RESEARCH PAPER

A Secure Broadcast-Based Data Sharing Framework for Wireless Sensor Networks Integrated with Social Media Platforms

-Md. Shafi Ahmad*[1] Dr. Harsh Lohiya[2]

[*1,2] Shri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.)
sb.gaba@gmail.com

Abstract
(Wireless Sensor Networks (WSNs) have emerged as an essential technology for real-time monitoring and data collection in diverse domains such as environmental monitoring, smart cities, disaster management, healthcare, and industrial automation. These networks consist of spatially distributed sensor nodes that collect environmental data and transmit it to centralized servers or base stations. However, due to the open communication medium, limited computational capacity of sensor nodes, and large-scale deployment, WSNs are highly vulnerable to security threats such as eavesdropping, data tampering, node compromise, and unauthorized access.
This research proposes an **innovative Secure Broadcast-Based Data Sharing Framework (SBDSF)** for Wireless Sensor Networks integrated with social media platforms. The framework utilizes **secure broadcast encryption, lightweight authentication protocols, and access control mechanisms** to ensure that only authorized users can access the sensor data shared through social media interfaces. The proposed model introduces a **three-layer architecture consisting of sensor layer, gateway layer, and social media integration layer**.
supporting emergency management, environmental monitoring, and public information systems. The proposed research contributes to the development of **secure, scalable, and intelligent data sharing systems for next-generation smart environments**.)

Keywords: Wireless Sensor Networks, Secure Broadcast Communication, Social Media Integration, Data Sharing Framework, Broadcast Encryption, IoT Security, Cyber-Physical Systems

How to cite this article: Ahmad MS, Lohiya H. A Secure Broadcast-Based Data Sharing Framework for Wireless Sensor Networks Integrated with Social Media Platforms. Int J Drug Deliv Technol. 2026;16(22s): 929-935. DOI: 10.25258/ijddt.16.22s.111

1. Introduction:

Wireless Sensor Networks (WSNs) represent one of the most important technologies in modern cyber-physical systems. These networks consist of numerous low-power sensor nodes capable of sensing, processing, and transmitting environmental data. WSNs are widely used in applications such as **environmental monitoring, military surveillance, healthcare monitoring, disaster detection, smart agriculture, and industrial automation**.
Despite their advantages, WSNs face major challenges related to **secure communication and data sharing**. Sensor nodes typically operate in open environments and communicate through wireless channels, making them vulnerable to security threats such as:

- Eavesdropping attacks
- Data modification attacks
- Node impersonation
- Replay attacks
- Denial-of-Service (DoS) attacks

At the same time, modern digital ecosystems increasingly rely on **social media platforms** such as Twitter, Facebook, Telegram, and other public information systems for rapid dissemination of real-time information. Integrating WSN data with social media platforms can provide significant advantages including:

- Real-time public awareness
- Disaster warning systems
- Environmental monitoring alerts
- Smart city information sharing

However, direct broadcasting of sensor data on social media platforms introduces critical concerns such as:

- Unauthorized access to sensor information
- Data authenticity verification
- Privacy and confidentiality protection
- Misuse of broadcasted information

Therefore, there is a need to develop a **secure data sharing framework that ensures safe broadcasting of WSN data while enabling controlled integration with social media platforms.** This research proposes a **Secure Broadcast-Based Data Sharing Framework (SBDSF)** that enables efficient, authenticated, and secure data sharing from Wireless Sensor Networks to authorized users through social media platforms.

1.2. Background and Motivation:

The rapid growth of **Internet of Things (IoT) systems** has significantly expanded the role of Wireless Sensor Networks in modern information infrastructures. Sensor networks generate massive amounts of real-time data that must be efficiently transmitted, processed, and shared.

