International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 71-76
Published Online December 2024 in IJEAST (http://www.ijeast.com)

WIRELESS DATA ENCRYPTION AND DECRYPTION USING IOT

Mr. R.Palani Kumar Assistant Professor,
Department of Information Technology,
Kongunadu College of Engineering and Technology Trichy,
Tamil Nadu, India.

M. Sivanesan Student,
Department of Information Technology,
Kongunadu College of Engineering and Technology Trichy,
Tamil Nadu, India.

P. Praveen Student,
Department of Information Technology,
Kongunadu College of Engineering and Technology Trichy,
Tamil Nadu, India.

S. Vishal Student,
Department of Information Technology,
Kongunadu College of Engineering and Technology Trichy,
Tamil Nadu, India.

Abstract – **Secure exchange of data is critical in IoT-based applications, especially for resource-limited devices such as the Arduino Uno. The project creates a secure data transmission system through serial communication via TX and RX lines, incorporating an XOR-based encryption scheme lightweight enough for efficient data protection. AES decryption is employed to enhance security during data reception to preserve both confidentiality and integrity. In addition, the ESP8266 Wi-Fi module supports encrypted data delivery to cloud services, providing real-time monitoring and remote visualization. This approach allows for secure communication even over public networks, providing a cost-effective and scalable solution for IoT applications like industrial automation, sensor networks, and smart environments at low computational overhead**

Keywords — **IoT Security, Secure Data Transmission, XOR-Based Encryption, AES Decryption, ESP8266 Wi-Fi Module, Real-Time Data Monitoring, Encrypted Cloud Communication, Serial Communication (TX/RX),Lightweight Cryptography, Smart Environment Monitoring Introduction**

I.INTRODUCTION

Internet of Things (IoT) has transformed many industries by facilitating the smooth communication of devices. Yet, as wireless data transmission expands in IoT networks, security is a major concern. Unauthorised access, data leakage, and cyberattacks are all grave threats to confidential data. This project aims to secure data through encryption and decryption algorithms for IoT communication. Encryption guarantees that the data being transmitted is transformed into an unreadable state to block unauthorized interception, while decryption permits the intended users to access the original data safely. Due to the limited resources of IoT devices, lightweight cryptography algorithms are utilized to ensure efficiency without sacrificing security. Secure key management techniques are also incorporated to further safeguard data integrity. This project is adaptable across different sectors, such as healthcare, smart cities, industrial automation, and remote monitoring, where secure data sharing is an absolute necessity. Using a reliable encryption framework, this project attempts to make IoT communication more robust in the fight against cyberattacks, providing confidentiality, reliability, and trust within wireless networks.

II. PROPOSED ALGORITHM

The work to be proposed will extend the current literature by creating a real-world, secure communication system for IoT based on symmetric and asymmetric encryption techniques. The system will consist of real-time data exchange through two microcontrollers that communicate wirelessly with two Android apps. The encryption methods selected will ensure

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 71-76
Published Online December 2024 in IJEAST (http://www.ijeast.com)

low latency and optimal resource utilization while ensuring strong security. The work proposed focuses on the design of a secure and strong wireless communication system specific to Internet of Things (IoT) applications, utilizing two microcontrollers in conjunction with two Android apps to enable data reception and transmission. The architecture consists of setting one microcontroller to act as a data sender (client) and the other as a receiver (server).

