iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6445

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

Secure Data Retrieval for Decentralized Data Communication

Ms. Madhu R[1], Ms. Shikha Rai[2]
[1]*Assistant professor, ISE-EC-Department, Sahyadri College of Engineering and management, Mangaluru*

Abstract: ***Network Security involves the warrantation of ingress to data in a network. Network security mainly deals with authentication which involves username and password. The confidential information that is transmitted within the system has to be more secure. Nowadays there are crisis on the data loss. Decentralized systems are becoming outstanding solutions that allows wireless devices to communicate with each other and ingress the confidential information more steadily. There will be end to end security between source and destination pair. The data will be encrypted in the source node and decrypted in the receiver node with the aid of One Time Password, there will be a key manager to store the encrypted keys. In this system we will be implementing two algorithms i.e. AES and DES algorithms. It demonstrates how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the decentralized network.***
Keywords: Warrantation, Decentralized Network, AES algorithm, DES algorithm

I. INTRODUCTION

Network security mainly focuses on protecting the usability and integrity of network and data. It targets a variety of threats and stops them from breaking into and spreading on the network. Source node sends the encrypted data which will be decrypted at the destination node, as a result security will be established within the network. With the increase in technology, it has become more and more essential to protect every aspect of online information and data. By increasing security, there will be decrease in the chance of attacking the confidential information and the theft of data.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

When we discuss about confidentiality of data, we mainly concentrate on safeguarding the data from disclosure to unauthorized parties. Data has importance, especially in today's world such as bank account details, credit card numbers, trade secrets, government documents. Everyone wishes to keep the data as a secret. Protecting such confidential data is a very vital part of information security. A better way to safeguard data confidentiality would be encryption. Encryption ensures that only the authorized users (users who knows the key) can ingress the data. Encryption is very wide ranging in today's environment and can be found in almost every major protocol in use.

In the existing system, a centralised encryption management is present which does the data encryption and decryption at the same place and stores the data with keys in centralized manner. Previously existing system is not secure. Centralized encryption provides higher range of security.

So in order to provide high security in the decentralized system, the source node sends the data which will be encrypted in the sender side and receives the decrypted data in receiver side. In this system we will make use of AES and DES algorithms.

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers including telecom providers, Internet providers, and even the provider of the communication service from being able to access the cryptographic keys needed to decrypt the conversation.[1] The systems are designed to defeat any attempts at surveillance or tampering because no third parties can decipher the data being communicated or stored. For example, companies that use end-to-end encryption are unable to hand over texts of their customers' messages to the authorities.

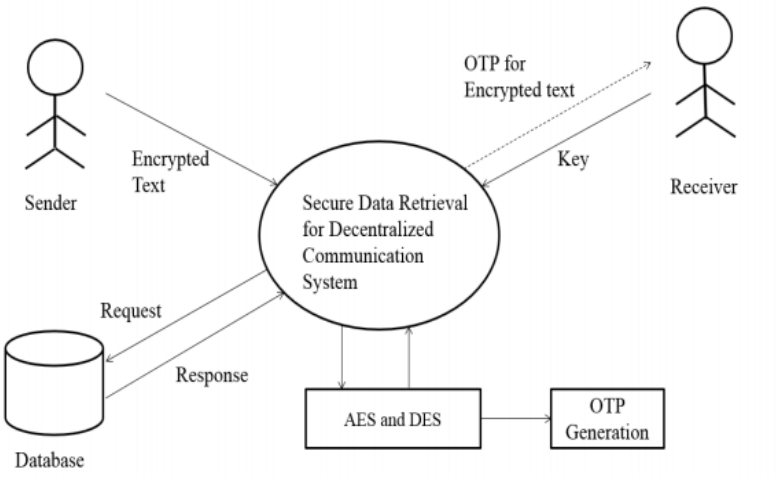
End-to-end encryption ensures that data is transferred securely between endpoints. But, rather than try to break the encryption, an eavesdropper may impersonate a message recipient (during key exchange or by substituting his public key for the recipient's), so that messages are encrypted with a key known to the attacker. After decrypting the message, the snoop can then encrypt it with a key that they share with the actual recipient, or their public key in case of asymmetric systems, and send the message on again to avoid detection. This is known as a man-in-the-middle attack

