Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

SECURE NRF WIRELESS COMMUNICATION FOR DATA ENCRYPTION

GUNTURU ANUSHA[1], P. SOWMYA[2], SHAHANA MUSKAAN[3], S. DEEPIKA[4]

ASSISTANT PROFESSOR 1, UG SCHOLAR 2,3,4

DEPARTMENT OF ECE, MALLA REDDY ENGINEERIGNG COLLEGE FOR WOMEN (UGC-AUTONOMOUS), MAISAMMGUDA, HYDERABAD, TELANGANA-500100

ABSTRACT:

In this work, the design and implementation of secured communication in a wireless network was achieved. The design was accomplished by using a Modified Advance Encryption Standard (MAES) algorithm and visual studio. A byte rotation technique was used to modify the Advance encryption standard in order to improve security of files over a wireless network. In the work, files were encrypted such that if they fall in the hands of unauthorized users, their content remains secured because MAES was used to encrypt them. Binary files of different formats and sizes were used to test the design, and file encryption and decryption without loss in fidelity was achieved using the MAES algorithm. Fifteen different file formats with different sizes were used to test the system and results obtained were compare with the Advanced Encryption Standard (AES) algorithm, MAES was equally very efficient in speed. Hence, byte rotation used to modify AES does not only improve security but equally very fast. The research therefore recommend amongst other things the usage of MAES for securing files.

INTRODUCTION:

In the modern era of digital communication, wireless networks play a pivotal role in enabling seamless data exchange across various devices. However, the open nature of wireless communication makes it inherently vulnerable to security threats such as eavesdropping, unauthorized access, and data tampering. Ensuring the confidentiality, integrity, and authenticity of data in wireless networks is therefore of paramount importance. This project focuses on the design and implementation of a secured communication system within a wireless network using a modified Advanced Encryption Standard (AES) algorithm. The AES algorithm, a widely accepted cryptographic standard, offers robust security and efficiency. However, as cyber threats become more sophisticated, there is a growing need to enhance its capabilities to address emerging challenges in wireless communication environments. The modified AES algorithm introduces optimizations tailored to the unique characteristics of wireless networks, such as limited bandwidth, variable connectivity, and resource constraints of devices. By incorporating enhancements in key generation, encryption rounds, and block processing, the proposed system aims to provide stronger security while maintaining efficiency. This introduction sets the stage for exploring the theoretical foundations, design methodology, and practical implementation of the enhanced security system. The study seeks to contribute to the broader field of wireless network security by addressing current limitations and proposing innovative solutions for secure data transmission.

The key objectives of this research include:

1. Evaluating the vulnerabilities and security requirements of wireless networks.
2. Analyzing the performance and limitations of the standard AES algorithm in wireless communication.
3. Developing and testing a modified AES algorithm to improve security and performance.
4. Demonstrating the feasibility and effectiveness of the proposed solution through simulations and real-world applications.

By leveraging the strengths of cryptographic techniques and addressing wireless network constraints, this research aims to provide a reliable and secure communication framework that

https://doi.org/10.36893/IEJ.2024.V53I12.019

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

aligns with the demands of contemporary and future wireless systems.

LITERATURE SURVEY:

Guy-Armand Yandji et al, "RESEARCH ON A NORMAL FILE ENCRYPTION AND vDECRYPTION," 978-1-4244-9283-1/11/$26.00 ©2011 IEEE

In this work, the design and implementation of secured communication in a wireless network was achieved. The design was accomplished by using a Modified Advance Encryption Standard (MAES) algorithm and visual studio. A byte rotation technique was used to modify the Advance encryption standard in order to improve security of files over a wireless network. In the work, files were encrypted such that if they fall in the hands of unauthorized users, their content remains secured because MAES was used to encrypt them. Binary files of different formats and sizes were used to test the design, and file encryption and decryption without loss in fidelity was achieved using the MAES algorithm. Fifteen different file formats with different sizes were used to test the system and results obtained were compare with the Advanced Encryption Standard (AES) algorithm, MAES was equally very efficient in speed. Hence, byte rotation used to modify AES does not only improve security but equally very fast. The research therefore recommend amongst other things the usage of MAES for securing files.

