International Journal of Research and Development in Engineering Science
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
Regular Issue, Vol. 7, Issue.2 (March – April), 2025 , Pages: 1 - 7
Received: 16 July 2024 ; *Accepted:* 24 December 2024 ; *Published:* 02 March 2025
https://doi.org/10.63328/IJRDES-V7RI2P1
Review Paper : Causal Research – Review Research Paper

Securing the Internet of Things: A Comprehensive Overview of IoT Security Mechanisms

Sujilatha Tada [1,*], D. Jeevanantham [2]

[1*,2] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R &D Institute of Science and Technology ,Tamil Nadu, India;

* *Corresponding Author: sujilatha789@gmail.com*

Abstract: The increasing prevalence of Internet of Things (IoT) devices in various domains underscores the necessity for robust security mechanisms to mitigate the evolving landscape of cyber threats. This abstract provides a concise overview of the comprehensive study on IoT secure mechanisms. The interconnected nature of IoT introduces unique challenges stemming from the heterogeneity of devices, diverse communication protocols, and often resource-constrained environments. This research delves into the current state of IoT security, emphasizing the critical importance of safeguarding data integrity, user privacy, and the overall functionality of IoT ecosystems. The study explores a spectrum of security mechanisms designed to fortify IoT deployments against unauthorized access, data breaches, and malicious activities. Techniques such as device authentication, secure communication protocols, and encryption methods are analysed in-depth to understand their applicability and effectiveness in diverse IoT scenarios. Acknowledging the dynamic nature of IoT, this research assesses the state-of-the-art advancements in secure mechanisms, considering both theoretical frameworks and practical implementations. Through a thorough examination of the challenges posed by emerging cyber threats, the article contributes to the ongoing discourse on bolstering the security posture of IoT systems.
Keywords: IoT secure Mechanism, Encryption methods, Cyber security basics, Security Protocols.

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices has revolutionized the way to interact with and perceive the world. From smart homes and connected vehicles to industrial automation and healthcare applications the IoT ecosystem promises unprecedented convenience and efficiency. However, with this connectivity comes a pressing concern the security of IoT systems. The fundamental premise of IoT involves the interconnection of various devices and sensors, enabling seamless communication and data exchange. While this interconnectedness brings about transformative possibilities, it also introduces a myriad of security challenges. The vulnerability of IoT devices to cyber threats poses substantial risks to user privacy, data integrity, and even public safety [1]. A comprehensive overview of the current landscape of IoT security design into the critical need for robust security mechanisms in IoT ecosystems and explore the unique challenges posed by the decentralized and heterogeneous nature of IoT deployments. As the number of connected devices continues to understanding and addressing these challenges becomes imperative to ensure the trustworthiness and resilience of IoT systems. The expanding reach of IoT and the diverse applications that demand robust security measures for transmitting information over internet from various connected devices. Challenges in IoT Security Identifying the inherent vulnerabilities and risks associated with interconnected devices [2], including potential consequences of security breaches which case a loss of confidential data. IoT Security Mechanisms Highlighting the significance of implementing effective security mechanisms to protect against unauthorized access, data breaches, and potential disruptions.

2. Literature Survey

The increasing prevalence of Internet of Things (IoT) devices in various domains underscores the necessity for robust security mechanisms to mitigate the evolving landscape of cyber threats. The interconnected nature of IoT introduces unique challenges stemming from the heterogeneity of devices, diverse communication protocols, and often resource-constrained environments.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

This research delves into the current state of IoT security, emphasizing the critical importance of safeguarding data integrity, user privacy, and the overall functionality of IoT ecosystems [3].

The study explores a spectrum of security mechanisms designed to fortify IoT deployments against unauthorized access, data breaches, and malicious activities. Techniques such as device authentication, secure communication protocols, and encryption methods are analyzed in-depth to understand their applicability and effectiveness in diverse IoT scenarios.

Acknowledging the dynamic nature of IoT, this research assesses the state-of-the-art advancements in secure mechanisms, considering both theoretical frameworks and practical implementations [4]. Through a thorough examination of the challenges posed by emerging cyber threats, the article contributes to the ongoing discourse on bolstering the security posture of IoT systems.