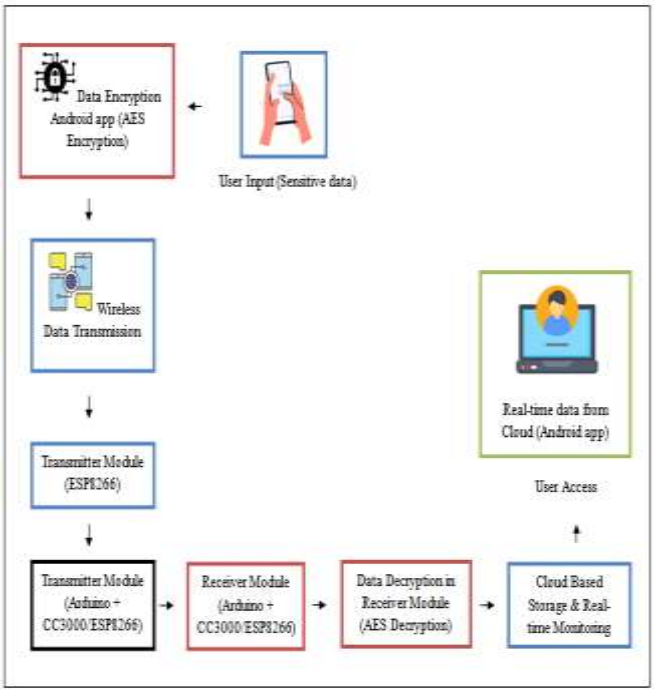

Fig.1. Proposed Architecture System

The Android apps are created with intuitive interfaces through which users can enter sensitive data to be encrypted, sending this information securely to the server microcontroller. On the receiving end, an ESP8266 and CC3000-based receiver module collects the transmitted data. To ensure data integrity, the receiver module decrypts the information using AES decryption.

After decryption, the data is sent to a cloud-based storage system, where it is securely stored and made accessible for real-time monitoring. Users can retrieve and view the processed data through the Android application, ensuring secure access and remote monitoring capabilities. This system enhances data security by integrating advanced encryption techniques while enabling seamless wireless transmission and cloud-based accessibility.

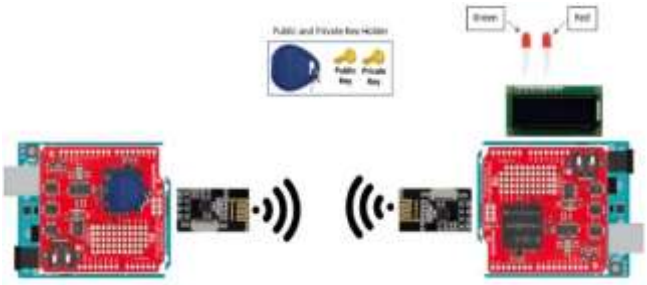

Fig.2..Wireless Data Encryption Process

(Figure.1)Illustrate the Architectural proposed approach for An Arduino-based wireless communication system utilizing RF transceivers, public-private key encryption, LED indicators, and an LCD display for secure monitoring.

The intended architecture of an Arduino wireless communication system involves various components to provide secure and effective transmission of data. Most central to the system are the RF transceivers, which are used to facilitate wireless communication between equipment. The transceivers, typically made up of modules such as the nRF24L01 or equivalents, work by communicating radio frequency signals for transmitting and receiving, making it possible for the system to communicate over short to medium ranges.

The use of public-private key encryption greatly improves the security of the system. The encryption scheme used ensures that the data being exchanged between the devices is kept confidential and safe from unauthorized access. The public key is employed to encrypt data prior to transmission, and the associated private key is used to decrypt the data upon receipt, thus providing secure communication between sender and receiver.

For the purpose of giving visual feedback and tracking system status, the design comprises LED indicators and an LCD display. The LED indicators are designed to indicate the operation status of the system—e.g., power, data transmission, and encryption status—via various color indications (e.g., green for normal, red for error). At the same time, the LCD screen provides a clearer picture of the system's operation, like showing messages about successful or failed encryption, system health, or even real-time updates of data from the communication system.

This integrated design not only provides efficient wireless communication among devices but also robust data security by encryption, while visual feedback mechanisms inform the user of the system status. Another aspect is the modularity of Arduino-based systems, which makes it easy to customize and scale up, allowing for future extensions such as real-time system diagnostics, logging capabilities, and addition of additional sensors or communications modules if necessary.

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 71-76
Published Online December 2024 in IJEAST (http://www.ijeast.com)

