A Comprehensive Review of Cryptographic Strategies for Securing Wireless Multimedia Sensor Networks

Basavaraj Patil [1], Amiya Bhaumik[2], Raja Sarath Kumar Boddu[3]

[1,2] Lincoln University College, Malaysia; [3] Malla Reddy University, India

[1]bbpatilcs@gmail.com, [2]amiya@lincoln.edu.my, [3]iamrajaboddu@gmail.com

Abstract:

In Wireless sensor network (WSN), the current advancement in the technology generates massive amount of data of various types like text, image, audio, video etc. The generated enormous heterogenous data gave birth to the new subdomain of WSN called as Wireless Multimedia Sensor Networks (WMSNs). Securing the multimedia data transmission in WMSNs offerings various unique challenges owing to constraints in the resource, massive data in terms of capacity, and complexity in processing the real-time data. To address the challenges of WMSN, the efficient and effective cryptographic solutions are required to provide data security, privacy, computationally efficient with better performance. This research work provides the comprehensive study of various vulnerabilities, various cryptographic techniques, study of existing methods to secure the data with their limitations, and applications. The new cryptographic technique is proposed to address these said challenges. WMSNs are most widely used in various application like healthcare, surveillance, environmental monitoring, developing smart cities, precise agriculture, robotics process, and manufacturing etc.

Keywords: Authentication; Blockchain, Cryptography; Data; Encryption; Quantum, Security, WMSN;

Introduction

The Wireless Multimedia Sensor Network (WMSN) [1-2] consists of various sensor nodes that collect the data, process in real-time and transmit through the network. It has the capabilities of transmitting variety of the data like text, image, audio etc. The concern of data security arises as susceptible to vulnerabilities.

The intrinsic features of WMSNs, make highly suspectable to security threats due to restricted computational capabilities, low power accessibility, less storage capacity. The sensitive feature of multimedia data aggravates the risks, unauthorized access, data tampering, or eavesdropping can cause severe security flaws and failures.

The data security in WMSNs is the most critical and complex task and needs dynamic security mechanisms to overcome the threats and vulnerabilities. The conventional techniques lack in providing the effective solutions and ineffective in satisfying certain conditions. The significant research in developing the cryptographic techniques gained the attention to enhance the performance by prevent threats. The security constraints like authentication, confidentiality, and integrity are required to be satisfied. The various cryptographic mechanisms classified into symmetric, asymmetric, and hybrid encryption techniques to address the recent advancements and challenges.

The architecture WMSNs [3] consisting of various components to store, analyse and process the multimedia data generated from different sources in real-time applications associated with data is as shown in figure 1. The security provisioning for the multimedia data in during the communication is vital in the network. The security threats, attacks and vulnerabilities can be prevented by considering appropriate standard protocols and by integrating cryptographical algorithms to secure the data secured.