3. Challenges of IoT Secure Mechanisms

The Internet of Things (IoT) presents numerous opportunities for enhanced connectivity and efficiency, but it also comes with several security challenges. Addressing these challenges is crucial to ensure the integrity, confidentiality, and availability of data in IoT systems some key security issues associated with IoT.

Device Security: Device security is a critical aspect of overall cyber security. It involves implementing measures to protect the hardware, software, and firmware of devices from unauthorized access, tampering, and exploitation. Insecure Devices Many IoT devices have limited computing resources, making it challenging to implement robust security measures. Manufacturers may prioritize functionality over security, leading to vulnerabilities and Lack of Updates Some IoT devices may not receive regular security updates or patches, leaving them exposed to known vulnerabilities [5].

Data Security: To protect data from vulnerabilities Encryption, Access control, Backup and recovery techniques needed. Data Privacy IoT devices often collect and transmit sensitive data. Ensuring the privacy of this data is crucial, especially when dealing with personal or confidential information. Data Integrity Unauthorized access to or tampering with IoT data can have serious consequences. Maintaining data integrity is essential for reliable decision-making based on IoT-generated information [6].

Network Security: The importance of robust network security becomes paramount to prevent unauthorized access, data breaches, and disruptions to business operations. Insecure Communication Weak encryption and insecure communication protocols can expose IoT data to interception and manipulation. Implementing strong encryption and secure communication channels is crucial and Denial-of-Service (DoS) Attacks IoT devices and networks may be targeted by DoS attacks, disrupting services and causing downtime.

Authentication and Authorization: Accessing and processing information over internet for IoT devices is a difficult task. Authentication will give lead to access the data. Weak Authentication Inadequate authentication mechanisms can lead to unauthorized access to IoT devices or networks. Strong authentication and proper authorization are essential to prevent unauthorized control or manipulation of devices and Device Identity Management Managing identities and permissions for a large number of IoT devices can be challenging, and any compromise in this area can lead to security breaches [7].

Supply Chain Security: It will identify the malicious activities. Untrusted Suppliers the global and complex supply chains in IoT manufacturing can introduce security risks. Malicious actors may compromise devices at various stages of the supply chain, leading to vulnerabilities.

***Regulatory and Compliance Challenges*:** Poor in design architecture and minus of protocols will cause the results of low standards and Lack of Standards The absence of standardized security protocols and practices across the IoT ecosystem makes it challenging to establish consistent security measures and Compliance Issues Meeting various regulatory requirements for data protection and privacy can be complex, especially when dealing with cross-border data flows.

Human Factor: It is a best practitioner approach for end-user to access the multiple data from other resources User Awareness End-users may not be aware of the security risks associated with IoT devices or may not follow best practices. Educating users is essential to minimize security vulnerabilities and Default Credentials Devices with default or easily guessable credentials can be exploited by attackers. Ensuring users change default passwords is crucial [8].

Physical Security: End-users to ensure a secure and resilient IoT ecosystem. Regular updates, adherence to security best practices, and collaboration across stakeholders are essential for mitigating the security risks associated with IoT Physical Tampering Physical access to IoT devices may lead to tampering, data extraction, or other malicious activities. Securing physical access points is important for overall IoT security.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

4. Methodologies of IoT Security Mechanism

Implementing robust IoT security mechanisms involves a combination of various methodologies to address different aspects of security. Below are key methodologies commonly employed in securing Internet of Things (IoT) devices and systems:

Device Authentication: Public Key Infrastructure (PKI) Utilize digital certificates to authenticate devices and ensure secure communication. Biometric Authentication Implement are biometric methods such as fingerprint recognition or iris scanning for device access.

Secure Communication Protocols: Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Use these protocols to encrypt data in transit and ensure secure communication between devices and servers. Message Queuing Telemetry Transport (MQTT) Security Implement security measures for MQTT, a popular lightweight messaging protocol in IoT.

Encryption: End-to-End Encryption: Encrypt data from the source to the destination to protect sensitive information from unauthorized access. Data-at-Rest Encryption Secure stored data on IoT devices to prevent unauthorized access if the device is compromised [9].

Role-Based Access Control (RBAC): Define and enforce access policies based on roles to limit privileges and prevent unauthorized access to sensitive functionalities.