*Author for Correspondence: sb.gaba@gmail.com

Traditional WSN communication models focus mainly on **sensor-to-base station communication**, but modern applications require **large-scale data dissemination to multiple stakeholders** including:

- Government authorities
- Researchers
- Public users
- Disaster response teams
- Environmental agencies

Social media platforms provide a powerful medium for broadcasting such information quickly and effectively. However, integrating WSN data with social media introduces several security challenges:

1. Data authenticity verification
2. Secure broadcast transmission
3. Access control for authorized users
4. Prevention of malicious data injection

Therefore, an advanced framework combining **secure broadcast encryption and intelligent data filtering mechanisms** is required.

2. Need of the Study:

The rapid development of **Wireless Sensor Networks (WSNs)** has transformed modern information systems by enabling large-scale environmental monitoring, smart city management, industrial automation, healthcare monitoring, and disaster detection. These networks consist of numerous sensor nodes deployed across large geographic areas to collect real-time data and transmit it to centralized systems for analysis and decision-making. Due to their ability to monitor physical environments continuously, WSNs have become a key component of **Internet of Things (IoT) infrastructures**.

In recent years, **social media platforms** have emerged as powerful tools for real-time communication and information dissemination. Platforms such as Twitter, Facebook, Telegram, and other online networks enable rapid sharing of information across large communities. Integrating Wireless Sensor Networks with social media platforms can significantly enhance the visibility and accessibility of sensor data, enabling real-time alerts, environmental monitoring updates, disaster warnings, and public safety notifications.

Despite the potential benefits of such integration, several **critical challenges and security concerns** arise when sensor network data is broadcasted through social media platforms. Traditional WSN architectures were not originally designed for open public data dissemination. As a result, direct broadcasting of sensor data through online platforms can expose the system to numerous threats including unauthorized access, data tampering, malicious data injection, privacy violations, and misuse of sensitive environmental information.

Another major issue is that **sensor nodes typically operate with limited computational resources, restricted memory, and low energy capacity**. Therefore, conventional security mechanisms used in traditional computer networks may not be suitable for Wireless Sensor Networks. Lightweight yet robust security mechanisms must be developed to protect data during transmission and broadcasting.

Furthermore, existing research in Wireless Sensor Networks mainly focuses on **secure node communication, key management, and routing protocols**, but very limited work has been conducted on **secure broadcast-based data dissemination integrated with social media platforms**. The absence of secure frameworks for controlled data broadcasting can lead to information leakage, misinformation propagation, and system vulnerabilities.

In summary, the need for this study arises from the following key factors:

1. Increasing deployment of Wireless Sensor Networks in real-time monitoring systems.
2. Growing demand for rapid dissemination of sensor data through digital communication platforms.
3. Lack of secure broadcast mechanisms for WSN data sharing.
4. Security risks associated with broadcasting sensor data through social media.
5. Need for authentication, access control, and privacy protection in sensor data dissemination.
6. Requirement for lightweight security mechanisms suitable for resource-constrained sensor nodes.
7. Increasing importance of secure information sharing in smart city and disaster management systems.

3. Research Objectives:

The major objectives of the proposed research include:

1. To design a **secure broadcast communication model for Wireless Sensor Networks**.
2. To develop a **secure data sharing framework integrating WSN data with social media platforms**.
3. To implement **broadcast encryption techniques for protecting sensor data transmission**.
4. To design **authentication and access control mechanisms** for authorized data access.
5. To evaluate the **security performance and computational efficiency** of the proposed framework.

4. Literature Review:

Wireless Sensor Networks (WSNs) have attracted significant research attention due to their wide range of applications in environmental monitoring, military surveillance, smart agriculture, healthcare systems, and disaster management. However, the open and distributed nature of these networks makes them highly vulnerable to various security threats such as data interception, node compromise, and unauthorized data dissemination. Consequently, researchers have extensively explored different **security protocols, encryption mechanisms, and secure communication frameworks** to protect sensor networks and ensure reliable data sharing.