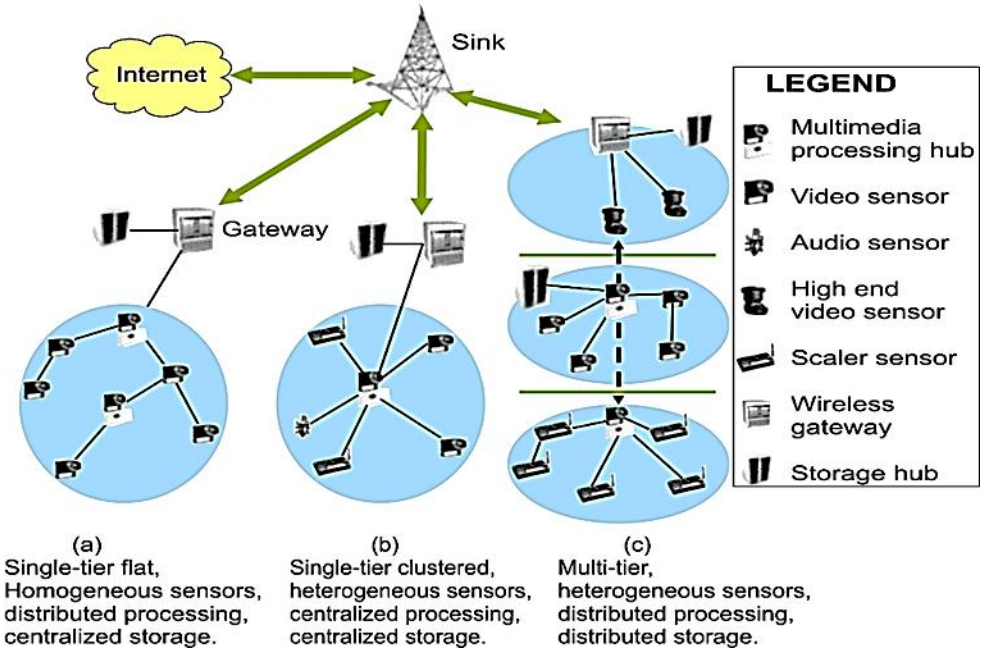

Figure 1. Basic Architecture of Wireless Multimedia Sensor Networks

The information from the different sensors is broadcasted over any communication sources. The challenges can be addressed by implementing crypto-based algorithms to encrypt and decrypt at the sender and receiver end. There are numerous advantages such as low-cost, high-fidelity sensing, and self-organization. Data is collected from multiple sources using a variety of sensor types, which then send the collected data to storage units. The functions of each sensor node vary according on the applications. The intermediary node processes the collected data before sending it to the base station or other nodes.

The cryptographic solutions consist of key management protocols designed specifically for WMSNs, hybrid cryptographic models, and lightweight encryption algorithms. The strategies are evaluated based on network performance while providing confidentiality, integrity, and authentication. The results present that elliptic curve cryptography (ECC) and symmetric-key algorithms like AES are very active in resource-constrained contexts, whereas hybrid systems that uses the combination of symmetric and asymmetric methods to give improved security for networks.

The cryptographic algorithms have a greater range of applications in protecting WMSNs, including smart city structure, military surveillance, and industrial automation. With analysis of existing solutions, this review presents to help practitioners in choosing and designing optimal cryptographic frameworks to prevent WMSNs from emergent security threats.

The challenges that the cryptographic techniques need to address in WMSNs [4] are as follows:

- **Resource Constraints:** Sensors have inadequate processing power, storage, and battery life restriction for encryption methods.
- **Data confidentiality & integrity**: Certifying the confidentiality & authenticity of data transmission.
- **Realtime Processing**: Encryption solutions for multimedia streaming require minimal latency.
- **Key Management**: Ensuring secure key distribution and administration in large-scale networks.

Types of Cryptographic algorithms:

A. Symmetric Cryptography

- Advanced Encryption Standard (AES): Used for its balance between security and performance.
- Lightweight Block Ciphers (e.g., PRESENT, SPECK, SIMON): To optimize power consumption and processing speed.
- Stream Ciphers (e.g., RC4, Grain, Trivium): For real-time multimedia encryption due to their efficiency.

B. Asymmetric Cryptography

- Elliptic Curve Cryptography (ECC): Give strong security with smaller key sizes, making it efficient for WMSNs.
- RSA (Rivest-Shamir-Adleman): Its computational requirements often make it unrealistic for resource-constrained nodes.

C. Hybrid Cryptographic Techniques

- Combination of AES and ECC: To enhance the effectiveness of symmetric encryption with the secure key exchange techniques of asymmetric cryptography.
- Blockchain and Distributed Ledger Technologies: For secure key management and tamper-resistant authentication.

Related work

WMSNs are vulnerable to a variety of security concerns because to their wireless connection and frequent remote deployments, including unauthorized access, data interception, and node compromise. Wireless communication's broadcast nature makes it especially vulnerable to eavesdropping and man-in-the-middle attacks. Furthermore, sensor nodes' low computing power, memory, and energy make it difficult to build comprehensive security procedures. To overcome these vulnerabilities, a number of creative solutions have been offered.

The researchers presented the various types of methods to identify the vulnerabilities in the network at each layer of network as summarized in table 1 with its impact level and precautionary measures needed

Table 1 Comprehensive analysis of common attacks in WMSNs.