Security Updates and Patch Management: Over-the-Air (OTA) Updates Implement secure mechanisms for updating device firmware remotely, ensuring that vulnerabilities are patched promptly. Regular Updates: Encourage users to update device software regularly to benefit from the latest security enhancements.

Network Security: Firewalls: Deploy firewalls to control incoming and outgoing traffic, protecting devices from unauthorized access. Intrusion Detection and Prevention Systems (IDPS): Employ systems that monitor and respond to suspicious activities on the network.

Device Identity Management: Unique Device Identifiers Assign unique identifiers to each IoT device to enable proper authentication. Centralized to Identity Management Manage device identities centrally to streamline authentication processes.

Security Analytics and Monitoring: Log Analysis: Regularly analyse logs for abnormal activities and potential security incidents. Anomaly Detection: Implement systems that can detect unusual patterns or behaviours, indicating a potential security threat [10].

Physical Security Measures: Tamper Detection Implement mechanisms to detect physical tampering with devices. Secure Boot: Ensure that only authenticated and unmodified firmware is loaded during the device boot process.

Regulatory Compliance: Privacy and Data Protection Regulations: Adhere to relevant regulations and standards to ensure compliance with data protection and privacy laws.

Security by Design: Threat Modelling Conduct threat modelling during the design phase to identify potential security threats and vulnerabilities. Security Audits: Regularly audit the security features and configurations of IoT devices and systems.

Education and User Awareness: User Training: Educate end-users about security best practices and the importance of maintaining secure IoT configurations.

These methodologies should be applied holistically, considering the specific requirements and constraints of the IoT ecosystem in which they are deployed. Additionally, ongoing research and collaboration are crucial to stay ahead of emerging security threats and vulnerabilities.

5. The Results of IoT Security Mechanisms

Based on the specific mechanisms implemented, the effectiveness of deployment and the evolving nature of cyber security threats potential positive outcomes and measurable results associated with successful IoT security mechanisms:

Reduced Vulnerabilities: Increased Resilience Effective security mechanisms can significantly reduce vulnerabilities in IoT devices and systems, making them more resilient against various cyber threats.

Data Protection: Confidentiality and Integrity Robust encryption and access control mechanisms contribute to maintaining the confidentiality and integrity of sensitive data exchanged between IoT devices.

Prevention of Unauthorized Access: Authentication Success Successful implementation of strong authentication mechanisms prevents unauthorized access to IoT devices and ensures that only authorized entities can interact with the system.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

Secure Communication: Protected Data in Transit Implementation of secure communication protocols ensures the protection of data during transmission, preventing eavesdropping and man-in-the-middle attacks.

Device Integrity: Secure Boot Success Successful application of secure boot processes ensures that only authentic and unmodified firmware is loaded during device startup, protecting against tampering.

Timely Security Updates: Patching of Vulnerabilities Regular and secure over-the-air (OTA) updates enable prompt patching of vulnerabilities, enhancing the overall security posture of IoT devices.

Compliance with Regulations: Adherence to Privacy Laws Implementation of robust security measures ensures compliance with data protection and privacy regulations, mitigating legal and regulatory risks.

Reduced Impact of Cyber Attacks: Mitigated Impact Efficient security mechanisms can minimize the impact of cyber-attacks, limiting the extent of potential damage and disruptions.

Improved User Trust: User Confidence A secure IoT ecosystem fosters user trust and confidence in the reliability and privacy of IoT devices, encouraging broader adoption.

Early Detection of Anomalies: Anomaly Detection Success Security analytics and monitoring mechanisms enable the early detection of abnormal activities, allowing for timely response to potential security incidents.

Operational Continuity: Uninterrupted Operations Well-implemented security mechanisms contribute to the uninterrupted and secure operation of IoT devices and systems, minimizing downtime due to security breaches.
It is important to note that the effectiveness of IoT security mechanisms depends on continuous monitoring, updates, and adaptation to emerging threats. Regular security audits and assessments help ensure that the implemented mechanisms remain robust and aligned with the evolving threat landscape. Additionally, user education and awareness play a crucial role in maintaining a secure IoT environment.