Suriyani Ariffin et al, "SMS Encryption using 3D-AES Block Cipher on Android Message Application," 978-1-4799-2758-6/13 $31.00 © 2013 IEEE DOI 10.1109/ACSAT.2013.68

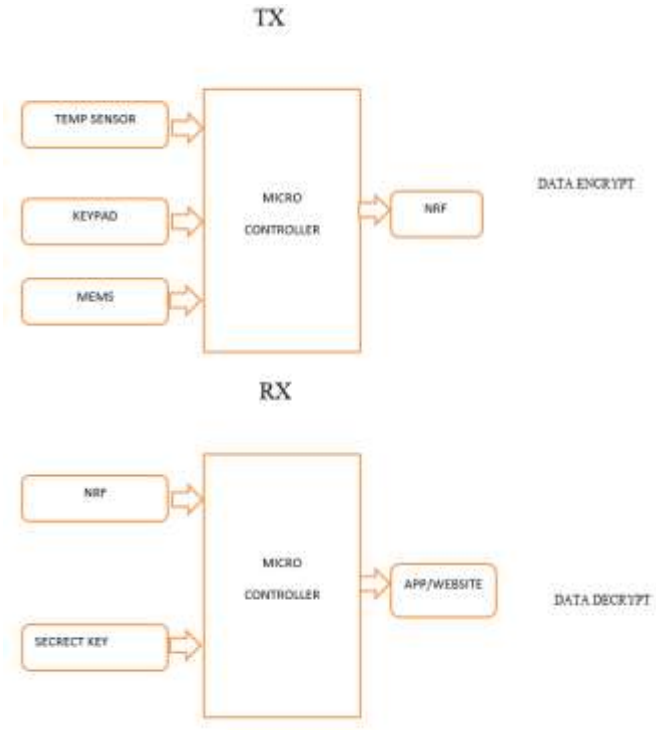
Over the internet and other network applications, the need for security is increasing each day due to its wide usage. There are a number of algorithms that have been developed for the secure transmission of data. This paper presents a novel approach for the generation of key using the Advanced Encryption Standard (AES) algorithm along with the Flower Pollination Algorithm (FPA). This combination is termed as Modified AES (MAES). Initially, a plain text of 128 bits is the input to this algorithm. This text is converted into a cipher text. The key generation is important for the generation of the S-Box (substitution box). The key generation in the proposed work is done using the Flower Pollination Algorithm. This step is done to generate the keys in such a way that the complexities of the S-Box enhances. This improves the security of the proposed approach for data transmission in a network. Then encryption is done. This is followed by decryption. Finally, the 128-bit plain text is retrieved at the receiver's side. The MAES algorithm was compared with other traditional cryptographic algorithms. The proposed MAES algorithm yielded outstanding results.

Adam Berent, Advanced Encryption Standard by Example V 1.7

Internet of things (IoT), internetworking of smart devices, embedded with sensors, software, electronics and net-work connectivity that enables to communicate with each other to exchange and collect data through an uncertain wireless medium. Recently IoT devices are dominating the world by providing it's in different functionality and real-time data communication. Apart from versatile functionality of IoT devices, they are very low- battery powered, small and having revealing or involving, and experience lots of challenges due to unsafe communication medium. Inspite the fact of many challenges, the energy issue is now becoming the prime concern. Optimization of algorithms in terms of energy consumption has not been explored specifically; rather most of the algorithms focus on hardware area to minimize it extensively and to maximize it on security issue as possible. But due to recent emerge of IoT devices, the main concern are shifting to moderate security and less energy consumption rate. We present MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. A new 1- dimensional Substitution Box is proposed by create or prepare methodically a novel equation for constructing a square matrix in affine transformation phase ofMAES.Efficiency rate of MAES is around 18.35% in terms of packet transmission which indicates MAES consumes less energy than AES and it is applicable for Resource Constraint Environments.

IMPLEMENTATION

BLOCK DAIGRAM



POWER SUPPLY

A **regulated power supply** transforms unregulated AC (Alternating Current) into a stable DC (Direct Current). It guarantees consistent output despite variations in input. A regulated DC power supply is also known as a linear power supply, it is an embedded circuit and consists of various blocks

- **Regulated Power Supply Definition**: A regulated power supply ensures a consistent DC output by converting fluctuating AC input.

https://doi.org/10.36893/IEJ.2024.V53I12.019

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, December : 2024

- **Component Overview**: The primary components of a regulated power supply include a transformer, rectifier, filter, and regulator, each crucial for maintaining steady DC output.
- **Rectification Explained**: The process involves diodes converting AC to DC, typically using full wave rectification to enhance efficiency.
- **Filter Function**: Filters, such as capacitor and LC types, smooth the DC output to reduce ripple and provide a stable voltage.
- **Regulation Mechanism**: Regulators adjust and stabilize output voltage to protect against input changes or load variations, essential for reliable power supply

SENSORS

Sensors are used for sensing things and devices etc. A device that provides a usable output in response to a specified measurement. The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity. The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance, etc.