III. WORK FLOW

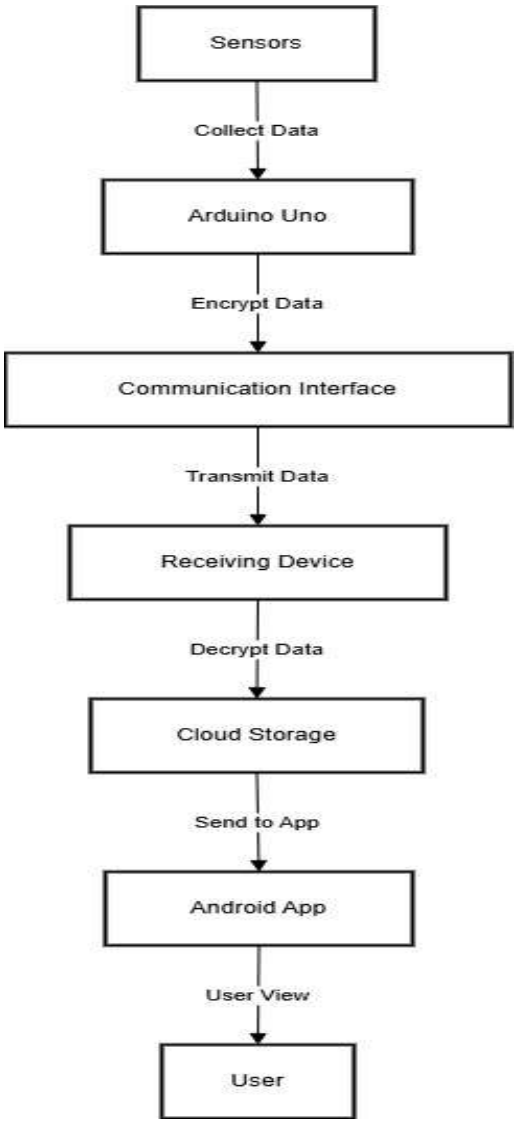

Fig.3.Architectural diagram for Work flow

(Figure.3)Illustrate the Architectural diagram of workflow for A sensor-based encrypted data acquisition system using Arduino, communication interface, cloud storage, and an Android app for secure real-time user access.

[1] Sensor Modules
Sensor modules are responsible for acquiring real-time environmental data by detecting physical parameters such as temperature, humidity, gas concentration, or motion. These sensors convert the detected analog or digital signals into readable data, which is then transmitted to the microcontroller unit (MCU) for further processing and analysis**.**

[2] Arduino Uno (Microcontroller Unit)
The Arduino Uno serves as the primary processing unit, interfacing with sensor modules to collect raw data. It performs signal conditioning, preprocessing, and formatting before encryption. Additionally, it controls data flow and manages wired or wireless communication protocols to ensure reliable data transmission.

[3] Encryption Module
The encryption module applies cryptographic algorithms such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) to secure transmitted data. It ensures data confidentiality and integrity by converting plaintext into an encrypted format, preventing unauthorized access and mitigating potential security threats.

[4] Receiving Device
The receiving device captures the encrypted data from the communication interface, validating its integrity and ensuring proper packet reconstruction. It acts as an intermediary between the transmission module and the decryption system, ensuring seamless data flow without loss or corruption.

[5] Decryption Module
The decryption module reverses the encryption process by applying the appropriate cryptographic decryption algorithm. It restores the encrypted data to its original readable format, ensuring that only authorized systems can access the sensitive information while maintaining data authenticity and confidentiality.
.

[6] Android Application (User Interface Module)
The Android application retrieves processed data from the cloud storage system, providing a graphical user interface (GUI) for data visualization, monitoring, and real-time alerts. It allows users to interact with the system via mobile or tablet devices, ensuring remote accessibility and seamless control.

IV. HARDWARE AND SOFTWARE SETUP

Hardware Setup:
A. Arduino Uno
The Arduino Uno is a microcontroller development board based on the ATmega328P microcontroller, designed for rapid prototyping and embedded system applications. It features 14 digital I/O pins, 6 analog input channels, and operates at a 5V supply voltage. The board supports serial communication interfaces such as UART, SPI, and I2C. It is programmed using the Arduino IDE, making it highly accessible for both novice and advanced developers. Due to its open-source architecture, it is extensively utilized in IoT, robotics, and automation applications.

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 71-76
Published Online December 2024 in IJEAST (http://www.ijeast.com)

B. DHT11/DHT22 Sensors
The DHT11 and DHT22 are digital temperature and humidity sensors that utilize a capacitive humidity sensing element and a thermistor for temperature measurement. The DHT11 offers a measurement range of 20–90% relative humidity (RH) and 0–50°C with ±5%RH and ±2°Caccuracy, making it suitable for basic environmental monitoring. The DHT22 provides a wider range of 0–100% RH and -40 to 80°C, with higher precision. Both sensors communicate via a single-wire digital protocol, commonly deployed in climate control, weather stations, and IoT-based monitoring systems.

C. MQ Series Gas Sensors
The MQ-series gas sensors utilize a semiconductor-based sensing element that alters its electrical resistance in the presence of target gases. These sensors convert the gas concentration into an analog voltage output, which can be processed using a microcontroller or analog-to-digital converter (ADC). Different MQ sensors are specialized for detecting specific gases, such as MQ-2 (LPG, methane, smoke), MQ-7 (carbon monoxide), and MQ-135 (air quality and hazardous gases). These sensors are widely applied in industrial safety systems, air quality monitoring, and gas leak detection.