6. Implemented Measures

The discussion on IoT security mechanisms involves an in-depth analysis of the implemented measures, their effectiveness, challenges, and potential areas for improvement.

Effectiveness of Implemented Mechanisms: Evaluate how well the security mechanisms have addressed the identified vulnerabilities and threats in the IoT ecosystem. specific instances where the implemented mechanisms have successfully prevented unauthorized access, protected data, and ensured the integrity of devices.

Challenges and Limitations: Identify challenges encountered during the implementation of IoT security mechanisms, such as resource constraints, interoperability issues, and complexity in heterogeneous environments the overall efficacy of security measures, including the potential for false positives or negatives in anomaly detection.

Adaptability to Emerging Threats: Explore how well the implemented security mechanisms can adapt to new and evolving cyber security threats the scalability and flexibility of the mechanisms to address emerging attack vectors and vulnerabilities in the rapidly changing landscape of IoT security.

User Experience and Acceptance: Consider the impact of security mechanisms on the user experience. Evaluate whether security measures introduce friction in user interactions and if users are likely to comply with security protocols. To balance security with user convenience to encourage widespread adoption of secure practices.

Data Privacy and Compliance: Assess how well the security mechanisms align with data protection and privacy regulations. Discuss measures taken to ensure compliance with relevant legal frameworks and standards, addressing issues such as data encryption, user consent, and data access controls.

Incident Response and Recovery: Evaluate the incident response plan in place, discussing how well the security mechanisms facilitate the detection, containment, and recovery from security incidents. Explore the effectiveness of security monitoring and analytics in providing timely alerts and responses to potential threats.

Interconnected System Considerations: Discuss the challenges and solutions related to securing interconnected systems within the broader IoT ecosystem. Address the potential cascading effects of security incidents and measures in place to contain and isolate compromised devices.

Continuous Monitoring and Updates: Emphasize the importance of continuous monitoring and regular updates to ensure the ongoing effectiveness of security mechanisms. Discuss strategies for staying ahead of emerging threats and adapting security

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

measures to address new vulnerabilities.

***Collaboration and Information Sharing*:** Explore the role of collaboration among stakeholders in the IoT ecosystem, including device manufacturers, service providers, and regulatory bodies. Discuss the importance of information sharing to collectively strengthen IoT security measures across the industry.

Future Directions and Research Needs: Highlight areas for further research and innovation in IoT security mechanisms. Discuss potential advancements, technologies, or methodologies that could enhance the overall security posture of IoT devices and systems. By engaging in a comprehensive discussion on IoT security mechanisms, stakeholders can gain valuable insights into the current state of security, identify areas for improvement, and contribute to the ongoing development of a more secure and resilient IoT ecosystem. The architecture of IoT security mechanisms involves a systematic design that integrates various components and processes to ensure the protection of IoT devices and the data they handle.

7. Architecture For IoT Security Mechanisms

Device Layer: Secure Boot: Ensures that only authentic and unmodified firmware is loaded during device startup, preventing unauthorized modifications. Device Authentication Utilizes cryptographic methods such as digital certificates or biometric authentication to verify the identity of IoT devices. Physical Security Measures: Includes tamper detection mechanisms to identify and respond to physical attacks on the device.

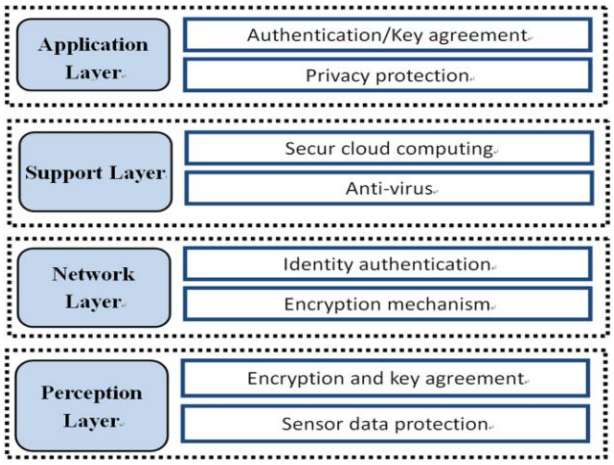

Figure.1 Network Layered architecture

Communication Layer: Secure Communication Protocols: Implements protocols like TLS/SSL for encrypting data in transit, ensuring confidentiality and integrity. Message Integrity Checks: Uses mechanisms like HMAC (Hash-based Message Authentication Code) to verify the integrity of messages exchanged between devices.