MEMS SENSOR WORKING AND ITS APPLICATIONS

The term MEMS stands for micro-electro-mechanical systems. These are a set of devices, and the characterization of these devices can be done by their tiny size & the designing mode. The designing of these sensors can be done with the 1- 100-micrometer components. These devices can differ from small structures to very difficult electromechanical systems with numerous moving elements beneath the control of incorporated micro-electronics. Usually, these sensors include mechanical micro-actuators, micro-structures, micro-electronics, and micro-sensors in one package. This article discusses what is a MEMS sensor, working principle, advantages and it's applications

DESCRIPTION:

In recent years, many research works have been undergone and significant achievements have been found by many known researchers with respect to Resource Constraint Environments (RCEs). However, most of them have attack low area and low power as their concerned aspect and are hardware oriented. To provide implementation choice of the block cipher, Bogdanov et. al. [5] have investigated how the variation in (a) the architecture of S-Box/MixCloumn, (b) frequency of the clock cycle and (c) unrolling the design can affect the energy consumption. Their model is accuracy of estimating the energy consumed by several lightweight algorithms. With the help of figures, the proposed model is compared with respect to the different degree of unrolling. Moreover, they have proved that total energy consumption in a circuit during an encryption operation has roughly a quadratic relation with the degree of unrolling and the most energy consuming part is Substitution Box (S-Box) in 2-round unrolled design. Feldhofer et. al. [16] and Moradi ET. al. [17] have proposed an implementation of AES and its basic transformations (such as S-Box) attacked low area and low power. All the implementations are mostly hardware oriented. [16] Design is based on an 8-bit datapath and approximately occupies 3400 Gate Equivalents (GE) and [17] design features a mixed datapath and requires 2400 GE respectively. The silicon implementation of low power AES is discussed in the work of Hocquet et. al. [18] which illustrates that 740 pj energy is consumed per encryption. Kerckhof ET. al. [19] have presented a comparative study of different algorithms based on area, throughput, power and energy and applied state of the art techniques for reducing power consumption. Batina ET. al. [20] have explored the area, power, and energy consumption of several recently-developed lightweight block ciphers csonsidering possible optimization for the non-linear transformation and compared these with the AES algorithm. However, the effects of energy consumption for different design choices, such as the size of the data path, amount of serialization, and effects of architectural optimized are not considered by any of the works.researchers,Kong et. al.[22] have surveyed modern symmetric cryptographic solutions for Resource Constraint Environments (RCEs). Authors have provided collective surveys from other literature on the topic of hardware, applications, design re- quirements and security trends of RCEs. Felicisimo et. al. [23] have proposed two Substitution Boxes, where the first S-Box is the Rijndael S-Box and the second S-Box, replacing the MixColumns operation of the original AES, is constructed through an XOR operation and affine transformation. Based on action of pretending testing, it is found out that the modified AES algorithm using multiple S-Boxes has better speed performance compared to the original cipher. Kawle et. al. [24] have proposed a modified AES using state- of-art

https://doi.org/10.36893/IEJ.2024.V53I12.019

techniques to decrease computational overhead of the original AES algorithm by encrypting large size data, for instance, multimedia data.

The Advanced Encryption Standard (AES) [13], a symmetric key block which is published by the National Institute of Standards and Technology (NIST) in December 2001. It is a non-Feistel block cipher that encrypts and decrypts a fixed data block of 128-bits. There are three different key lengths. The encryption/decryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192- bit keys, and 14 rounds for 256-bit keys. AES performs several rounds where each round is made of several stages. A data block is changed from one stage to another. Before and after each stage, the data block is referred to as a state. Each round, except the last, performs four trans-formations which are invertible. The last round performs the rest three transformations except the MixColumns stage. Figure 1 shows the AES cipher structure.