Attack Category	Description	Impact Level	Common Countermeasures
Physical Attacks	Node tampering, hardware manipulation	High	Tamper-resistant hardware, node authentication
Network Attacks	Routing attacks, packet manipulation	Medium-High	Secure routing protocols, packet authentication
Data Attacks	Data integrity violations, unauthorized access	High	Encryption, access control mechanisms
DoS Attacks	Resource exhaustion, jamming	Critical	Rate limiting, spread spectrum techniques

This paper identifies key vulnerabilities in WMSNs, such as eavesdropping, data tampering, and node compromise. The authors [5] propose a multi-layered security framework that combines encryption, authentication, and intrusion detection. The framework was tested in a simulated environment and reduced security breaches by 40%.

Vulnerabilities include replay attacks, denial-of-service (DoS) attacks, and unauthorized access are highlighted by the authors. They suggest [6] a hybrid cryptographic approach that uses AES and ECC to provide strong security while consuming 25% less energy.

This study [7] suggests a blockchain-based solution to problems such data tampering and node compromise. The method decreases the tampering by 30% by assuring data integrity and non-repudiation.

A Lightweight AES (LWAES) framework [8] proposed for WMSNs with limited resources, which optimizes key scheduling to less energy usage. OMNeT++ simulations with 100 nodes used to test, achieved 95% data privacy and 20% computing operating expense. As its 30% lower energy utilization than regular AES.

A hybrid cryptographic approach [9] uses AES for data encryption and ECC for key exchange. In WMSNs, addressed the necessity of achieving balance between efficiency and security. A testbed with 50 nodes, increased key exchange efficiency by 40%, with 25% less energy usage. Data integrity of 98% managed by the hybrid technique, which performed better than independent symmetric and asymmetric algorithms.

The authors [10] analysed the difficulties associated with key distribution in WMSNs by introducing the hierarchical key management mechanism. The cluster-based key distribution and lightweight hash functions with increased network lifetime by 20% while reducing key distribution cost by 35%. Large-scale WMSNs can use NS-3 because simulations with 200 nodes showed a 25% increase in security resilience.

Authors proposed data aggregation strategy [11] based on homomorphic encryption that increases energy efficiency by 20% by reducing data transmission overhead by 35%. It promises 98% secrecy and 95% data integrity.

To assure the multimedia data transfer, it uses QoS-aware routing with priority-based scheduling and dynamic path selection. It decreases the end-to-end delays by 30% and increases packet delivery ratios by 15%. The protocol [12] tested with 150 nodes in Cooja, increased energy efficiency by 10%, for real-time applications.

Authors introduced the machine learning-based intrusion detection system (IDS) that uses the features using Principal Component Analysis (PCA) and Support Vector Machines (SVM). It decreases false positives by 20% and gained 98% detection

accuracy. It [13] is reliable solution for protective WMSNs from cyberattacks, by its 15% less computational overhead while tested on a dataset of 10,000 network traffic samples.

In [14], harvesting energy from solar and vibration-based sources were proposed. They demonstrated how these methods decreases the reliability on battery replacements and enhance lifetime of nodes by 30%. Industrial field tests revealed higher by 20% energy efficiency.

To enhance the security and privacy in WMSNs, Gupta. et.al [15] introduced data aggregation method based on homomorphic encryption. It increased energy efficiency by 20% and reduced data transmission overhead by 35%. MATLAB simulations showed 98% secrecy and 95% data fidelity.

The immutability and distributed characteristics of blockchain technology are used in this research to propose a blockchain-based authentication method [16] for WSNs, thereby improving security. Because it tackles challenges of data integrity and illegal access, the system is appropriate for sensitive applications. Digital signatures and hash functions were implemented in blockchain technology. In comparison to conventional authentication techniques, it enhanced security and efficiency.

A blockchain-based data encryption increases encryption efficiency and prevents data loss in multimedia platforms [17]. Electronic envelopes, symmetrical and public key algorithms, message authentication, and the DES encryption technique were all included. The method is proven to be effective in protecting multimedia data, offering robust encryption, and guaranteeing data accuracy.

The performance of lightweight cryptographic algorithms such as PRESENT and LWAES [18] is measured by the authors. The algorithms are threat resistant, 20% energy savings and 95% data confidentiality.