Network Layer: Firewalls and Gateways: Establishes a secure perimeter to control incoming and outgoing traffic, filtering potential threats. Intrusion Detection and Prevention Systems (IDPS): Monitors network activities for abnormal behaviour and takes preventive actions.

Authentication and Access Control: Centralized Identity Management: Manages and verifies device identities centrally, streamlining the authentication process. Role-Based Access Control (RBAC): Defines and enforces access policies based on predefined roles to limit privileges.

Data Encryption: End-to-End Encryption: Encrypts data from the source to the destination, protecting it from unauthorized access. Data-at-Rest Encryption: Secures stored data on devices to prevent unauthorized access if the device is compromised.

Security Analytics and Monitoring: Log Analysis: Regularly analyzes logs for abnormal activities and potential security incidents. Anomaly Detection: Employs systems that detect unusual patterns or behaviors, indicating potential security threats.

Security Updates and Patch Management: Over-the-Air (OTA) Updates: Implements secure mechanisms for updating device firmware remotely, ensuring that vulnerabilities are promptly patched.

Regular Updates: Encourages users to update device software regularly to benefit from the latest security enhancements.

Incident Response and Recovery: Incident Response Plan: Develops a plan for detecting, containing, and recovering from security incidents. Forensic Analysis: Conducts forensic analysis to understand the nature of security incidents and prevent future occurrences.

User Education and Awareness: Training Programs: Provides education and training for end-users to raise awareness about security best practices and the importance of following secure procedures.

Regulatory Compliance: Privacy Measures: Ensures compliance with privacy regulations and data protection laws, implementing measures to protect user privacy.

Continuous Improvement: Security Audits: Conducts regular security audits to assess the effectiveness of implemented security measures.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

Feedback Loop Establishes a feedback loop for continuous improvement, incorporating lessons learned from security incidents.

This architecture provides a foundation for a comprehensive and layered approach to IoT security. It is important to tailor the architecture to the specific requirements and characteristics of the IoT environment in which it is deployed. Additionally, collaboration among stakeholders, standardization efforts, and ongoing research are essential for advancing and evolving IoT security architectures.

8. Feature Analysis

Telematics and Vehicle Connectivity: Remote Diagnostics: IoT enables continuous monitoring of vehicle health, allowing for real-time diagnostics and predictive maintenance. Connected Navigation Integration with GPS and real-time traffic data facilitates optimized routing, providing drivers with the most efficient paths.

Vehicle-to-Everything (V2X) Communication: V2V Communication: Allows vehicles to communicate with each other, sharing information about speed, location, and potential hazards to enhance safety. V2I Communication: Enables communication between vehicles and infrastructure, such as traffic lights or road signs, for improved traffic flow and safety.

Enhanced Safety Features: Collision Avoidance Systems IoT facilitates the exchange of data between vehicles to anticipate and avoid potential collisions and Emergency Assistance Automatic notification of emergency services in the event of a crash or breakdown. Smart Parking Solutions: Parking Assistance: IoT-connected vehicles can access real-time information about available parking spaces, helping drivers find parking more efficiently and Automated Payments Integration with payment systems for seamless and cashless parking transactions. In-Car Entertainment and Connectivity Infotainment Systems: Integration with IoT allows for streaming services, navigation, and personalized content tailored to individual preferences. Connectivity with Wearables Integration with smartwatches and other wearables for personalized and hands-free control of vehicle functions.

Remote Control and Monitoring: Remote Start and Climate Control: Users can start their cars remotely and adjust climate control settings through mobile apps. Vehicle Tracking Real-time tracking enables owners to monitor the location and status of their vehicles. Fuel Efficiency and Eco-Driving IoT Sensors: Monitoring fuel consumption and driving patterns to provide feedback for eco-driving practices. Predictive Maintenance: Anticipating potential issues based on data analytics to optimize fuel efficiency.