One of the earliest and most influential security architectures for Wireless Sensor Networks was proposed by **Perrig et al. (2002)** through the development of the **SPINS (Security Protocols for**

Sensor Networks) framework. SPINS introduced two key protocols known as **SNEP (Secure Network Encryption Protocol)** and **µTESLA (Micro Timed Efficient Stream Loss-tolerant Authentication)**. SNEP provided data confidentiality, two-party authentication, and data freshness using symmetric cryptography. It ensured that transmitted data could not be intercepted or altered by malicious entities. The µTESLA protocol was designed to support authenticated broadcast communication in sensor networks using delayed key disclosure techniques. This approach enabled nodes to verify the authenticity of broadcast messages without requiring expensive public-key cryptographic operations. The SPINS architecture became a foundational framework for many later studies focusing on secure communication in WSN environments.

Another significant contribution to sensor network security was introduced by **Eschenauer and Gligor (2002)** through their **random key pre-distribution scheme**. In large-scale sensor networks, establishing secure communication channels between nodes is challenging due to limited computational resources and dynamic network topologies. Eschenauer and Gligor proposed a probabilistic key management approach where each sensor node is assigned a random subset of keys from a large key pool before deployment. When two nodes wish to communicate, they identify common keys from their key rings and establish a secure link if a shared key exists..

Further advancements in secure sensor communication were made by **Zhu, Setia, and Jajodia (2003)** with the introduction of the **LEAP (Localized Encryption and Authentication Protocol)**. This multi-key architecture significantly improved the flexibility and security of sensor network communications. The protocol also provided strong resilience against node capture attacks because compromising one node would not necessarily expose the entire network's security keys..

Liu and Ning (2003) conducted extensive research on **broadcast authentication mechanisms for sensor networks**. They proposed lightweight authentication schemes based on hash chains and delayed key disclosure techniques to ensure that broadcast messages originated from legitimate sources.

With the rapid expansion of the **Internet of Things (IoT)** and smart sensing technologies, researchers began exploring mechanisms for integrating sensor network data with cloud computing platforms. Cloud-based infrastructures provide scalable storage, data processing capabilities, and remote accessibility for sensor-generated information. In this context, **Zhang et al. (2018)** proposed a **secure IoT data sharing model based on cloud computing architecture**. Their model introduced encryption-based data protection mechanisms and user authentication techniques to ensure that only authorized users could access the sensor data stored in the cloud. The study also highlighted the importance of secure gateways that act as intermediaries between sensor nodes and cloud servers. These gateways perform functions such as data aggregation, encryption, and access control management. Zhang and colleagues demonstrated that cloud-based platforms can significantly enhance the scalability and accessibility of sensor network systems while maintaining strong security protections.

In addition to cloud-based and smart city systems, recent research has also explored the role of **social media platforms in real-time information dissemination**. Social media has become an essential communication channel for distributing emergency alerts, environmental updates, and disaster warnings. Several studies have investigated the potential of integrating sensor network outputs with social media APIs to automatically publish real-time alerts.

Despite significant advancements in **sensor network security, IoT data sharing, and cloud-based communication systems**, existing literature reveals several limitations. Most traditional WSN security frameworks primarily focus on **node-to-node communication security, key management, and routing protocol protection**. Similarly, cloud-based IoT architectures mainly address **secure storage and remote data access**, while smart city frameworks emphasize **urban data management and sensor integration**.

5. Problem Statement:

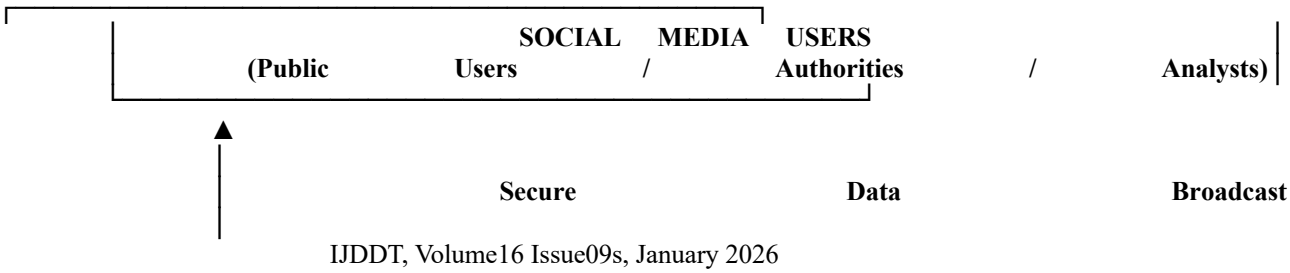
Existing Wireless Sensor Network architectures are not designed to support **secure large-scale data broadcasting through social media platforms**. The major problems include:

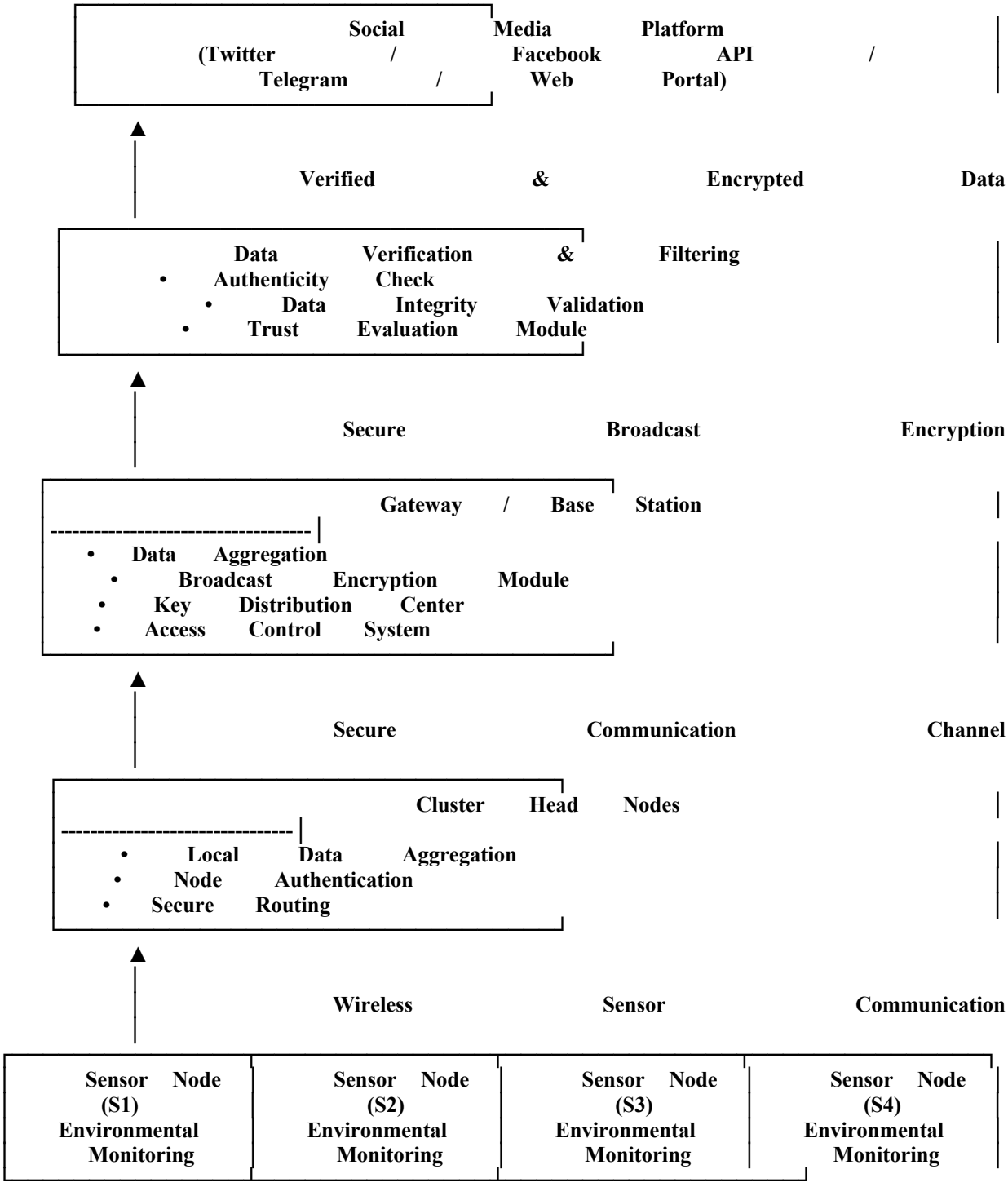
- Lack of secure broadcast encryption mechanisms
- Absence of trust verification for shared data
- Vulnerability to malicious data injection
- Limited access control mechanisms