D. Hardware Security Modules (HSMs)
A Hardware Security Module (HSM) is a dedicated cryptographic processor designed to generate, manage, and securely store cryptographic keys for encryption, authentication, and digital signature operations. HSMs provide tamper-resistant hardware protection, ensuring compliance with FIPS 140-2 and Common Criteria standards. These modules support cryptographic algorithms such as AES, RSA, ECC, and SHA and are widely integrated into payment processing, secure transactions, digital identity management, and enterprise security infrastructures to safeguard sensitive data against cyber threats.

Software Setup:
A. Arduino Cryptography Library
The Arduino Cryptography Library provides a suite of cryptographic algorithms, including AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (Rivest-Shamir-Adleman), to enable secure data transmission in embedded systems. It facilitates encryption, decryption, hashing (SHA, MD5), and key management operations, ensuring data integrity and confidentiality.

B. SSL Client Library
The SSL Client Library implements SSL (Secure Sockets Layer) and TLS (Transport Layer Security) encryption, providing secure end-to-end communication over the internet. It establishes encrypted client-server connections by layering SSL/TLS over standard networking protocols, ensuring data confidentiality, authentication, and integrity. This library is essential for preventing unauthorized interception (man-in-the-middle attacks) and is extensively used in secure web transactions, IoT cloud communication, and encrypted data exchange for Arduino-based applications.

C. WiFi101/ WiFiNINA Libraries
The WiFi101 and WiFiNINA libraries enable wireless communication between Arduino microcontrollers and WiFi networks, facilitating Internet of Things (IoT) applications. The WiFi101 library is designed for older modules such as the ATWINC1500 (MKR1000), while WiFiNINA supports newer modules, including NINA-W102. These libraries provide functionality for establishing, managing, and terminating TCP/IP connections, enabling Arduino-based devices to perform data transmission, HTTP requests, and real-time cloud interaction.

D. Software Serial Library
The Software Serial Library enables UART (Universal Asynchronous Receiver-Transmitter) communication on digital pins of an Arduino board, overcoming hardware limitations by creating additional software-based serial ports. It facilitates interaction with multiple serial devices, including GPS modules, Bluetooth modules, GSM modules, and RFID readers, without being restricted to the Arduino's dedicated hardware serial ports.

V. EXPERIMENT AND RESULT

The picture demonstrates an IoT-based secure data transfer system comprising a microcontroller, LCD display, PIR sensor, and a USB-to-serial adapter plugged into a laptop. The system provides encrypted communication through an XOR-based encryption scheme over TX and RX lines, with AES decryption to add data integrity. A secure cloud-based data transfer for real-time monitoring is enabled through an ESP8266 WiFi module.

Fig.4..Wireless Data Encryption Process

International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 71-76
Published Online December 2024 in IJEAST (http://www.ijeast.com)

The IoT-based secure data transmission system is designed to ensure encrypted communication and real-time monitoring through the integration of various components. A microcontroller serves as the central processing unit, managing data flow, encryption, and decryption. The PIR sensor detects motion and triggers data transmission, optimizing efficiency by preventing unnecessary communication. A USB-to-serial adapter connects the microcontroller to a laptop, facilitating data transfer and debugging via TX and RX serial lines.

To enhance security, XOR-based encryption is applied to outgoing data, making it unreadable without the proper decryption key, while AES decryption ensures data integrity upon reception. The ESP8266 Wi-Fi module enables encrypted cloud-based communication, allowing remote access and monitoring. Additionally, an LCD display provides real-time feedback on the transmission status, making the system more interactive.

By combining encryption, secure data transfer, and cloud connectivity, this system is ideal for applications requiring reliable and protected communication, such as industrial automation, smart home security, and surveillance systems.

Fig.5..Data Encryption

The picture demonstrates an IoT-based secure data transmission system with an LCD display, a PIR sensor, and a microcontroller-based system. The display indicates a message of successful communication.

The system uses serial communication with XOR-based encryption for secure data transfer, and AES decryption for data integrity. The ESP8266 Wi-Fi module provides encrypted cloud transmission for remote monitoring.

Fig.6..Data Decryption

The IoT-based secure data transmission system integrates a microcontroller, an LCD display, a PIR sensor, and a Wi-Fi module to ensure encrypted communication and remote monitoring. The PIR sensor detects motion and triggers data transmission, making the system efficient by sending information only when necessary.