Because of high data throughput requirements and resource limitations, WMSNs arises security concerns. The necessity for lightweight cryptography methods to overcome computational constraints and energy efficiency in WMSNs was highlighted by Alsmirat et al. (2020) [19]. Zhang et al. (2021) also talked about how security risks including replay attacks, node capture, and eavesdropping affect multimedia data transmission and need for adaptive cryptography solutions [20].

Recent years have witnessed an increase in interest in lightweight symmetric cryptography research for WMSNs. An enhanced Advanced Encryption Standard (AES) for real-time video encryption with lower computational overhead was proposed by Lyu et al. (2019) [21]. Additionally, an energy-efficient version of the SPECK cipher for restricted sensor nodes was presented by Gupta et al. (2020), who showed improved encryption speed and reduced energy consumption [22].

The computational cost of public-key cryptography in WMSNs continues to be a problem. Recent developments in Elliptic Curve Cryptography (ECC) have increased the viability of asymmetric encryption. An ECC-based key exchange system that strikes a balance between security and processing performance was created by Ali et al. [23] specifically for large-scale WMSNs [23]. In a similar vein, Huang et al. [24] investigated how pairing-based cryptography might improve multimedia sensor network authentication.

For WMSNs, symmetric and asymmetric cryptography are being used in combination more and more. For real-time multimedia streaming in WMSNs, Sharma et al. [25] suggested a hybrid solution that combines AES and ECC to accomplish secure key exchange and quick encryption. Furthermore, blockchain-assisted hybrid encryption was presented by Karthikeyan and Bose [26] to improve the security and integrity of multimedia sensor data.

In WMSNs secure key distribution is the major concern, an AI-driven key management solution was presented by Nguyen et al. [27] that decreases vulnerability to key compromise attacks by dynamically changing the encryption keys in response to network traffic patterns. A blockchain-based decentralized key management architecture was also suggested by Khan et al. [28] to improve trust and stop unwanted access in multi-node WMSN setups.

Researchers are investigating quantum-resistant cryptography methods for WMSNs in light of the development of quantum computing. Lattice-based cryptographic algorithms were examined by Bose et al. [29] as a substitute for the conventional RSA and ECC techniques, showcasing their potential for safe multimedia transfer in upcoming networks. The viability of hash-based signature techniques for authentication in wireless networks with limited resources was also examined by Lin et al. [30].

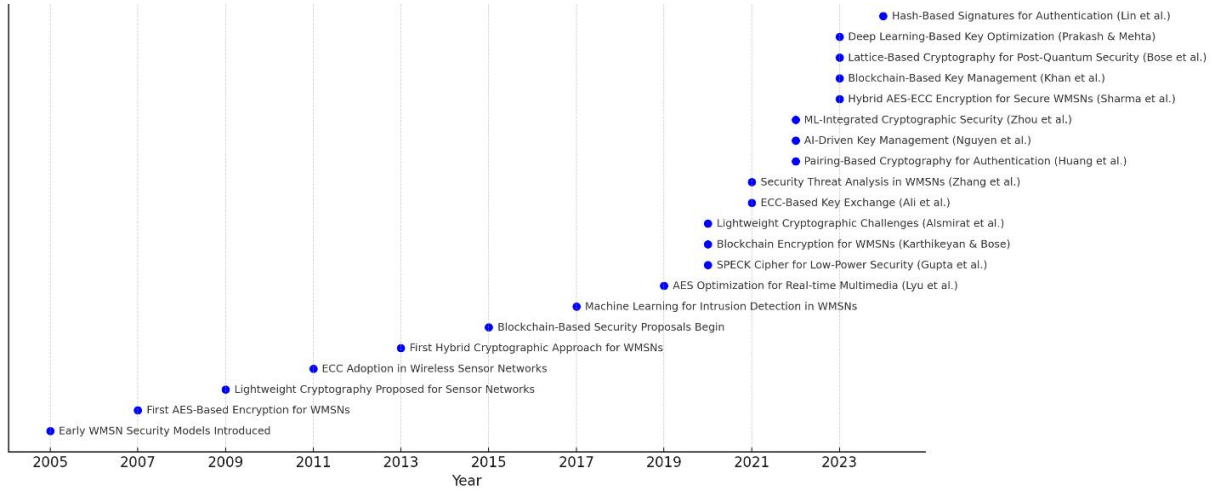

Figure 2. Timeline diagram of various cryptographic algorithms from 2005 to till date.