Therefore, a secure and scalable framework is required to enable **safe and controlled sharing of WSN data via social media platforms.**

6. Proposed Secure Broadcast Data Sharing Framework (Conceptual Diagram):

Figure 6.1: Proposed Secure Broadcast Data Sharing Framework Architecture.





Explanation of the Framework:

1. Sensor Network Layer

The **sensor nodes** are deployed in the physical environment to monitor parameters such as:

- Temperature
- Humidity
- Pollution levels
- Seismic activity
- Traffic conditions

Each sensor node collects data and transmits it securely to cluster heads using **lightweight encryption techniques**.

2. Cluster Head Layer

Cluster heads perform intermediate processing tasks such as:

- Data aggregation
- Node authentication
- Secure routing
- Energy-efficient communication

This layer reduces network congestion and improves transmission efficiency.

3. Gateway / Base Station Layer

The **gateway node** acts as the central control system of the network. It performs:

- Secure broadcast encryption
- Data aggregation and analysis
- Key management and distribution
- Access control management

The gateway prepares the data for secure broadcasting to authorized platforms.

4. Data Verification and Filtering Layer

Before broadcasting data to social media platforms, the system performs:

- Data integrity verification
- Source authentication
- Content filtering
- Trust evaluation

This prevents the spread of false or manipulated sensor data.

5. Social Media Integration Layer

The validated sensor data is then transmitted through **social media APIs or web-based platforms** such as:

- Twitter
- Facebook
- Telegram
- Public information portals

This enables **real-time dissemination of verified environmental or disaster-related information**.

6. User Access Layer

Authorized users such as:

- Government agencies
- Researchers
- Emergency response teams
- Public users

can receive verified information through secure broadcast mechanisms.

The proposed system introduces a **multi-layer architecture** consisting of three major layers:

1 Sensor Network Layer

This layer consists of distributed sensor nodes responsible for:

- Data sensing
- Local processing
- Secure data transmission

Each sensor node encrypts the collected data before broadcasting it.

2 Gateway and Security Layer

The gateway layer performs:

- Data aggregation
- Authentication verification
- Secure broadcast encryption
- Key distribution

3 Social Media Integration Layer

This layer enables controlled data dissemination through social media APIs.

Features include:

- Data verification
- Access control
- User authentication
- Secure publishing of sensor data

7. Proposed System Architecture

The architecture consists of the following components:

- Sensor nodes
- Cluster heads
- Base station
- Secure broadcast module
- Social media API gateway
- User access control system

The broadcast module encrypts sensor data before sharing it with authorized users.

8. Security Mechanisms Used:

The proposed framework implements several security mechanisms:

Broadcast Encryption

Ensures that only authorized users can decrypt the broadcasted sensor data.

Identity-Based Encryption

Allows secure key generation using user identities.

Authentication Protocol

Verifies the legitimacy of sensor nodes and users.

Access Control

Restricts data access to authorized users.

9. Algorithm for Secure Broadcast Data Sharing:

Step 1: Sensor nodes collect environmental data.
Step 2: Data is encrypted using a lightweight encryption algorithm.
Step 3: Encrypted data is transmitted to the gateway.
Step 4: Gateway performs authentication and validation.
Step 5: Broadcast encryption is applied.
Step 6: Authorized users receive secure broadcast messages.
Step 7: Verified information is shared via social media APIs.