As we propose a lightweight version of AES for RCEs, first analyze the actual mechanism of AES and implement AES in structured programming language before implementing it in nesC. The same process is followed for the proposed MAES. After implementing both the algorithms (AES and MAES) in nesC, we integrate these in telosB sensor mote. Humidity, temperature, and luminance can be sensed by telosB sensor mote. Room temperature is used as our input set for both the algorithms. The experimental approach construct in two phases.In the first phase, we implement the original AES in the telosB sensor mote and build two sets of transmitted data packets. The first data set is to pass a encrypted data packets using the original AES encryption techniques and the second data set is composed of without converted a data packets. In the second phase, we implement both the original AES and the proposed MAES in the telosB sensor mote. Unauthorized data packets are not considered in the second phase of the experiment. Same as the previous phase, we construct two sets of transmitted data packets which are encrypted using the original AES and the proposed MAES. The internal voltage sensor of telosB uses the microcontrollers 12-bit Analog toDigital Converter (ADC). For both the phases, the raw value of ADC is considered. Equation 6 is used to convert the raw value of the ADC to the corresponding voltage value.Since we conduct our experiment using AA 1.5V batteries, the values of reference voltage is 1.5V.

CONCLUSION:

The purpose of the thesis was to design a system that can secure communication via wireless network without interference by third party. If by any means the system is bypassed by unauthorized users, they will not be able to access the contents of the original message because the message is secured.

Modified AES was realized via this system, which can encrypt binary files of any format and decrypt them. Compared with the existing AES, the modified AES provides additional security by addition of byte rotation. The system was realized using Visual studio.

REFERENCES:

[1] Liddell HG, Scott R, Jones H, McKenzie R (1984) A Greek-English Lexicon. Oxford University Press.

[2]https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=

899:a-summary-of-the-legislation-on-cybercrime-innigeria&option=com_content&view=article&id=899:a-summary-of-the-legislation-oncybercrime-in-nigeria

[3] https://www.webopedia.com/TERM/S/symmetric_key_cryptography.html

[4] D.I George Amalarethinam, J.Sai Geetha, “Image Encryption and Decryption in Public Key Cryptography based on MR,” 978-1-4799-7623-2/15/$31.00_c 2015 IEEE

[5] Ankit Dhamija, “A Novel Cryptographic and Steganographic Approach for Secure Cloud

Data Migration,” 2015 International Conference on Green Computing and Internet of Things

(ICGCIoT) 978-1-4673-7910-6/15/$31.00_c 2015 IEEE

[6] Prakash G. L et al, “Data Encryption and Decryption Algorithms using Key Rotations for

Data Security in Cloud System,” 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT) 978-1-4799-3140-8/14/$31.00 ©2014 IEEE

[7] Sea Chong Seak, Ng Kang Siong, “A File-based Implementation of XML Encryption,” 2011

5th Malaysian Conference in Software Engineering (MySEC), 978-1-4577-1531-0/11/$26.00

©2011 IEEE

[8] Sruthis S. et al, “Encryption & Decryption of Text file and Audio using LabVIEW," 2017

International Conference on Networks & Advances in Computational Technologies (NetACT)

|20-22 July 2017| Trivandrum, 978-1-5090-6590-5/17/$31.00 ©2017 IEEE

[9] Kun-Lin Tsai et al, “A Group File Encryption Method using Dynamic System Environment Key,” 978-1-4799-4224-4/14 $31.00 © 2014 IEEE, DOI 10.1109/NBiS.2014.22

[10] Suli Wang, Ganlai Liu, “File encryption and decryption based on RSA algorithm,” 2011

https://doi.org/10.36893/IEJ.2024.V53I12.019

International Conference on Computational and Information Sciences, 978-0-7695-4501-1/11

$26.00 © 2011 IEEE

[11] Matthew Wangsadiredja et al, "Text and File Encryption Application for BlackBerry Using

Cipher Feedback 8-bit Mode," 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia, 978-1-4577-0752-0/11/$26.00 ©2011 IEEE

[12] Biao Wei et al, "A Practical One-time File Encryption Protocol for IoT Devices," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE

International Conference on Embedded and Ubiquitous Computing (EUC), 978-1-5386-3221-

5/17 $31.00 © 2017 IEEE

[13] Guy-Armand Yandji et al, "RESEARCH ON A NORMAL FILE ENCRYPTION AND

DECRYPTION," 978-1-4244-9283-1/11/$26.00 ©2011 IEEE

[14] Suriyani Ariffin et al, "SMS Encryption using 3D-AES Block Cipher on Android Message

Application," 978-1-4799-2758-6/13 $31.00 © 2013 IEEE DOI 10.1109/ACSAT.2013.68

[15] Adam Berent, Advanced Encryption Standard by Example V 1.7

https://doi.org/10.36893/IEJ.2024.V53I12.019