II. METHODOLOGY

The project "Secure Data Retrieval for Decentralized Data Communication" focuses on encryption of the text and key at the source node with the aid of AES and DES algorithm respectively and decryption of the key at the destination node is done with OTP, transmitted by sender. This system also comprises of storage node and key manager

A. Architecture Diagram

Architecture Diagram of the proposed system between the various modules of the proposed system. It is very essential to know the whole concept of the proposed system. Architectural Diagram of the Secure Data Retrieval for Decentralized Data Communication. In this proposed system data will be encrypted in the source node and decrypted in the receiver node with the aid of One Time Password, there will be a key manager to store the encrypted keys. In this system we will be implementing two algorithms i.e. AES and DES algorithms. It exhibits how to make use of the proposed structure to safely and systematically manage the confidential information disseminated in the decentralized proposed system network.



III.IMPLEMENTATION

In order to accomplish the aim of the project we define the methods which can help in fulfilling the goals of the proposed project. According to the proposed project the SCS makes use of Encryption and Decryption techniques which comprises of AES and DES algorithms. SCS embraces various modules for users to exchanging of the crucial information.

A. Registration

Input username, password, confirm password and user type Check if username exists If exist then Display error message Else Check if password and confirm password matches If password matches then New user created End if End if

B. Login

If username exists, then Input username, password Check whether password matches 19 Secure Data Retrieval for Decentralised Data Communication Chapter 6 If password matches, then Successful Login Else Display error message End if End if

C. Change Password

Input username, current password, and new password and confirm new password If username exists and current password matches the database password, then Change the password for particular user name and store it in database Else Display error message End if

D. Chat Text

Begin input text, phone number Set random r Set s = r. next double S = substring (3,8) AES encrypt (plain text, s, 256) Get enc encrypted value Store in DB Set random r1 Set s1 = r1. next double S1 = substring (3,8) DES encrypt (s, s1) Store in key manager Send SMS key

E. Chat File

input file, phone number Set random r Set s = r. next double S = substring (3,8) Read file teBeginxt AES encrypt (file text, s ,256) Get enc encrypted value Write file(enc) Save file Store in DB Set random r1 Set s1 = r1. next double S1 = substring (3,8) DES encrypt (s, s1) Store in key manager Send key as SMS end

F. Chat Decrypt

Begin Read session of user Read chatid Bind to list box Read chatid from selected item Create DES object DES decrypt (key manager text, SMS key) Set label text = decrypt text Create AES object AES decrypt (label text, key, 256) Display result end

G. File Decrypt

Begin Read session of user Read File Read Text Create DES object DES decrypt (File Text, SMS key) Set label Text = decrypt Text Create AES object AES decrypt (label Text, key, 256) Get Plain Text Write file (Plain Text) Display File Text end

H. OTP

Begin Generate random Key Set s = Key s = substring s(4,8) create ATSSMS object set send SMS parameter send SMS(phone, message) commit end

