International Journal of Science and Technology (IJST)
ISSN: 3049-1118, Volume- 2, Issue- 4 (Oct – Dec 2025)

A Study of Cryptographic Scheme for Safe Data Transfer in Wireless Sensor Network Involving Logic Gate

Deepali Chouhan[1*], S. S. Shrivastava[2]
[1,2]Department of Mathematics, Institute for Excellence in Higher Education, Bhopal

ABSTRACT:

The objective of this paper is to establish a lightweight logic gate–based cryptographic technique for secure data transfer in small to medium Wireless Sensor Networks, ensuring data confidentiality and efficient key management with minimal resource consumption. Wireless Sensor Networks (WSNs) are made up of small sensor nodes that collect data from their surroundings and send it to a central base station. As these networks grow, they become more exposed to security threats. So, it's important to use strong and efficient security methods. To keep communication secure and smooth in WSNs, cryptographic techniques are used. These techniques help protect the data and manage the keys used for encryption. However, choosing the right cryptography method is challenging because sensor nodes have limited power, processing speed, and memory. In large networks, symmetric cryptography (where the same key is used for both encryption and decryption) may not work well. That's why asymmetric cryptography (using different keys) is often preferred.

In this study, we suggest a new method based on electronic logic gates for symmetric encryption. This technique works well for small to medium-sized WSNs, offering secure communication without putting too much load on the sensor nodes.

Keywords: Encryption and Decryption, Symmetric Cryptography, Asymmetric Cryptography, Key management, Logic gates, WSN.

1. INTRODUCTION:

Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) are a new technology that is growing very quickly and has a bright future. They are made by combining modern electronic parts with wireless communication systems.

Wireless Sensor Networks (WSNs) are large systems made up of multiple small, wireless sensor nodes that collect and transmit data from their surrounding environment. Each sensor node is equipped with key components such as memory (storage), a small processor (for basic computations), sensors (to detect changes like temperature or motion), and a transmitter (to send data). While these components have limited computing power, they play a vital role in processing and sharing information within the network. [4, 6, 7]

*Corresponding Author Email: deepalii2004@gmail.com
Published: 20/10/2025
DOI: https://doi.org/10.70558/IJST.2025.v2.i4.241109

These nodes work together by collecting data and passing it from one node to another until it reaches a central system or base station. This cooperative process allows the network to function as a single, unified system. WSNs are used in a wide range of applications, including monitoring human health (like tracking organ activity), observing environmental changes, controlling temperature and humidity levels, and managing traffic flow in smart transportation systems. Their wireless nature and remote deployment, however, also make them vulnerable to security risks. [2]

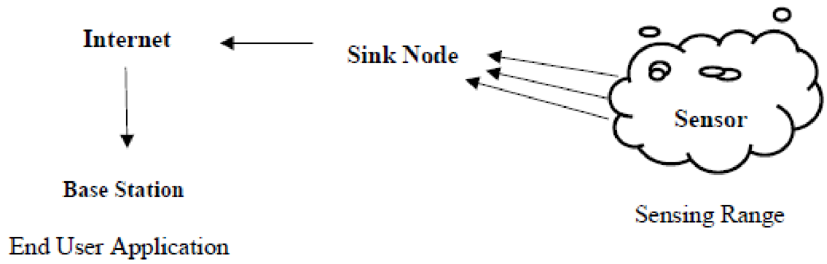

Figure 1: Wireless Sensor Networks

The main purpose of WSNs is to connect the real world with digital systems. A WSN has hundreds or even thousands of tiny devices. Each device can sense, process, and share information to watch what is happening in the environment.

These networks are used in large areas, even in places that are difficult or unsafe to reach. Because they are cheap and easy to install, WSNs are used in many different fields.

They help in studying human activities like health care, military security, and traffic control. They also help in monitoring nature and the environment, such as oceans, wildlife, earthquakes, pollution, wildfires, and water quality. In industries, WSNs are used to make buildings safer and to check how well machines are working. [5]

Attacks on WSNs:

In a Wireless Sensor Network (WSN), sensor nodes are usually scattered over a wide area rather than being placed in fixed locations. Because of this, it becomes difficult to monitor and control all the nodes from one central point. This lack of direct control makes it easier for unauthorized users to attack the network and cause security issues, even without physically touching the sensor nodes. [8]

2. SECURITY REQUIREMENT IN WSN:

A Wireless Sensor Network (WSN) is a special kind of network. It is similar to a regular computer network in some ways but also has many unique features. The security in a WSN is very important. It must protect both the data being shared and the network resources from attacks or harmful behaviour by nodes. The main security needs of a WSN are:

A. Confidentiality:

Confidentiality ensures that messages sent between users and receivers cannot be understood by anyone else in the network. Data Confidentiality is obtained in WSN with the help of the following statements:

1. Keeping data limited to the network.

2. Using secure connections for key management.

B. Integrity:

Integrity is about trusting the accuracy of data. Data integrity ensures that information is not changed accidentally or through malicious attacks. Source integrity ensures that the data truly comes from a trusted sender.

C. Authenticity:

Authenticity allows the receiver to confirm the true identity of the sender. This is usually done using passwords, keys, or other unique identification methods.

D. Non-repudiation:

Non-repudiation ensures that the sender cannot deny sending a message and the receiver cannot deny receiving it.

E. Availability:

Availability ensures that network data and resources are always accessible to authorized users. Even if there are internal or external problems, failures, or attacks, the data should remain available to legitimate users.

F. Freshness:

Data freshness ensures that the information received is new and has not been reused. In a WSN, there can be delays in data transfer, so it is important to confirm that the data is still fresh. This is done by using timestamps. There are two types of freshness:

- **Weak freshness:** Gives only a basic order of the data but does not allow measuring delays.
- **Strong freshness:** Provides a clear order of the data and makes it possible to calculate delays. [1]

3. ROLE OF CRYPTOGRAPHY IN SECURING WIRELESS SENSOR NETWORKS:

Wireless Sensor Networks (WSNs) are becoming more popular for various uses, such as climate studies, environmental monitoring, traffic control, and home automation. However, keeping these networks secure is a big challenge. Cryptography is one effective way to ensure security. It can be applied using symmetric key methods, asymmetric key methods, or hash functions.

Because WSNs have limited computing power, communication capacity, and battery life, they need lightweight cryptographic algorithms. Therefore, choosing the right cryptographic technique is very important to maintain security while matching the limitations of sensor nodes.

4. CRYPTPGRAPHIC TECHNIQUES:

To prevent the attacks mentioned above and to secure data in WSNs, cryptographic techniques are widely used as a key part of the network's security design. Cryptography is an encryption method that converts normal data packets into coded packets before sending them across the network. Instead of sending the original data directly, encrypted data is transmitted.

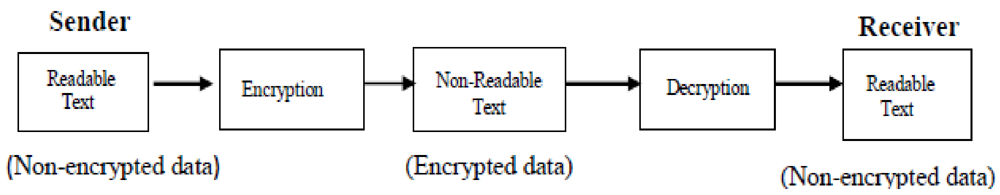

Figure 2: Cryptographic Technique

During this process, extra security bits are added to the data bits. This protects the original information from unauthorized access by attackers. These encryption methods also work well with existing network systems because they fit into the network's layered structure.

Choosing the right cryptographic method is very important because all security needs in WSNs depend on it. The cryptographic techniques used should match the limitations of sensor nodes and be checked for factors like code size, data size, processing speed, and power usage.

However, sensor nodes have limited processing power, storage, and memory. Because of this, traditional cryptographic methods cannot be directly applied to WSNs. To meet the security needs, existing methods must be adjusted, or new techniques need to be created specifically for WSNs.

Cryptographic techniques are used to ensure the fundamental security needs of confidentiality and integrity in networks. Broadly, there are two main types of cryptographic algorithms: Symmetric Cryptography (Secret Key) and Asymmetric Cryptography (Public Key)**.**

4.1 Symmetric Cryptography:

It uses one shared secret key for both encrypting and decrypting data packets in the communication network, and this key is kept confidential within the network as illustrated in the figure:

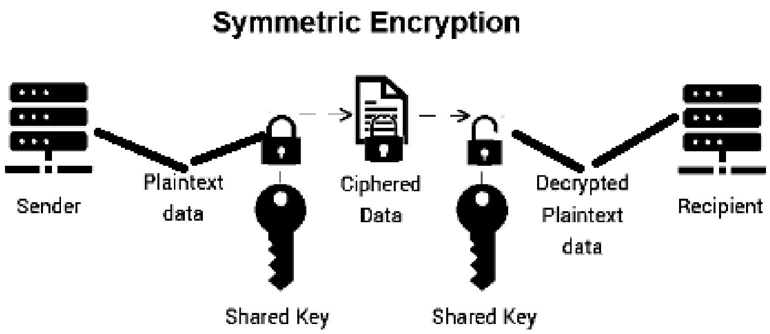

Figure 3: Symmetric Key Cryptography

In Symmetric Key Cryptography, a single key is used for both encrypting and decrypting information. For communication to work, all devices in the network must share this secret key and ensure it remains protected from unauthorized access. Managing and installing this key, however, can be challenging, especially when relying solely on symmetric keys. In open or less secure environments, where the chances of attacks are higher, the key must be updated frequently to maintain security.

4.2 Asymmetric Cryptography:

It uses two keys, a public key and a private key, for encrypting and decrypting data. This removes the risk of sharing a single key in the network and provides safer and more reliable security, as shown in the figure:

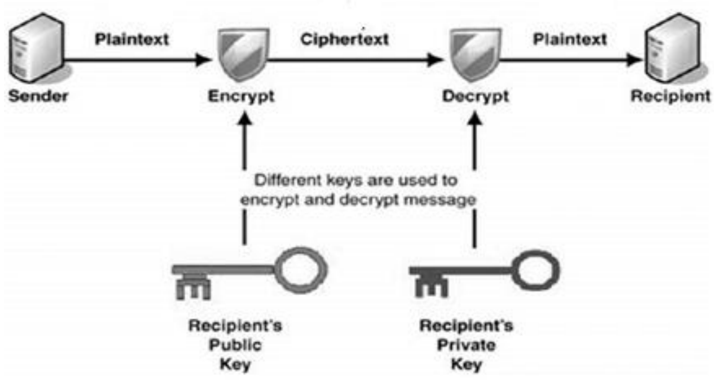

Figure 4: Asymmetric Key Cryptography

The keys work together to provide two-layer security. The public key is used to encrypt the data, while the private key is used to decrypt it. The private key is given only to authorized users so they can access the data. At the receiving end, a user can decrypt the data using their private key that matches the public key.

Public key systems are an alternative to symmetric key methods. They make key management easier and provide extra features that symmetric systems don't offer. Public key cryptography is an important and widely used technology that helps secure communication in both private networks and public networks like the Internet.

Public key cryptography uses two keys: a private key that is kept secret and a public key that is shared openly. In this method, the key used for encryption is different from the key used for decryption. This type of security method is known as asymmetric cryptography.

5. PROPOSED CRYPTOGRAPHIC TECHNIQUE FOR WSN:

The proposed method uses symmetric cryptography with a simple hardware or software setup. It works by using basic electronic logic gates like OR, AND, XOR, making it a logic gate–based cryptography approach. Each node in the WSN requires an IC chip containing these logic gates. Additionally, a Key Distribution Center (KDC) at the base station is needed to generate keys for every data transmission.

5.1 Logic Gate–Based Symmetric Cryptography:

The following points outline this method:

- A random key is generated with the same length as the plain text message to be encrypted.
- Each key is used only once and then discarded.
- The symbols and their representations are provided in Table 1.
- The key is combined with the message using OR gate as shown in Table 2.
- The key is then combined with the message using XOR gate to generate the cipher, as explained in Table 2.

- With the key and the cipher, the receiver applies the same process to recover the original message.

Symbols	**Meanings**
S	Sender
R	Receiver
REQ	Request for data
ACK	Acknowledgement
K	Key
Kd	Dummy Key
M	Message
Ck	Key Cypher
Cm	Message Cypher

Table 1: Abbreviations used in method

Input		Output			
A	B	OR GATE	AND GATE	XOR Gate	XNOR Gate
		Y = A+B	Y = A.B	Y = A’B+AB’	Y = A’B’+AB
0	0	0	0	0	1
0	1	1	0	1	0
1	0	1	0	1	0
1	1	1	1	0	1

Table 2: Truth table for used logic gates

5.2 Sender Side Request:

If sender S wants to send data to receiver R, it first sends a request to R for permission to transmit the data, as shown in the figure.

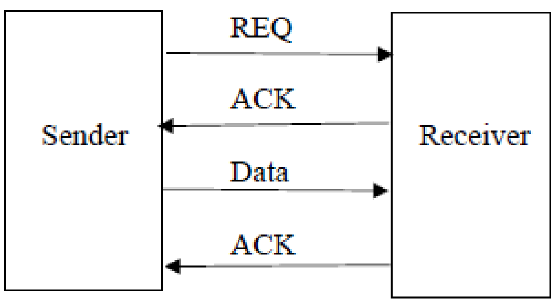

Figure 5: Sender Side Request

- Receiver R accepts the request and verifies whether S is an authorized node in the network.
- R then sends an acknowledgment (ACK) to S confirming the request.
- After getting the ACK, sender S transmits the data in encrypted form.
- Receiver R receives the encrypted data and decrypts it.
- Finally, R sends an acknowledgment to S confirming the successful receipt of the data.

5.3 Receiver Side Request:

If receiver R needs data from sender S, it first sends a request to S asking for the data, as shown in the figure 5.

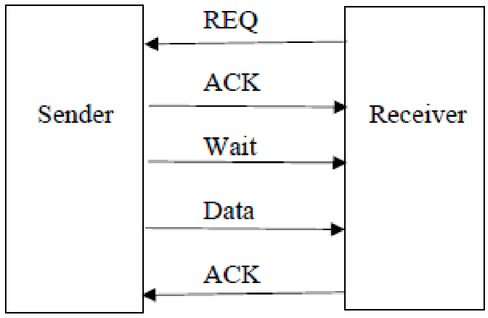

Figure 6: Receiver side request

- Sender S receives the data request and verifies if R is an authorized node in the network.
- S then sends an acknowledgment (ACK) confirming the request.
- S sends a wait signal, indicating some time is needed to locate the requested data.
- Once ready, S transmits the data to R in encrypted form.
- Receiver R receives the encrypted data and decrypts it.
- Finally, R sends an acknowledgment (ACK) to S confirming the successful receipt of the data.

6. METHODOLOGY:

Logic Gate–Based Encryption and Decryption

This cryptographic method uses electronic logic gates for both encryption and decryption. The key used for encryption is the same size as the message and is valid for one-time use only. A new key is generated for every new data transmission. [3]

Sender Side Process

1. The Key (K) and Dummy Key (Kd) are passed through an OR gate to generate the Key Cipher **(**Ck**)**.
2. The Key (K**)** and Swapping Adjacent Bits (say Ms) of Message **(**M**)** are passed through an XOR gate to create the Message Cipher **(**Cm**)**.
3. The same Key **(**K**)** is used only once and discarded after transmission.
4. The generated Key Cipher **(**Ck**)** and Message Cipher **(**Cm**)** are then sent to the receiver (R).

Receiver Side Process

ISSN: 3049-1118, Volume- 2, Issue- 4 (Oct – Dec 2025)

1. The receiver (R) receives both Key Cipher (Ck) and Message Cipher (Cm).
2. The Key Cipher (Ck) is combined with the Key (K) through an AND gate to retrieve the original key.
3. The retrieved key is matched with the stored key to ensure the authenticity of the message.
4. If the keys match, it confirms that the cipher is secure and no tampering has occurred.
5. Finally, the Key (K) and Message Cipher (Cm) are passed through an XOR gate (or XNOR gate) to reconstruct the original message.

Figure 7: Encryption of Key with Dummy Key **using OR gate and Decryption of Cipher Key with** Key **using AND gate**

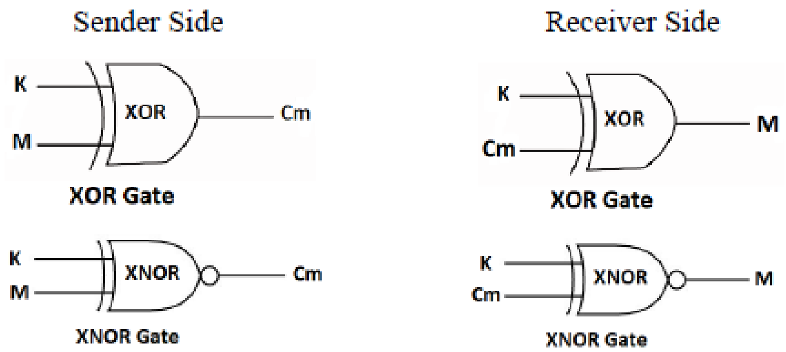

Figure 8: Encryption and Decryption of Message with key using XOR gate (or XNOR Gate)

7. ILLUSTRATION:

Now, we will illustrate the working of the proposed logic gate–based symmetric cryptography method using an example sentence for encryption and decryption.

