W. Min et al. A secure data aggregation approach in hierarchical wireless sensor networks.
7. Prasadu Peddi (2015) "A review of the academic achievement of students utilisinglarge-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.
8. K. Parmar et al. Aggregate MAC based authentication for secure data aggregation in wireless sensor networks
9. J. Kurmi et al. An approach for data aggregation strategy in wireless sensor

ISSN: 2366-1313

network using MAC authentication. Adv. Comput. Sci. Technol. (2017)

10. Prasadu Peddi (2019), "AN EFFICIENT ANALYSIS OF STOCKS DATA USING MapReduce", ISSN: 1320-0682, Vol 6, issue 1, pp:22-34.

AUTHORS

Mr. T. Layaraja,Assistant Professor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.

Email: Layaraaja@gmail.com

Miss. Punna Aishwarya, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: aishwaryapunna2002@gmail.com

Mr. P.Sampath, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: psk630200@gmail.com

Miss. V.Suraksha, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: velpulasuraksha01102002@gmail.com