International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Secure Military Communication with AES Crypto Algorithm

[1] Rushikesh Vijay Chaukate , [2] Samruddh Santosh Sohoni , [3] Hrushikesh Madhukar Dawange , [4]Sarojini Naik

[1,2,3] UG Student, P.E.S's Modern College Of Engineering Pune, India

[4] Assistant Professor,P.E.S's Modern College Of Engineering Pune, India
[1]rushikesh_chaukate@moderncoe.edu.in, [2]samruddh_sohoni@moderncoe.edu.in, [3]hrushikesh_dawange@moderncoe.edu.in , [4]Sarojini.naik@moderncoe.edu.in

Abstract - **This paper introduces a robust and secure communication system specifically designed for military applications, employing the Advanced Encryption Standard (AES) algorithm to ensure the confidentiality and integrity of sensitive data. The system integrates Java for backend operations, SQL for secure data storage, and Bootstrap for a responsive user interface, all managed through an Apache Tomcat server. The primary goal is to provide a reliable and secure communication platform in environments prone to connectivity disruptions and cyber threats. Our implementation encrypts messages before transmission and storage, ensuring data remains protected against unauthorized access. Extensive testing confirms the system's efficacy in maintaining secure communications with minimal performance impact.**

Keywords— AES, cipher, DES, data encryption, data decryption, DTNs.

I. INTRODUCTION

In the modern era, the proliferation of digital devices such as computers and mobile phones for communication and data storage has surged. Consequently, there has been a significant increase in unauthorized attempts to access data. Ensuring data security has become a paramount concern. Cryptography, the science of encrypting and decrypting information, plays a crucial role in securing data during transmission and storage.

Cryptographic systems consist of two essential components: the algorithm and the key. The security of these systems relies heavily on the key used for encryption and decryption. Cryptographic mechanisms can be divided into two categories: symmetric key cryptography, where the same key is used for both encryption and decryption, and asymmetric key cryptography, which employs different keys for each process. Symmetric key algorithms, such as the Advanced Encryption Standard (AES), are known for their speed, ease of implementation, and lower computational requirements compared to asymmetric algorithms. AES, a widely adopted encryption standard, was developed by Joan Daemen and Vincent Rijmen and published by the National Institute of Standards and Technology (NIST) in 2001.

This paper explores the application of AES in a secure data retrieval scheme for decentralized Disruption-Tolerant Networks (DTNs). These networks are crucial in military environments where connectivity is intermittent, and security is paramount. We propose a method where multiple key authorities manage their attributes independently, ensuring robust data protection even in hostile conditions.

Goals and Objectives:

- Develop a secure data retrieval scheme using AES for decentralized DTNs.
- Demonstrate the application of this mechanism in managing confidential data within Disruption-Tolerant Military Networks.

Area of Project: Network Security

Technical Keywords:

- **Access Control:** A selective restriction of access to a place or resource, ensuring that only authorized users can access specific data.
- **Advanced Encryption Standard (AES):** A symmetric encryption algorithm that transforms data into an unreadable format to protect privacy during transmission. The same key can be used for both encryption and decryption.
- **Disruption-Tolerant Network (DTN):** A network designed to withstand temporary or intermittent communication issues, ensuring reliable data transmission even under adverse conditions.

Problem Statement:
Disruption-tolerant network (DTN) technologies are increasingly effective in military applications, allowing soldiers' wireless devices to communicate and access confidential information reliably. These networks face challenges in enforcing authorization policies and updating policies for secure data retrieval. While AES is a promising

solution for access control, its application in decentralized DTNs presents security and privacy challenges, such as attribute revocation, key escrow, and coordination among different authorities.

II. AES ALGORITHM SPECIFICATION

AES comes in three variants based on key length: AES-128, AES-192, and AES-256. These numbers indicate the size of the key in bits, with larger keys providing higher security. The AES algorithm uses a round function composed of four byte-oriented transformations for encryption:

- **Substitute Byte:** Non-linear byte substitution using an S-box.
- **Shift Row:** Cyclically shifts bytes in the state matrix.
- **Mix Columns:** Combines bytes in each column.
- **Add Round Key:** Combines the state with a portion of the key.