IV. RESULTS AND ANALYSIS

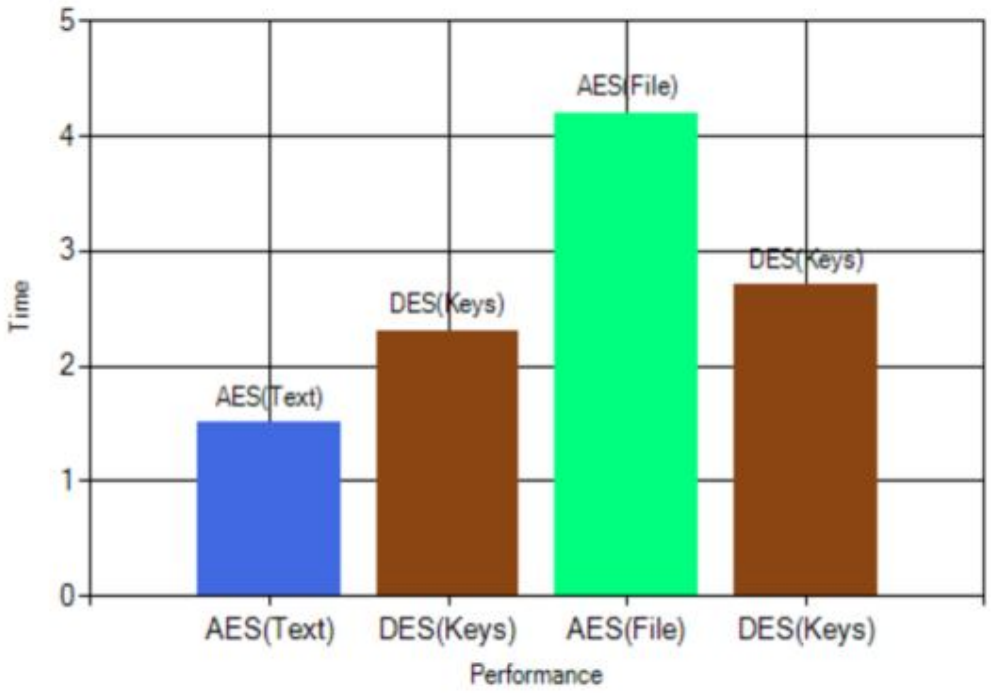


Figure 4.1: Performance Analysis of AES and DES for Encryption

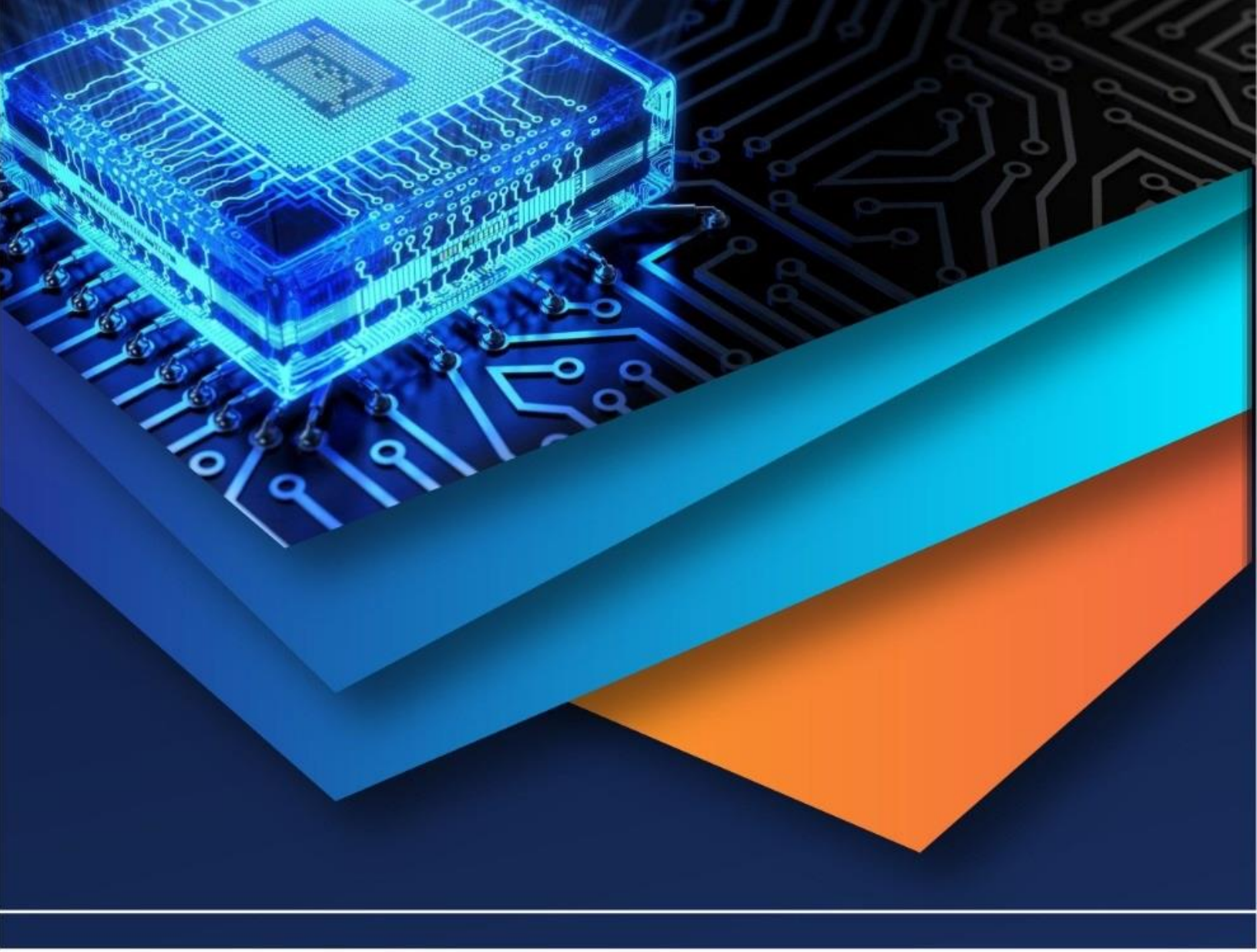
The above graph shows the performace analysis of AES and DES for encryption(text message and file). AES takes more time for encrypting the file than for encrypting the text messages. Similar to AES even DES also takes more time to encrypt the keys of file than for encrypting the keys of text messages.