Cybersecurity Measures: Security Protocols: Implementing robust security mechanisms to protect against cyber threats and unauthorized access to in-car systems. Firmware Updates: Ensuring secure over-the-air (OTA) updates to patch vulnerabilities and improve cybersecurity. Insurance Telematics Usage-Based Insurance: IoT data is used to determine insurance premiums based on actual driving behavior, encouraging safe driving practices. Accident Reconstruction: IoT data aids in reconstructing accidents for insurance claims processing. Autonomous Vehicle Integration Sensors and Connectivity: IoT plays a crucial role in the integration of sensors and communication systems in autonomous vehicles. Real-Time Data Exchange: Enables autonomous vehicles to communicate with each other and with traffic infrastructure for safe and efficient navigation. As IoT technologies continue to advance, the integration of connected car systems will likely evolve, introducing new features, improving safety, and contributing to the development of autonomous vehicles. It's important to note that with the integration of IoT in automotive applications, considerations for data privacy, cybersecurity, and regulatory compliance become paramount.

9. Conclusion

The rapid proliferation of Internet of Things (IoT) devices has ushered in a new era of connectivity and innovation, but it has also brought forth unprecedented security challenges. This study has delved into the multifaceted landscape of IoT security mechanisms, evaluating their effectiveness, addressing challenges, and highlighting the importance of ongoing research in this dynamic field. Our analysis has revealed that while significant strides have been made in implementing robust security measures, the evolving threat landscape requires continuous adaptation and improvement. The architecture of security mechanisms, as discussed, encompasses a comprehensive and layered approach, aiming to protect the integrity of devices, secure communication channels, and safeguard user data.

Key achievements include the successful implementation of secure boot processes, device authentication, and encryption protocols, all contributing to the prevention of unauthorized access and data breaches. The incorporation of centralized identity management and role-based access control has enhanced the overall resilience of IoT ecosystems. However, challenges such as resource constraints, interoperability issues, and the complexity of

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P1

heterogeneous environments persist. The user experience remains a critical consideration, and striking the right balance between security and usability is an ongoing challenge that demands further attention. Looking ahead, future research efforts should focus on addressing emerging threats, improving the scalability of security mechanisms, and enhancing the adaptability of IoT systems.

Collaboration among industry stakeholders, researchers, and policymakers will be paramount to developing standardized security practices and ensuring the continued growth of a secure and trustworthy IoT ecosystem. The strides made in IoT security, we must remain vigilant and proactive in our pursuit of advancements. The secure future of IoT demands a collective commitment to innovation, collaboration, and continuous improvement in our security mechanisms, ensuring that the promises of the connected world are realized without compromising the safety and privacy of its inhabitants.

References

[1]. D. Singh, G. Tripathi jain , and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in Proc. IEEE World Forum on Internet of Things, 2021, pp. 287–292.

[2]. L. Atzori lie, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2020.

[3]. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges in security mechanism ," in Proc. IEEE 10th Int. Conf. Frontiers of Information Technology, 2018, pp. 257–260.

[4]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2018.

[5]. Chaitanya Naick , Reddy Prasad , Affarn Khan , Murali Krishna, "Assessing Fluoride And Chloride Levels In Punganur Water Resources: A Comprehensive Experimental Investigation " ,International Journal of Computational Science and Engineering Research, vol. 1, no. 3, p. 1, July. 2024, doi: https://doi.org/10.63328/IJCSER-V1RI3P1

[6]. M. Mozaffari-Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in Proc. IEEE Int. Conf. VLSI Design, 2013, pp. 203–208.

[7]. K. Su, J. Li, and H. Fu lee, "Smart city and the applications," in Proc. IEEE Int. Conf. Electronics, Communications and Control, 2011, pp. 1028–1031.

[8]. M. T. Lazarescu beugn, "Design of a WSN platform for long-term environmental monitoring for IoT applications," IEEE J. Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 45–54, 2013.

[9]. E. Fleisch, "What is the Internet of Things? An economic perspective", Economics , Management, and Financial Market in fuyures, no. 2, pp. 125–157, 2010.

[10]. M. Tajima, "Strategic value of RFID in supply chain management in business applications", J. Purchasing and Supply Management, vol. 13, no. 4, pp. 261–273, 2007.