For decryption, these steps are reversed:

- **Inverse Shift Row**
- **Inverse Substitute Byte**
- **Add Round Key**
- **Inverse Mix Columns**

The number of rounds depends on the key length:

- AES-128: 10 rounds
- AES-192: 12 rounds
- AES-256: 14 rounds

III. SOFTWARE CONTEXT:

The project utilizes J2EE as the implementation language and MySQL for backend development. Eclipse IDE is the chosen development environment, and Apache Tomcat serves as the temporary server. These tools are readily available and widely used in software development, ensuring ease of access and implementation.

IV. METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY ISSUES:

To address the problem of secure data retrieval in DTNs, the project employs AES, a symmetric encryption algorithm known for its efficiency and robustness. The proposed scheme ensures that even in hostile environments where key authorities may be compromised, the confidentiality of stored data is maintained. Additionally, the scheme supports fine-grained key revocation for each attribute group, enhancing security and flexibility.

4.1 Outcome:

An efficient and secure data retrieval method using Advanced Encryption Standard (AES) for decentralized DTNs. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group.

4.2 Applications

• This system is very helpful to send the secrete message in military.
• We can use this application anywhere that required to send the secret information

V. PROJECT ESTIMATE

The project follows the Waterfall Model, a linear-sequential life cycle model ideal for small projects with well-defined requirements. Each phase must be completed before the next begins, ensuring a structured and organized approach. The phases include:

- **Requirements Analysis:** Identifying and documenting project requirements.
- **System Design:** Creating the system architecture based on requirements.
- **Implementation:** Developing the system components.
- **Integration and Testing:** Combining and testing all components to ensure they work together.
- **Deployment:** Releasing the system to the operational environment.
- **Maintenance:** Ongoing support and updates as needed.

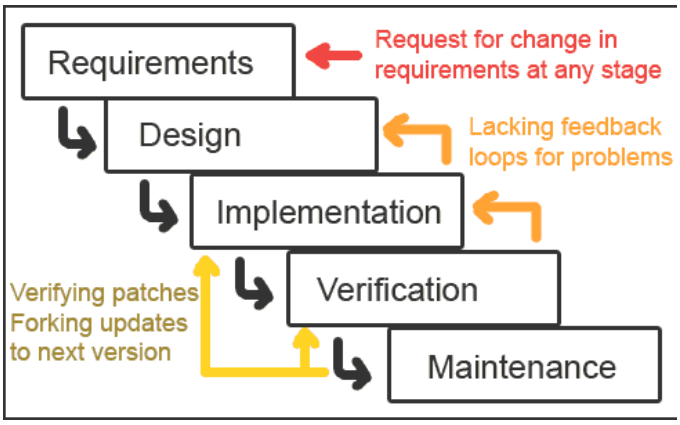
Project Resources

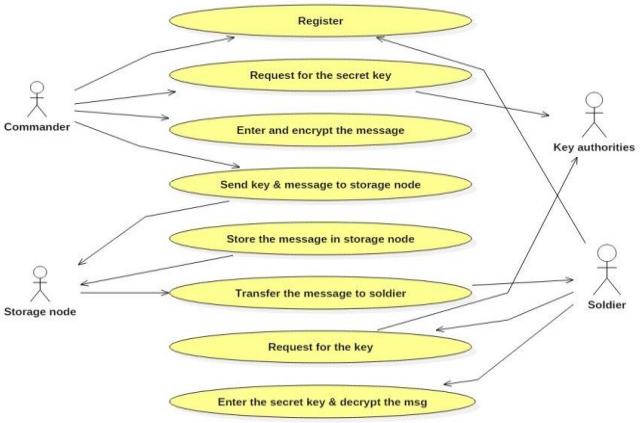
Hardware Requirements:

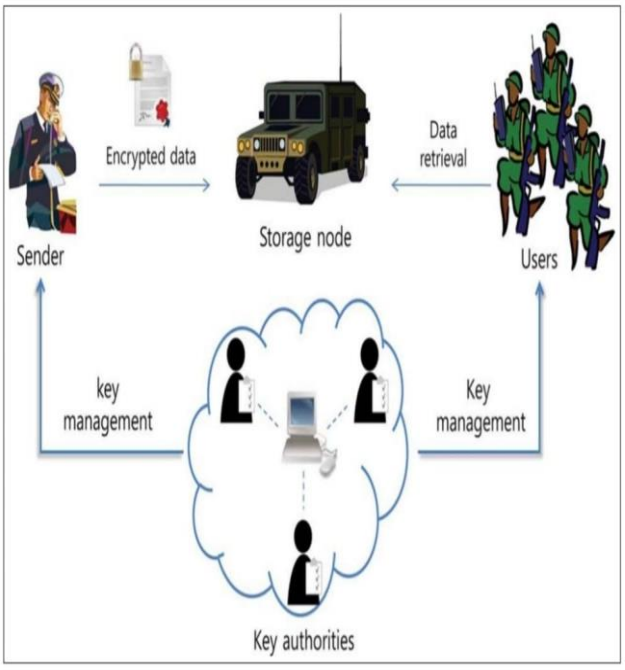
- Minimum 2 GB RAM
- Pentium IV Processor or above
- Minimum 80 GB hard disk
- Standard resolution monitor