Example Message (M):

"Operation Sindoor successfully evacuated thousands of Indian citizens from conflict zones, ensuring their safe return home under the government's coordinated rescue mission."

To better understand the process, let us demonstrate encryption and decryption for a **single word** from the message — **"evacuated."** To explain the process more clearly, let us take an example using **8-bit data transmission**.

To demonstrate the process in a more focused way, let us illustrate the encryption and decryption of the **alphabet "E"** from the word **"evacuated."**

Step 1: Let us consider a key (K) = 11110000, Dummy Key (Kd) = 10101010 and a message (M) = 00001110 (E = 00001110 from ASCII table), also Swapping Adjacent Bits of the message and say it Ms (i.e. 00001101).

Step 2: Generate Key Cipher (Ck)

- Pass K and Kd through an OR gate to get the Key Cipher **(**Ck**)**.

Step 3: Generate Message Cipher (Cm)

- Pass K and Ms through an XOR gate (or XNOR gate) to get the Message Cipher (Cm)**.**

Step 4: Transmission

- Send both Ck and Cm to the receiver for decryption.

Step 5: Decryption at Receiver Side

1. Use Ck and the key K with the AND gate to retrieve the original key.
2. Verify the key for authenticity.
3. Use Cm with the key K through the same XOR gate (or XNOR gate) to get back the Ms, after applying the Swapping Adjacent Bits we get original message (M).

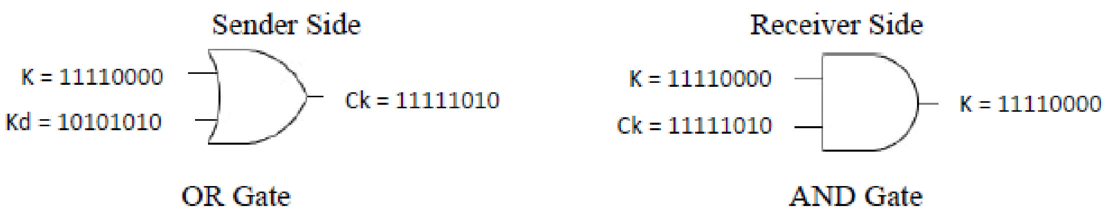

Figure 9: Key Cypher for 8-Bit System

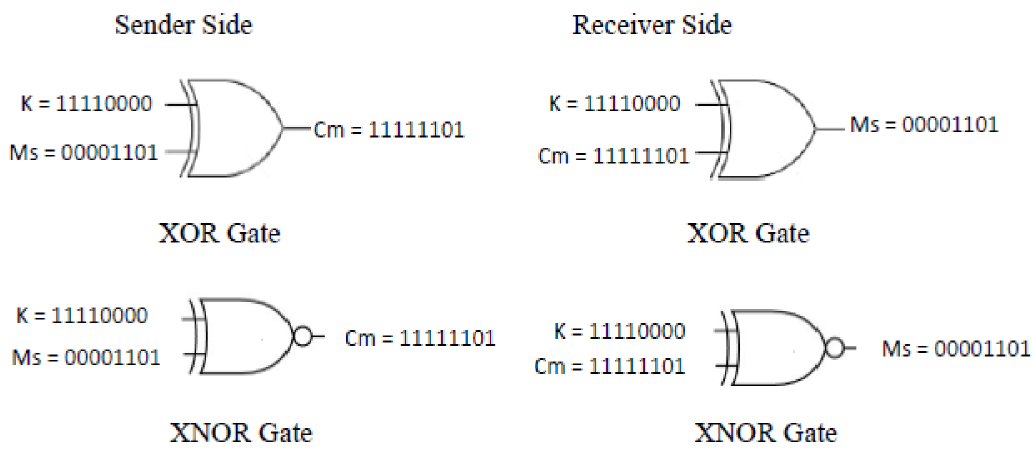

Figure 10: Message Cypher for 8-Bit System

By following this process, the entire word **"evacuated"** can be securely encrypted.

This example shows the complete encryption and decryption cycle for 8-bit binary data, demonstrating how secure transmission is achieved with this logic gate–based symmetric cryptography method.

8. ADVANTAGES OF THE PROPOSED LOGIC GATE–BASED SYMMETRIC CRYPTOGRAPHY

- Requires only a small electronic circuit integrated on an IC chip.
- Utilizes simple logic gates for both encryption and decryption.
- Places no additional load on the processor, ensuring efficient operation.
- Eliminates the need for complex mathematical calculations, making the process faster.
- Consumes very low battery power, ideal for resource-constrained devices like WSN nodes.
- Reduces the risk of attacks, as specialized hardware would be needed to compromise the system.

9. DISCUSSION:

- **XOR** remains dominant due to its equivalence to addition modulo 2, used in OTP and modern block ciphers.
- **XNOR** provides reversible encryption but lacks the strong mathematical integration found in XOR. It is more applicable in **hardware-efficient systems**.
- **Swapping Technique** enhances security by providing **diffusion**: even if attackers guess the key, swapped ciphertext adds complexity to brute-force and pattern analysis.

The 8-bit example confirms that XOR, XNOR, and swapping preserve reversibility while adding layers of security.

10. CONCLUSION AND FUTURE WORK:

Wireless Sensor Networks (WSNs) are becoming increasingly important in various applications, but their security remains a major concern due to issues like noise, interference, and limited energy, processing, and storage capacities. Cryptography plays a vital role in securing these networks. Among different techniques, the use of logic gate-based symmetric cryptography with secret sharing shows promising results for improving data security while keeping energy usage low. This makes them especially suitable for small and medium WSNs. Ensuring strong security mechanisms is essential for maintaining data integrity, confidentiality, and availability in these networks as their usage continues to grow.

This paper compared XOR and XNOR encryption with an added swapping technique. XOR remains the preferred operation in mainstream cryptography due to mathematical properties and efficiency. XNOR, while less common, holds promise in lightweight and embedded applications. Incorporating bit-swapping improves security by adding an additional obfuscation layer, making encryption more resistant to attacks. Future research may explore hybrid systems combining XOR, XNOR, and permutation strategies for lightweight cryptographic designs.

In the future, this research can be extended to improve the encryption of complex data types, such as images and videos, to make the method more efficient and applicable in real-world scenarios. Exploring advanced cryptographic techniques like pairing-based cryptography and Identity-Based Cryptography (IBC) could help achieve stronger and more flexible security solutions. These methods can also be improved to make them simpler and faster while still performing well, which will make them more useful for larger WSN networks.

REFERENCES

1. A. Faquihand & P. Kadam. Cryptographic Techniques for Wireless Sensor Network Security – A Survey, International Journal of Advanced Computational Engineering and Networking, Vol. 3, Issue 6, pp. 106-110, 2015.
2. E. Shi & A. Perrig. Designing secure sensor networks, Wireless communication magazine, Vol. 11(6), pp. 37-43, 2004.
3. Gupta Kumar Dinesh and Pathak Deepika: Safe Data Transfer Using Logic Gate Based Cryptographic Technique in Wireless Sensor Network, International Journal of Advanced Trends in Computer Science and Engineering, Volume- 10(4), pp. 2877-2884, 2021.
4. H. Dogra and J. Kohli: Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey, Indian Journal of Science and Technology, Volume- 9(47), pp. 1-5, 2016.
5. M. Panda. Security in Wireless Sensor Networks using Cryptographic Techniques, American Journal of Engineering Research (AJER), Vol. 03, Issue 01, pp. 50-56, 2014.
6. Satpute S. Reena and Thakare N. Amit: A Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 10, 2608-2613.
7. Sen, Jaydip. "A Survey on Wireless Sensor Network Security." International Journal of Communication Networks and Information Security (IJCNIS), Volume- 1, no. 2, pp. 55-78, 2009.
8. Y. Wang, G. Attebeery & B. Ramamurthy. A survey of security issues in Wireless Sensor Networks, IEEE Communication Surveys and Tutorials, Vol. 8(2), pp. 02-23, 2006.