The microcontroller processes and encrypts data using an XOR-based encryption method before transmission, while AES decryption ensures data integrity upon reception.

The ESP8266 Wi-Fi module enables secure, encrypted cloud communication, allowing remote monitoring and control. The LCD display provides real-time feedback by showing messages such as "Successful Communication" to indicate successful data transfer.

By incorporating these technologies, the system enhances security, minimizes unauthorized access, and ensures reliable data exchange in IoT applications.

VI. CONCLUSION

The project provides an efficient means of applying data encryption and decryption methods to protect wireless communication in Internet of Things networks. Through the incorporation of lightweight cryptographic algorithms, IoT devices with limited computing power can still have robust security without suffering noticeable performance degradation. Central security concerns across a variety of Internet of Things uses, such as smart residences, industrial control, and healthcare tracking, are handled by the system's focus on encryption and decryption processes that ensure data privacy, integrity, and authenticity being transferred. Additionally, the system is more immune to online threats such as data tampering and eavesdropping when safe key exchange systems and real-time encryption are implemented. By combining powerful cryptographic techniques with IoT infrastructure, the proposed solution demonstrates that data security can be improved while maintaining energy efficiency.

REFERENCES

[1]. Ahmed, I., & Kim, H. (2020). A lightweight encryption protocol for IoT devices with limited processing power. International Journal of Network Security, 22(3), 417-425.

[2]. Chen, Z., & Zhang, Y. (2021). End-to-end encryption schemes for secure IoT communications. IEEE Internet of Things Journal, 8(6), 4521-4530.

[3]. R. Sathya, Sekar K, S. Ananthi, and Dheepa T "Adversarially Trained Variational Auto-Encoders With Maximum Mean Discrepancy-based Regularization", 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), IEEE Xplore, ISBN: 978-1-6654-5637-1, March 2023.

[4]. Gao, Z., & Liu, P. (2022). Blockchain-based encryption for secure data exchange in IoT networks.

Journal of Cryptography and Information Security, 34(4), 301-312.

[5]. Gupta, R., & Sharma, S. (2023). IoT data security: Using quantum cryptography for advanced encryption. Journal of Quantum Computing and Cryptography, 9(1), 23-38.

[6]. Hassan, M. A., & Ahmed, S. (2021). Efficient lightweight cryptographic algorithms for IoT-enabled systems. Computers, 10(5), 57-65.

[7]. Khan, A., & Khan, M. Z. (2020). Secure key management for encrypted IoT communications. International Journal of Information Technology, 8(4), 350- 357.

[8]. Li, Q., & Wang, T. (2023). Privacy-preserving encryption methods for healthcare IoT applications. Journal of Healthcare Informatics Research, 7(2), 123-134.

[9]. Patel, S., & Singh, N. (2021). A survey of cloud-based encryption models for IoT systems. Journal of Cloud Computing and Security, 16(2), 112-123.

[10]. Zhou, Y., & Zhang, L. (2022). Machine learning-based anomaly detection for encrypted IoT networks. IEEE Transactions on Industrial Informatics, 18(5), 3804-3812.

[11]. Al-Fuqaha, A., &Guizani, M. (2021). Secure and efficient encryption methods for IoT networks. Journal of Network and Computer Applications, 178, 102977.

[12]. Kim, S., & Choi, M. (2022). Adaptive encryption strategies for low-power IoT devices. IEEE Transactions on Mobile Computing, 21(7), 2789-2801.

[13]. M. Mythili, R. Sathya, N. Gayathri, M. Yogeshwaran, and S. Madhanbabu "A Novel Framework for Smart Classroom Lecture Attendance Management System (LAMS) using IoT", Proceedings of the Third International Conference on Smart Electronics and Communication (ICOSEC 2022), IEEE Xplore, ISBN: 978-1-6654-9764-0, pp. 519-525, December 2022.

[14]. Martínez, P., & García, M. (2023). Privacy-enhancing encryption techniques for IoT-based smart cities. International Journal of Smart City Applications, 11(3), 45- 57. S

[15]. Sathya Ramasamy, Ananthi Selvarajan, Vaidehi Kaliyaperumal, Prasanth Aruchamy "A Hybrid Location-Dependent Ultra Convolutional Neural Network-Based Vehicle Number Plate Recognition Approach for Intelligent Transportation Systems", Concurrency and Computation: Practice and Experience, Vol. 35, Issue. 8, e7615, pp. 01-15, 2023.