Software Requirements:

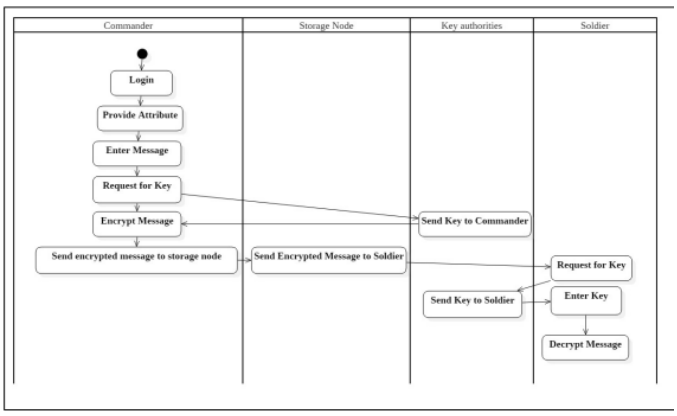
- Operating System: Windows 8 or above
- Eclipse IDE
- Java JDK 11
- MySQL 8.0
- Apache Tomcat 9.0







VI. IMPLEMENTATION DIAGRAM:



VII. SECURITY ANALYSIS

The security of our system is paramount, given the sensitive nature of military communication. The AES algorithm is employed to ensure the confidentiality of transmitted data. However, we must also consider potential vulnerabilities and threat models:

Man-in-the-Middle Attacks: Our system uses encrypted channels to prevent unauthorized interception of data.

Key Management Risks: Regular key rotation and secure key distribution mechanisms are in place to mitigate the risk of key compromise.

Attribute Revocation: We use fine-grained key revocation methods to ensure that users who lose their access privileges cannot decrypt sensitive information.

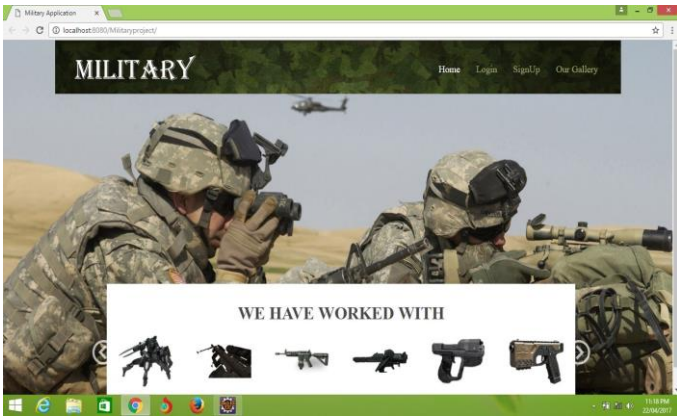
Insider Threats: Role-based access control (RBAC) ensures that only authorized personnel can access specific data, reducing the risk of insider attacks.