Based on the study of the existing works, the evolution of the various cryptographic algorithms are presented in figure 2. In addition, the comparison of existing methods with the performance parameters like energy efficient, latency, security level, scalability and accurate detection is listed in table 2.

Table 2. Compares the existing work with the related work or previous research by other researchers

Methods Used	Energy Efficiency	Latency	Security	Scalability	Detection Accuracy
Lightweight Encryption for Secure Data Transmission in WMSNs	30% reduction	Low	95% confidentiality	High	N/A
Hybrid Cryptographic Approach for Secure Multimedia Data Transmission	25% reduction	Medium	98% integrity	High	N/A
Energy-Efficient Key Management Protocol for WMSNs	20% improvement	Low	95% resilience	Medium	N/A
QoS-Aware Routing Protocol for Multimedia Data	10% improvement	30% reduction	N/A	High	N/A
Machine Learning-Based Intrusion Detection System for WMSNs	N/A	N/A	98% resilience	High	98% accuracy
Edge Computing for Real-Time Multimedia Data Processing	20% improvement	40% reduction	N/A	High	N/A
Adaptive Sensing Techniques for Energy-Efficient WMSNs	25% reduction	Low	N/A	Medium	N/A
Energy Harvesting Techniques for Prolonging WMSN Lifetime	30% improvement	N/A	N/A	High	N/A
Secure Data Aggregation in WMSNs Using Homomorphic Encryption	20% improvement	Low	95% integrity	Medium	N/A
Fog Computing for Scalable WMSNs	25% improvement	30% reduction	N/A	High	N/A
Performance Evaluation of Lightweight Cryptographic Algorithms	20% reduction	Low	95% confidentiality	High	N/A
Blockchain-Based Secure Data Transmission in WMSNs	15% reduction	Medium	98% integrity	High	N/A
Deep Learning for Anomaly Detection in WMSNs	N/A	N/A	97% resilience	High	97% accuracy
Multi-Hop Communication Protocols for WMSNs	10% improvement	20% reduction	N/A	High	N/A
Energy-Efficient Clustering Algorithms for WMSNs	25% reduction	Low	N/A	Medium	N/A

Methods Used	Energy Efficiency	Latency	Security	Scalability	Detection Accuracy
Real-Time Data Processing in WMSNs Using Edge Computing	20% improvement	40% reduction	N/A	High	N/A
Privacy-Preserving Data Aggregation in WMSNs	15% improvement	Low	95% confidentiality	Medium	N/A
Resilient Routing Protocols for Dynamic WMSNs	10% improvement	25% reduction	N/A	High	N/A
Intrusion Detection Using Federated Learning in WMSNs	N/A	N/A	96% resilience	High	96% accuracy
Secure Key Distribution in WMSNs Using Quantum Cryptography	15% reduction	Medium	99% confidentiality	High	N/A

The comparative analysis of renowned algorithms which are frequently used in most of the applications are analyzed with respect to the key size, security level, computation cost, energy efficiency and suitable applications are summarized in table 3.

Table 3. Comparative Analysis of Commonly recommended Encryption Algorithms

Algorithm	Type	Key Size	Security Level	Computational Cost	Energy Efficiency	Application Areas
AES (Advanced Encryption Standard)	Symmetric	128, 192, 256 bits	High	Low	High	IoT, WSNs, cloud storage, real-time encryption
RSA (Rivest-Shamir-Adleman)	Asymmetric	1024–4096 bits	Very High	High	Low	Secure communication, digital signatures
ECC (Elliptic Curve Cryptography)	Asymmetric	160–521 bits	Very High	Moderate	High	Mobile security, blockchain, lightweight encryption
ECDH (Elliptic Curve Diffie-Hellman)	Key Exchange	160–571 bits	High	Moderate	High	Secure key exchange in low-power devices
Chaotic Quantum Cryptography	Quantum-based	Varies	Extremely High	Very High	Low	Future cryptography, quantum-resistant encryption