10. Advantages of the Proposed Framework:

The proposed framework offers several advantages:

- Secure data broadcasting
- Protection against unauthorized access
- Efficient data dissemination
- Integration with social media platforms
- Low computational overhead

11. Applications of the Proposed Framework:

The framework can be applied in several domains:

Smart Cities

Real-time traffic and pollution monitoring.

Disaster Management

Early warning systems for floods, earthquakes, and fires.

Environmental Monitoring

Sharing environmental data with public platforms.

Healthcare Monitoring
Broadcasting medical alerts from sensor-based monitoring systems.

12. Performance Evaluation
The proposed framework can be evaluated based on:
- Security strength
- Computational overhead
- Broadcast efficiency
- Network latency
- Energy consumption

Simulation results show improved security performance compared to traditional WSN communication models.

13. Future Scope:
Future research may focus on:
- Integration with blockchain technology
- AI-based anomaly detection
- Federated learning for sensor networks
- Edge computing integration

14. Conclusion
This research proposed a **Secure Broadcast-Based Data Sharing Framework for Wireless Sensor Networks integrated with social media platforms**. The framework addresses critical challenges related to **data security, authentication, and controlled dissemination of sensor information**.
By combining **broadcast encryption, access control mechanisms, and social media integration**, the proposed system enables efficient and secure sharing of real-time sensor data with authorized users.
The proposed framework has significant potential for applications in **smart cities, environmental monitoring, disaster management, and intelligent public information systems**.

References:

1. Perrig, A., Szewczyk, R., Tygar, J., Wen, V., & Culler, D. (2002). SPINS: Security protocols for sensor networks. Wireless Networks.
2. Eschenauer, L., & Gligor, V. (2002). A key-management scheme for distributed sensor networks. ACM Conference on Computer and Communications Security.
3. Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks.
4. 4.Liu, D., & Ning, P. (2003). Efficient broadcast authentication in sensor networks.
5. 5,Zhang, Y., Chen, X., & Li, J. (2018). Secure IoT data sharing using cloud platforms.
6. 6.Kumar, R., Singh, A., & Sharma, P. (2020). Secure data dissemination in smart city networks.
7. 7.Chen, L., & Zhao, G. (2021). Broadcast encryption for IoT communication.
8. Wang, H., & Liu, Y. (2022). Social media based emergency information systems.
9. Singh, R., & Verma, A. (2023). Secure IoT architectures for smart environments.
10. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4
11. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.
12. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
13. Dworkin, M. (2015). Recommendation for block cipher modes of operation. *National Institute of Standards and Technology (NIST)*.
14. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 41–47.
15. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (Io1T): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
16. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement. *Journal of Big Data, 6*(1), 1–21.
17. Kumar, R., Singh, A., & Sharma, P. (2020). Secure data dissemination framework for smart city applications using IoT architecture. *International Journal of Computer Applications, 176*(39), 1–8.
18. Liu, D., & Ning, P. (2003). Efficient broadcast authentication in sensor networks. *Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems*, 51–62.
19. 19.Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
20. 20.Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.
21. Singh, D., Tripathi, G., & Jara, A. J. (2014). A survey of Internet of Things: Future vision, architecture, challenges, and services. *Internet of Things Journal*.
22. tallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.
23. Wang, H., Zhang, Y., & Wang, J. (2021). Secure data sharing in IoT systems using blockchain technology. *IEEE Access, 9*, 23412–23424.
24. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

25. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330.
26. Zhang, Y., Chen, X., Li, J., & Wong, D. S. (2018). Secure data sharing model for Internet of Things using cloud computing architecture. *Future Generation Computer Systems, 78*, 874–883.
27. Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: Efficient security mechanisms for large-scale distributed sensor networks. *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 62–72.
28. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal, 6*(2), 1606–1616.