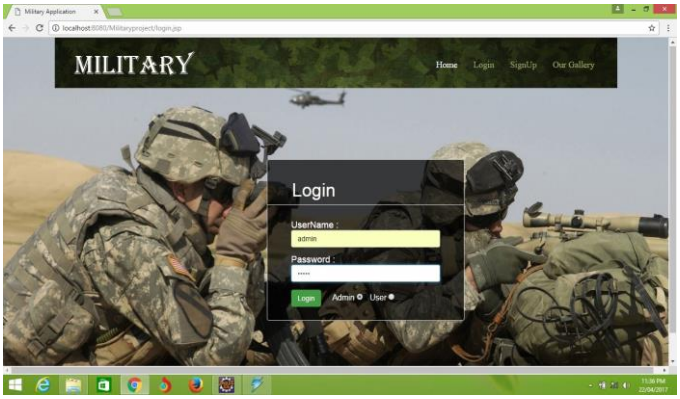
VIII. REAL-WORLD APPLICATION SCENARIOS

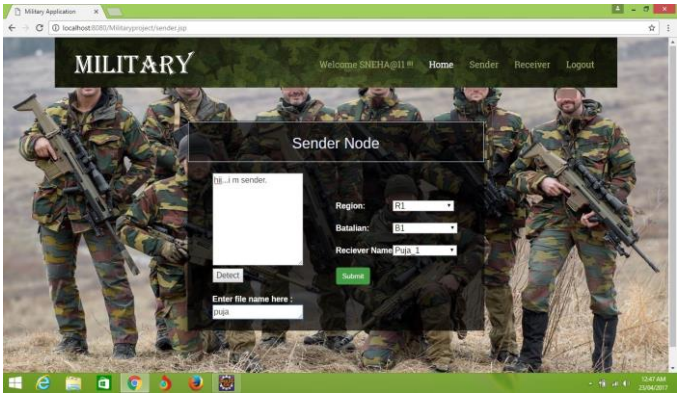
Real-World Application Scenarios: Our secure communication system can be applied in various military and other high-security environments:

- **Field Operations:** Ensures secure real-time communication between troops and command centers, even in disrupted networks.
- **Intelligence Gathering:** Protects sensitive information collected from field agents, ensuring it can be safely transmitted and stored.
- **Emergency Response:** Facilitates secure coordination among different agencies and units during disaster response operations.

IX. OUTPUT:







X. CONCLUSION:

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes.

CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group.

We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

XI. REFERENCES:

[1] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, Systematic classification of side-channel attacks: A case study for mobile devices, IEEE Commun. Surv. Tutor., vol. 20, no. 1, pp. 465–488, 2018.

[2] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas, Sifa: Exploiting ineffective fault inductions on symmetric cryptography, IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 3, pp. 547– 572, 2018.

[3] F. Zhang, X. Lou, X. Zhao, S. Bhasin, W. He, R. Ding, S. Qureshi, and K. Ren, Persistent fault analysis on block ciphers, IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 3, pp.150–172, 2018.

[4] X. X. Wang, H. Wei, T. Jing, Z. Jiacheng, and T. Shibo, Correlation fault attack on aes, Journal of Xidian University, vol. 48, no. 4, pp. 192–199, 2021

[5] L. Han, N. Wu, F. Ge, F. Zhou, J. Wen, and P. Qing, Differential fault attack for the iterative operation of AES192 key expansion, in Proc. 2020 IEEE 20th Int. Conf. Communication Technology (ICCT), Nanning, China, 2020, pp. 1156–1160

[6] M. Gay, T. Paxian, D. Upadhyaya, B. Becker, and I. Polian, Hardware-oriented algebraic fault attack framework with multiple fault injection support, in Proc. 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Atlanta, GA, USA, 2019, pp. 25–32.

[7] S. Saha, M. Alam, A. Bag, D. Mukhopadhyay, and P. Dasgupta, Leakage assessment in fault attacks: A deep learning perspective, https://eprint.iacr.org/2020/306, 2020

[8] F. Zhang, Y. Zhang, H. Jiang, X. Zhu, S. Bhasin, X. Zhao, Z. Liu, D. Gu, and K. Ren, Persistent fault attack in practice, IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2020, no. 2, pp. 172–195, 2020

[9] G. Xu, F. Zhang, B. Yang, X. Zhao, W. He, and K. Ren, Pushing the limit of PFA: Enhanced persistent fault analysis on block ciphers, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 40, no. 6, pp. 1102–1116, 2021.

[10] X. Wang, J. Zheng, L. Wu, J. Zhu, and W. Hu, A correlation fault attack on rotating S-box masking AES, in Proc. 2021 Asian Hardware Oriented Security and Trust Symp. (AsianHOST), Shanghai, China, 2022, pp. 1–6

[11] C. Dobraunig, M. Eichlseder, H. Gross, S. Mangard, F. Mendel, and R. Primas, Statistical ineffective fault attacks on masked AES with fault countermeasures, in

Proc. 24th Int. Conf. Theory and Application of Cryptology and Information Security, Taipei, China, 2018, pp. 315–342.