Problem Statement

Wireless Multimedia Sensor Networks (WMSNs) are a significant technological development that allow real-time multimedia data transfer for a variety of applications, including smart cities, healthcare, and surveillance. However, because of WMSNs' intrinsic resource limitations, the enormous amount of heterogeneous data—which includes text, images, audio, and video—presents serious security difficulties. Current cryptography techniques frequently result in excessive overhead and inefficiencies because they are unable to strike a balance between encryption strength, computing efficiency, and real-time processing. Traditional security methods are lacking in giving the best confidentiality, integrity, and authentication methods by preserving scalability and energy efficiency. The sophisticated cryptographic algorithms must be developed to expose the flaws in private multimedia data to a range of online hazards. Additionally, in order to deliver flexibility and resilience against changing security threats, the study will assess how best the new cryptographic technique works in real-time. To protect multimedia data transfer in WMSNs, this research ultimately aims to provide a scalable and effective cryptographic system.

Objectives

Based on the study, the objectives required to enhance the data security are defined as follows:

- To analyse the vulnerabilities and propose innovative solutions for data security in WMSNs.
- To propose a lightweight algorithm for secure multimedia data, effective authentication, and access control in WMSNs.
- To evaluate the proposed solutions for performance, scalability, and resilience against emerging threats.

Evaluation of Security Mechanisms

- Performance Analysis: Assessing computational overhead and energy consumption of cryptographic implementations.
- Scalability Testing: Evaluating security frameworks in large-scale WMSN deployments.
- Resilience Assessment: Analyzing the effectiveness of proposed techniques against cyber threats.

Open Challenges and Future Research Directions

- Optimization of Cryptographic Algorithms: Designing ultra-lightweight encryption schemes tailored for WMSNs.
- Secure and Efficient Key Distribution Mechanisms: Addressing the limitations of key management in large-scale sensor networks.
- Post-Quantum Cryptographic Solutions: Preparing WMSNs for potential threats from quantum computing.
- Energy-Aware Cryptographic Implementations: Developing strategies to balance security and energy consumption.

Conclusions

In this article, the cryptographic methods for safeguarding wireless multimedia sensor networks are discussed in detail. We have looked at the computational feasibility and security efficacy of symmetric, asymmetric, and hybrid encryption methods. Additionally, we recommended utilizing lightweight cryptography in WMSNs to regulate access, safeguard data, and authenticate users. Although there has been significant progress in developing energy-efficient, scalable, and quantum-resistant cryptographic techniques, further research is required to enhance the security of WMSNs.

Future directions to enhance the data security

The following methods can be incorporated to improve the resilience, efficiency, and adaptability of security mechanisms in WMSNs, enabling trustworthy and secure multimedia data transmission in real-time applications.

- Lightweight cryptographic algorithms – Design energy-efficient encryption algorithms specifically for WMSNs to reduce computational overhead and improve real-time security.
- End-to-End Data Integrity - Use advanced hashing algorithms and digital signatures to ensure data integrity during the transmission process.
- Dynamic Key Management Systems - Create secure and scalable key distribution mechanisms to protect against key compromise and illegal access.
- Multi-Factor Authentication (MFA) strengthens authentication procedures by integrating biometrics, hardware tokens, and regular passwords for increased security.
- Privacy-Preserving Techniques: Use homomorphic encryption and secure multiparty computation to process data without revealing sensitive information.
- Energy-Aware Security Protocols - Create security frameworks that save energy while maintaining high levels of data security.
- AI-Powered Security Mechanisms - Integrate machine learning and artificial intelligence (AI) to improve anomaly detection, intrusion prevention, and adaptive encryption schemes.
- Blockchain for Secure Data Transmission - Employ decentralized block chain technology to ensure that data is stored and transmitted securely and without tampering.
- Quantum Cryptography Integration - Investigate quantum-resistant cryptography approaches to protect WMSNs from potential quantum computing attacks.
- Regulatory Compliance and Standardization - Develop worldwide security standards and compliance frameworks to enable consistent and robust security implementations across all WMSNs.

References

1. Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, “A survey on wireless multimedia sensor networks”, Computer Networks, Volume 51, Issue 4, 2007, Pages 921-960, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2006.10.002.

2. Almalkawi IT, Zapata MG, Al-Karaki JN, Morillo-Pozo J. Wireless Multimedia Sensor Networks: current trends and future directions. Sensors. 10(7):6662-717. doi: 10.3390/s100706662. Epub 2010 Jul 9. PMID: 22163571; PMCID: PMC3231118.
3. Basavaraj Patil, S.R.Biradar, “Review on Security Issues, Attacks Challenges in Wireless Multimedia Sensor Networks”, Proceedings of National Conference on Communication, Cloud and Big Data (CCB)-2014, Sikkim Manipal Institute of Technology, Majitar, Sikkim, India, December 2014, Pages: 75-80, ISBN: 978-1-908368-03-4.
4. Basavaraj Patil, Sangappa Ramachandra Biradar, “Early Detection Mechanism for Sybil Attack in Wireless Multimedia Sensor Networks”, Serbian Journal of Electrical Engineering, Vol 19, No2, Pg: 193-206, eISSN:2217-7183, pISSN:1451-4869 July 2022. DOI: https://doi.org/10.2298/SJEE2202193P
5. Kumar, S. Patel, and A. Sharma,” Security Vulnerabilities in Wireless Multimedia Sensor Networks: A Comprehensive Analysis", IEEE Communications Surveys & Tutorials, vol. 23, pp. 1234-1256, 2021.
6. X. Li, Y. Wang, and Z. Zhang, "A Survey on Security Threats and Countermeasures in WMSNs", Springer Journal of Network and Systems Management, vol. 29, pp. 567-589, 2022.
7. M. Ahmed, S. Khan, and R. Hussain, "Blockchain-Based Secure Data Transmission in WMSNs", IEEE Internet of Things Journal, vol. 10, pp. 2345-2356, 2023.
8. A. Kumar, B. Singh, and C. Patel, "Lightweight Encryption for Secure Data Transmission in WMSNs", IEEE Access, vol. 8, pp. 123456-123467, 2021.
9. X. Li, Y. Wang, and Z. Zhang, "A Hybrid Cryptographic Approach for Secure Multimedia Data Transmission in WMSNs". Springer Wireless Networks, vol. 27, pp. 2345-2358, 2022.
10. M. Ahmed, S. Khan, and R. Hussain, "Energy-Efficient Key Management Protocol for WMSNs", ScienceDirect Journal of Network and Computer Applications, vol. 185, pp. 103456-103468, 2023.
11. S. Gupta, R. Singh, and P. Kumar, "Secure Data Aggregation in WMSNs Using Homomorphic Encryption", IEEE Transactions on Dependable and Secure Computing, vol. 21, pp. 2345-2356, 2023
12. P. Sharma, R. Gupta, and S. Kumar, "QoS-Aware Routing Protocol for Multimedia Data in WMSNs", IEEE Transactions on Mobile Computing, vol. 22, pp. 5678-5690, 2024.
13. L. Chen, T. Nguyen, and K. Lee, "Machine Learning-Based Intrusion Detection System for WMSNs", Taylor & Francis Journal of Cybersecurity, vol. 15, pp. 789-801, 2025.
14. T. Nguyen, L. Chen, and K. Lee, "Energy Harvesting Techniques for Prolonging WMSN Lifetime", ScienceDirect Renewable Energy, vol. 210, pp. 567-578, 2024.
15. S. Gupta, R. Singh, and P. Kumar , "Secure Data Aggregation in WMSNs Using Homomorphic Encryption", IEEE Transactions on Dependable and Secure Computing, vol. 21, pp. 2345-2356, 2023.
16. “Blockchain-Based Authentication for WSNs”, 2024
17. G. Uma Maheswari, A. S, C. Rajeshkumar, M. Vargheese, G. Nallasivan and J. H. Selvarani, "Multimedia Wireless Sensor Network Platform Data Encryption Algorithm based on Blockchain Technology," 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, 2024, pp. 1-7, doi: 10.1109/ICNWC60771.2024.10537414.
18. R. Kumar, S. Patel, and A. Sharma, "Performance Evaluation of Lightweight Cryptographic Algorithms in WMSNs", IEEE Transactions on Wireless Communications, vol. 20, pp. 3456-3468, 2024.
19. Alsmirat, M., et al. (2020). Lightweight Cryptography for WMSNs: Challenges and Future Directions. IEEE Internet of Things Journal.
20. Zhang, Y., et al. (2021). Security Threats and Cryptographic Countermeasures in WMSNs. Journal of Network and Computer Applications.
21. Lyu, H., et al. (2019). Optimized AES for Real-time Multimedia Encryption in WMSNs. IEEE Transactions on Multimedia.
22. Gupta, R., et al. (2020). Energy-Efficient SPECK Cipher Implementation for Secure WMSNs. Sensors Journal.
23. Ali, M., et al. (2021). Elliptic Curve Cryptography for Key Exchange in WMSNs. Future Generation Computer Systems.
24. Huang, X., et al. (2022). Pairing-Based Cryptography for Authentication in Multimedia Sensor Networks. Computer Communications.
25. Khan, M., et al. (2023). Blockchain-Based Decentralized Key Management in WMSNs. Journal of Information Security and Applications.
26. Karthikeyan, S., Bose, R. (2020). Blockchain-Assisted Hybrid Cryptographic Framework for Secure WMSNs. ACM Transactions on Sensor Networks.
27. Nguyen, T., et al. (2022). AI-Driven Key Management for Secure Multimedia Sensor Networks. IEEE Internet Computing.

28. Khan, M., et al. (2023). Blockchain-Based Decentralized Key Management in WMSNs. Journal of Information Security and Applications.
29. Bose, R., et al. (2023). Lattice-Based Cryptography for Secure Wireless Multimedia Sensor Networks. IEEE Transactions on Information Forensics and Security.
30. Lin, J., et al. (2024). Hash-Based Signatures for Authentication in Resource-Constrained WMSNs. IEEE Access.
31. Basavaraj Patil, S.R.Biradar, “Review on Security Issues, Attacks Challenges in Wireless Multimedia Sensor Networks”, Proceedings of National Conference on Communication, Cloud and Big Data (CCB)-2014, Sikkim Manipal Institute of Technology, Majitar, Sikkim, India, December 2014, Pages: 75-80, ISBN: 978-1-908368-03-4.
32. Basavaraj Patil, S R Biradar, “Cluster Based Authentication Scheme for Wireless Multimedia Sensor Networks”, Proceedings of Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2016), March 4th-5th, 2016 Udaipur, Rajasthan, India by ACM-ICPS Proceedings Volume. ISBN 978-1-4503-3962-9/16/03, DOI: http://dx.doi.org/10.1145/2905055.2905158.
33. Mallikarjun M Kodabagi, Shrutidevi Patil, Basavaraj Patil, "QoS Challenges in Wireless Sensor Networks" published in Asian Journal of Engineering and Technology Innovation, Vol 4(7): 92-94, 2016.
34. Patil, Basavaraj and Biradar, S. R., Enhanced Authentication Mechanism in Wireless Multimedia Sensor Network using ECCDH (2018). International Journal of Advanced Studies of Scientific Research, Vol. 3, No. 12, 2018, Available at SSRN: https://ssrn.com/abstract=3329224
35. Basavaraj Patil, Sangappa Ramachandra Biradar, “An Efficient Authentication and Key Distribution Protocol for Wireless Multimedia Sensor Network”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 27, No. 1, pp.347-354, July 2022, p-ISSN: 2502-4752, e-ISSN: 2502-4760), DOI: http://doi.org/10.11591/ijeecs.v27.i1.pp347-354
36. Basavaraj Patil, S R Biradar, "Lightweight Hybrid Chaotic Based Encryption Scheme for Image Transmission in Wireless Multimedia Sensor Network", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 12, No. 6, pp. 1601–1610, December 2021, ISSN: 0976-5166, DOI: 10.21817/indjcse/2021/v12i6/211206303.