V. CONCLUSION AND FUTURE WORK

System Security centers around ensuring the uprightness of information that should be secured .Thus Encryption would be the most ideal approach to secure information .It permits to safely ensure the information that you don't need any other individual to access to. Here the content are encoded with the goal that exclusive approved individual can access to it and who are not approved can't. The information here will be scrambled in the sender side and unscrambled in the recipient side. Hence this venture causes in giving security to the information. The application is outlined such that any further upgrades should be possible effortlessly. New modules can be added to the current framework with less exertion. In future this framework can be outlined as portable/Ios application so the client can distribute the online production without cost per click.

REFERENCES

[1] Faizan Badshah, Syed Tauhid Ullah Shanh, Syed Roohullah Jan, Izaz Ur Rehaman, "Communication between multiple processes on same device using TCP/IP suite", in Proc. 2017 IEEE, pp.29-42.
[2] Javier Sanchez, Ronny Correa, Hernando Buenano, Susana Arias and Hector Gomez, "Encryption technique :A theoretical overview and the future proposals", in Proc. 2016 IEEE, pp.59-70.
[3] Rini Wisnu Wardhani, Dion Ogi, Mohamad Syahral, Dedy Septono Catur P, "Fast implementation of AES on Cortex-M3 for security information devices", in Proc. 2017 IEEE,pp.45- 78.
[4] Thanh Nguyen, Snehasis Mukhopadhyaya , "Selective Decentralization to improve Reinforcement learning in unknown linear noise systems", in Proc. 2017 IEEE,pp.75-85.
[5] Karthik , Chinnasamy, Deepalakshmi, "Hybrid Cryptographic Technique using OTP : RSA", in Proc. 2017 IEEE, pp.75-90.
[6] Gotimukul Venkatesh , Sunkara Venu Gopal, Marudula Meduri, Sindhu C, " Application of Session Login and One Time Password in Fund Transfer System using RSA algorithm", in Proc. 2017 IEEE, pp.55-60.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY