A

Project-I Report

on

SECURITY OF DATA WITH RGB COLOR AND AES ENCRYPTION TECHNIQUES

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Jagruti J. Patil
Prajakta D. Dusane
Ruchita M. Pandya
Urvashi M. Jain

Under the Guidance of

Miss. Sweta Pandey

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)
2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Project-I entitled *Security of Data with RGB Color and AES Encryption techniques*, submitted by

Jagruti J. Patil
Prajakta D. Dusane
Ruchita M. Pandya
Urvashi M. Jain

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: September 28, 2016
Place: Jalgaon

Miss. Sweta Pandey
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

"Security of Data with RGB Color and AES Encryption techniques" project consumed huge amount of work, research and dedication. Still, implementation would not have been possible without the support of many individuals and guide.

Therefore, project group would like to extend the sincere gratitude to all of them. First of all a very grateful thanks to Principal, Dr. Kishor S. Wani for providing facilities and excellent infrastructure and special thanks to Dr. Girish K. Patnaik, Head of Department for giving necessary guidance concerning projects implementation and help whenever required. Co-ordination and guidance of the project guide Miss. Sweta Pandey helped in completion of project and provided their helping hand in all technical aspects. Also like to express gratitude towards parents, colleagues and friends for their kind co-operation and encouragement which help in the completion of the project.

Jagruti J. Patil
Prajakta D. Dusane
Ruchita M. Pandya
Urvashi M. Jain

Contents

List of Figures

Abstract

In RSA algorithm the encryption is done using the receivers public key. Since a users public key is available to everyone in the network. RSA provides confidentiality but the main disadvantage of RSA is that there is no authentication i.e anyone can send messages to anyone. In existing work RSA with RGB model is used for providing confidentiality and authentication but with less accuracy. Due to less accuracy existing system is not fully secure. In proposed work AES encryption technique with RGB color is use to increase the accuracy of the system. It will provides both confidentiality, authentication and more privacy to the data(Audio and Text) which is sent across the network.

Chapter 1

Introduction

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful now a days. To ensure secure data transmission there are several techniques being followed. One among them is cryptography which involves encryption and decryption of data. In this system, use RSA algorithm to perform encryption and decryption. To provide authentication between two intended along with security, colors are used. With the help of colors, both sender and receiver will get validated. RSA involves public key and private key where public key can know to everyone and is used for encrypting messages[1]. Messages encrypted using public key can only be decrypted using corresponding private key.

In Section 1.1 background and problems related "Security of Data with RGB Color and AES Encryption techniques" are described. By whom and by which things motivate the project is described in Section 1.2 motivation. In Section 1.3 problem definition of project is described, objectives of project is described in Section 1.4, in Section 1.5 a short description of each chapter is described. Finally, summary is presented in the last Section.

1.1 Background

Many research works have focused on the security of RSA algorithm. This model provides both confidentiality and authentication to the data sent across the network. RSA algorithm uses public key and private key to encrypt and decrypt the data and thus provides confidentiality. But the public key is known to everyone and so anyone can encrypt the data and send the message. Hence authentication of users is needed. But using RGB color model, it provide authentication[2]. Every user will have a unique color assigned to him.

1.2 Motivation

The motivation for proposed solution lies in problem with encryption and decryption. Sometimes in passing the text, data used to get hacked. Messages encrypted using public key can only be decrypted using corresponding private key. In order to counter the common threats to communications, and apply several of the fundamental security services, including authentication, integrity, confidentiality and authorization. A secure data transmission may use all or a combination of these services to achieve the desired security level[4]. So these basic problems in the algorithm must be overcome to make the data communication more secure.

1.3 Problem Defination

With the fast changing technologies today, more and more multimedia data are generated and transmitted, leaving our data vulnerable to be edited, modified and duplicated. In our existing work RSA with RGB color is used for providing confidentiality and authentication to the system. Authentication and confidentiality is maintained but its accuracy is less. Due to less accuracy in existing system data which is send and receive is not fully secure. To over come this problem, in proposed work AES encryption technique with RGB color is use to increase the accuracy of the system and also provide confidentiality as well as authentication. It will provides more privacy to the data (Audio and Text) which is sent across the network.

1.4 Objectives

Main objective of Security with colors using RSA and AES algorithm are listed below[1] :

1. **Authentication** :- The services provide assurance of a participating host identity. Therefore, the availability and distribution of keys should be restricted to only authorize group members according to the policy of trust established for the session. Authentication mechanisms can identify the source of the key material and provide a means to counter various masquerades and replay attacks that may be launched against a secure data transmission.

2. **Integrity** :- It requires the data and control packets originated at an authorized source not to be intercepted or altered while traversing through the network. The possibility of preventing a denial-of-service attack through the transmission of such packets can be minimized or eliminated.

3. **Confidentiality** :- The services are essential in creating a private data transmission session. It should also be applied to key management transactions during the exchange of key material and can be applied to session announcements allowing them to advertise publicly through standard methods while keeping the details of the session private.

4. **Authorization** :- It can be implied to only those entities with specific permission that may use the network to send messages after they have been suitably authenticated.

1.5 Organization of Report

In chapter 1, "Introduction" about Security of Data with RGB Color and AES Encryption techniques in which background, motivation, problem definition, scope, objective and organization of report is described briefly. In chapter 2, "System Analysis" of Security of Data with RGB Color and AES Encryption techniques in which literature survey, proposed system, project scheduling is described briefly. In chapter 3, "System Requirement Specification" of Security of Data with RGB Color and AES Encryption techniques in which hardware requirement, software requirement, functional requirement and non functional requirements is described briefly. In chapter 4, "System Design" of Security of Data with RGB Color and AES Encryption techniques in which architectural design, E-R diagrams, data base design, dataflow diagram and behavioral modeling through UML diagrams is described briefly. In chapter 5, "Conclusion, Limitation and Future Scope" of Security of Data with RGB Color and AES Encryption techniques in which conclusion and future scope is described briefly.

1.6 Summary

In this chapter, "introduction of Security of Data with RGB Color and AES Encryption techniques" is described. In the next chapter methodology is described. In the next chapter "System Analysis" of project is described.

Chapter 2

System Analysis

In analysis of Security of Data with RGB Color and AES Encryption techniques, it includes purpose, requirements and it is able to solve the problem of resume writing. A project which having some literature need to be done which is followed by design proposed system. The proposed system which is feasible or not it must need to be checked. All analyzing parts and things of system and development of dynamic resume builder using Java project are covered by some sections of the chapter.

In Section 2.1, literature survey is done for the proposed solution described. Proposed system of the development of dynamic resume builder using Java project is described in Section 2.2. In Section 2.3, feasibility study of project is described. In Section 2.4, risk analysis of project is described. Finally, summary is presented in the last Section.

2.1 Literature Survey

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful now a days. To ensure secure data transmission there are several techniques being followed. One among them is cryptography which involves encryption and decryption of data. In this system AES algorithm is used to perform encryption and decryption[5]. To provide authentication between two intended along with security, colors are used. With the help of colors, both sender and receiver will get validated. AES involes keys, used for encrypting messages[3].

2.2 Proposed System

There are a lots of hackers who can steal the data using RSA algorithm. Use RGB color model to provide authentication for both sender and receiver. In our existing work RSA with RGB color is used for providing confidentiality and authentication to the system[1]. Authentication and confidentiality is maintained but its accuracy is less. In proposed work

AES encryption technique with RGB color is use to increase the accuracy of the system and also provide confidentiality as well as authentication. It will provides more privacy to the data (Audio and Text) which is sent across the network.

2.3 Feasibility Study

The purpose of the feasibility study is not to solve the problem, but to determine the problem is worth to solving. This helps to decide whether to proceed with project or not[7]. As such, a well-designed feasibility study should provide a historical background of the business or project, description of the product or service, accounting statements, details of the operations and management, marketing research and policies, financial data, legal requirements and tax obligations. Generally, feasibility studies precede technical development and project implementation. It should involves questions such as how much time is available to build this project, when it can be built, whether it interferes with normal operations, type and amount of resources required, dependencies, etc. the project's alternatives are evaluated for their impact on the user also on the viewer. Aims of feasibility study is come under following point-

1. Making sure there is a true market for the project product or a service (supply, Demand).
2. Estimation the market share of the project.
3. Identifying the project product specifications.
4. Estimating the fixed assets needs (web server, Building, System and so on).
5. Estimating manpower of the project.
6. Estimating Working capital of the project.
7. Estimating the expected net income, rate of return on investment, Internal rate of return, payback period, and break-even sales of the project.
8. Estimate net cash flows of the project.

It is the high level capsule version of the entire requirement analysis process. There are few types of feasibility are exist so developer should take care of these feasibility or developer must aware about these feasibility. The objective of feasibility study is to determine whether the proposed system can be developed with available resources.

There are three steps to be followed for determining feasibility study of proposed systems.

1. Technical Feasibility
2. Operational Feasibility
3. Economical Feasibility

2.3.1 Technical Feasibility

It is concerned with hardware and software feasibility. In this study, one has to test whether the proposed system can be developed using existing technology or not. As per client requirements the system to be developed should have speed response because of fast exchange of information, reliability, security, scalability, integration and availability. To meet these requirements. We as a developer found JSP specifications as a right choice because of its features platform independence and reusability.

2.3.2 Operational Feasibility

Operational feasibility determines whether the proposed system satisfied the user objectives and can be fitted in to current system operation. The system Security of Data with RGB Color and AES Encryption techniques can be justified if the proposed system satisfies the user objectives and can be fitted in to current system operation[6]. This system can be justified as operationally feasible based on the following :

1. The methods of processing and presentation are completely acceptable by the users because they meet all their requirements.
2. The users have been involved during the preparation of requirement analysis and design process.
3. The system will certainly satisfy the user objectives and it will also enhance their capability.
4. The system will certainly satisfy the user objectives and it will also enhance their effectively.

2.3.3 Economical Feasibility

This includes an evaluation of all incremental costs and benefits expected if proposed system is implemented. Costs-benefit analysis which is to be done during economical feasibility delineates costs for project development and weighs them against system benefits. The system adds information of colleges and companies for which colleges and companies pays as it provides their information as well as company jobs. So developing this system is economically feasible.

2.4 Risk Analysis

▮ *Introduction of Risk Analysis*

Risk Analysis and management are a series of steps that help a software team to understand and manage uncertainty. As developing Unit converter, if input is given which is out of range, the result may be wrong. Exponential conversion may also sometimes go wrong. The goal of risk assessment is to prioritize the risks so that attention and resources can be focused on the more risky items[8]. Risk identification is the last step in risk assessment, which identifers all the different risks for a particular project. The problems or risks that commonly faced are listed below:-

A Estimation and Scheduling : The unique nature of individual software projects creates problems for developers in estimating and scheduling development time. We should refer existing project experience to overcome this problem.

Sudden growth in requirements : There can be a sudden growth in resources that we have not thought earlier while project planning. This sudden growth can also lead in being late for project completion.

Breakdown of specification : At the initial stage of integration or coding, we felt that requirements and specifications are incomplete or insufficient. As coding got progressed, requirement of specification was fulfilled. These risks are project-dependent and identifying them is an exercise in envisioning what can go wrong. Methods that can aid risk identification include checklists of possible risks, surveys, meetings and brainstorming, and reviews of plans, processes, and work products.

▮ *Components of Risk Analysis*

Everyone involved in the software process managers, software engineers, and customers participate in risk analysis and management.

▮ *Needs of Risk Analysis*

Think about the Boy Scout motto: ”Be prepared” software is a difficult undertaking. Lots of things can go wrong, and frankly, many often do. It’s for a reason which being prepared understanding the risks and taking proactive measures to avoid or manage them-is a key element of good software project management.

Software Risk

Although there has been considerable debate about the proper definition for software risk, there is general agreement of the risk always involves two characteristics:-

1. Uncertainty :- The risk may or may not happen; which is, there are no 100 percent probable risks.

2. Loss :- If the risk becomes a reality, unwanted consequences or loss will occur. When risks are analyzed, it is important to quantify the level of uncertainty and the degree of loss associated with each risk. To accomplish this, different categories of risks are considered.

Project Risks

Threaten the project plan. Which is, if project risks become real, it is likely that project schedule will slip and the costs will increase. Project risks identify potential budgetary, schedule, personnel (staffing and organization), resource, customer, and requirements problems and their impact on a software project. In the project, project risk occurs if requirement of technical member means technical team is unavailable according to the project plan and estimation and if the project is not completed within time then situation project risk can occurs.

Technical Risks

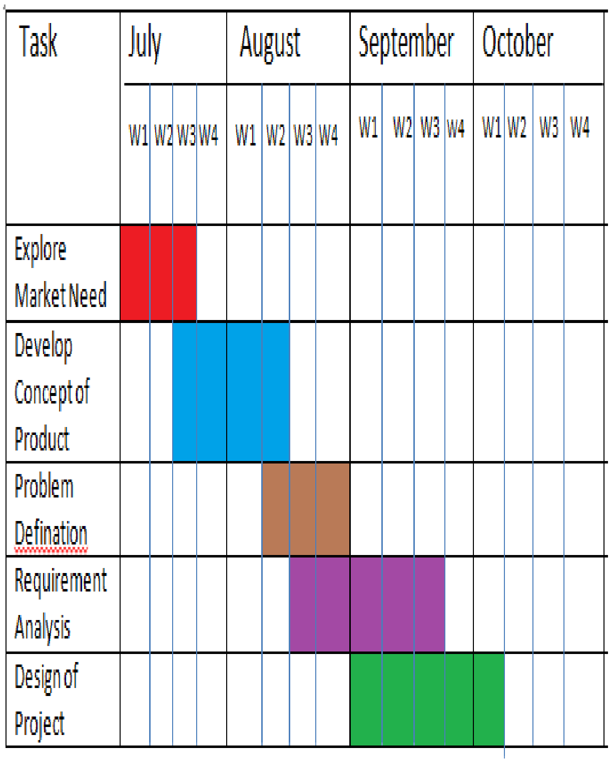
Threaten the quality and timeliness of the software to be produced. If a technical risk becomes a reality, implementation may become difficult or impossible. Technical risks identify potential design, implementation, interface, verification, and maintenance problems. In addition, specification ambiguity, technical uncertainty, technical obsolescence, and ”leading edge” technology are also risk factors. Technical risks occur because the problem is harder to solve than thought it would be. In the project if any module of resume builder is not worked properly according to developer expectation then technical risk may occur.

Business Risks

Threaten the viability of the software to be built. Business risks often jeopardize the project or the product. Candidates for the top five business risks are:-

1. Building a excellent product or system that no one really wants (market risk),
2. Building a product that no longer fits into the overall business strategy for the company (strategic risk).
3. Building a product that the sales force doesn't understand how to sell.
4. Losing the support of senior management due to a change in focus or a change in people (management risk).
5. Losing budgetary or personnel commitment (budget risks). It is extremely important to note that simple categorization won't always work. Some risks are simply unpredictable in advance.

2.5 Project scheduling



Task	July				August				September				October			
	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
Explore Market Need	🟥	🟥	🟥													
Develop Concept of Product			🟦	🟦	🟦	🟦										
Problem Defination						🟫	🟫	🟫								
Requirement Analysis							🟪	🟪	🟪	🟪	🟪					
Design of Project									🟩	🟩	🟩	🟩	🟩			

Figure 2.1: Project scheduling

2.6 Summary

In this chapter, development of the Security of Data with RGB Color and AES Encryption techniques and "analysis of the system" is described in briefly. In next chapter "System Requirement Specification" of project is discussed.

Chapter 3

System Requirement Specification

It provides requirements, needs of project and those things which help to complete project. System requirement describe a system from a technical perspective, which describe the essential characteristics of the hardware and software that will meet those needs. It should specify the capabilities, capacities and characteristics of the system in both qualitative and quantitative terms. In project requirements and its details information measure from specification. In project it requires JVM which are must be available on computer system. Supportive softwares also required in system.

In Section 3.1, hardware requirement and development of Security of Data with RGB Color and AES Encryption techniques is described. Software requirement for development of Security of Data with RGB Color and AES Encryption techniques is described in Section 3.2. Finally, summary is presented in the last Section.

3.1 Hardware Requirements

In the hardware requirement, processor having minimum Intel core i3 or as system configuration which contain may be core i5. The system memory having minimum 2 GB RAM up to depend upon other system configuration. Operating system may having Windows 7, Windows 8 or Linux for softwares which are need to development of project.

3.2 Software Requirements

The software requirements analysis process covers the complex task of eliciting and documenting the requirements of all these users, modeling and analyzing these requirements and documenting of the basis for system design. Development of required software consist Java language in which Jdk1.6, MySQL will be used for simulation purpose.

3.3 Summary

In this chapter, “System Requirement Specification” of the project is described. In the next chapter “System Design” of project is described.

Chapter 4

System Design

Design is an activity concerned with making major decisions, often of a structural nature. It shares with programming a concern for abstracting information representation and processing sequences, but the level of detail is quite different at the extremes. Design builds coherent, well planned representations of programs which are concentrate on the inter relationships of parts at the higher level and the logical operations involved at the lower levels[8].

In Section 4.1 Data flow diagrams are illustrated. In Section 4.2 shows flowchart for RSA with RGB model is illustrated. In Section 4.3 shows behavioral model of the system and it describe through UML diagram. Finally, summary is presented in the last Section.

4.1 DFD diagrams

Data flow diagram (DFD), also called as 'Bubble chart is a graphical technique, which is used to represent information flow, and transformers those are applied when data moves from input to output. In figure 4.1 data flow diagram at level 0 is illustrated. In figure 4.2 data flow diagram at level 1 is illustrated. In figure 4.3 data flow diagram at level 2 is illustrated.

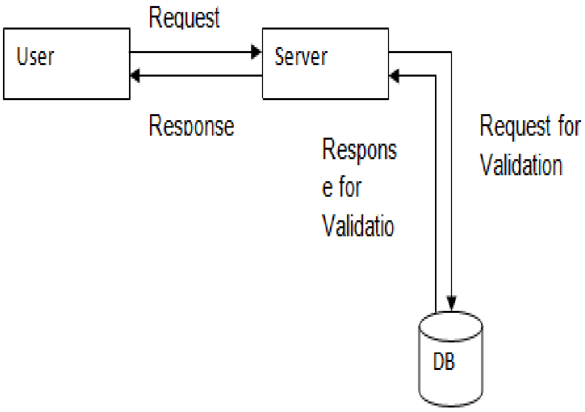


Figure 4.1: DFD level0

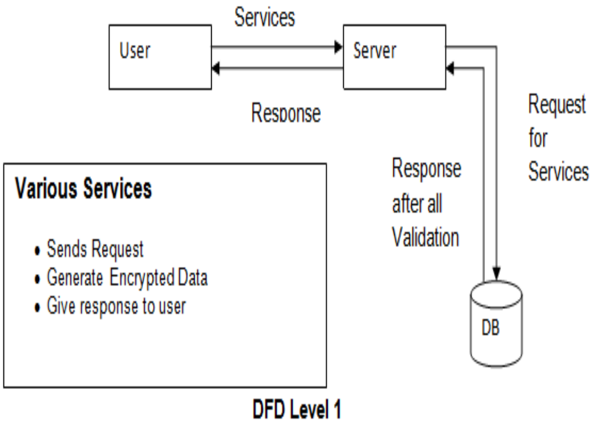


Figure 4.2: DFD level1

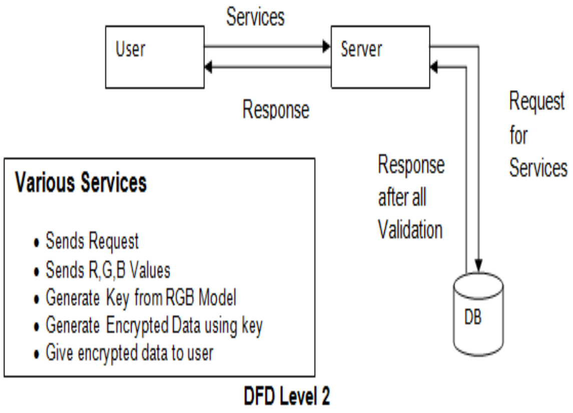


Figure 4.3: DFD level2

4.2 Flowchart

Figure 4.4 shows flowchart for RSA algorithm working with RGB color model in which sender passes input(data) which is encrypted using RSA algorithm with RGB color model. After encrypting, receiver will decrypt message using keys, but for decryption of data authentication is required. Key generation:-

1. Generate two distinct prime numbers p and q.
2. Find n such that n=p*q, n will be used as modulus for both public and private keys.
3. Find the Euler totient of n, f(n) f(n) = (p-1)*(q-1)
4. Choose e such that 1 is less than e is less than f(n), and such that e and f(n) share no divisors other than n(e and f(n) are relatively prime). e is kept as the public key exponent.

5. Determine d (using modular arithmetic) which satisfies the congruence relation de = 1 (mod f(n)).

6. Public key is (e, n).

7. Private key is (d, n).

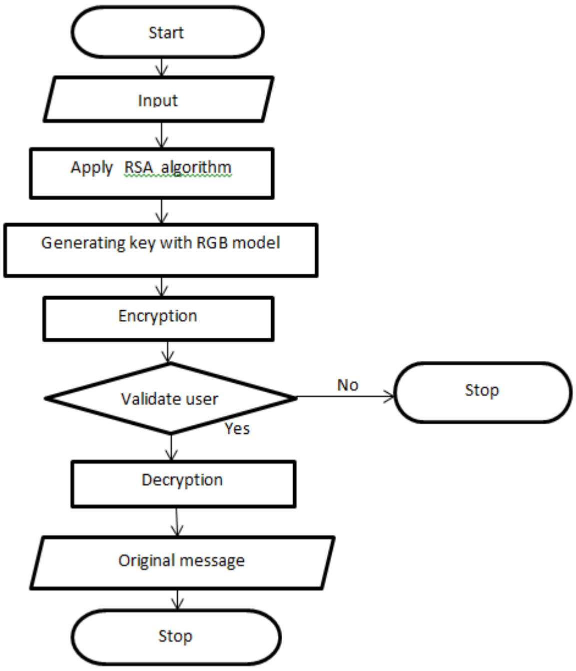


Figure 4.4: Flowchart for RSA with RGB model

Figure 4.5 shows flowchart for AES algorithm working with RGB color model in which sender passes input(data) which is encrypted using AES algorithm with RGB color model. After encrypting, receiver will decrypt message using keys, but for decryption of data authentication is required and AES provide more security for transmission of data.

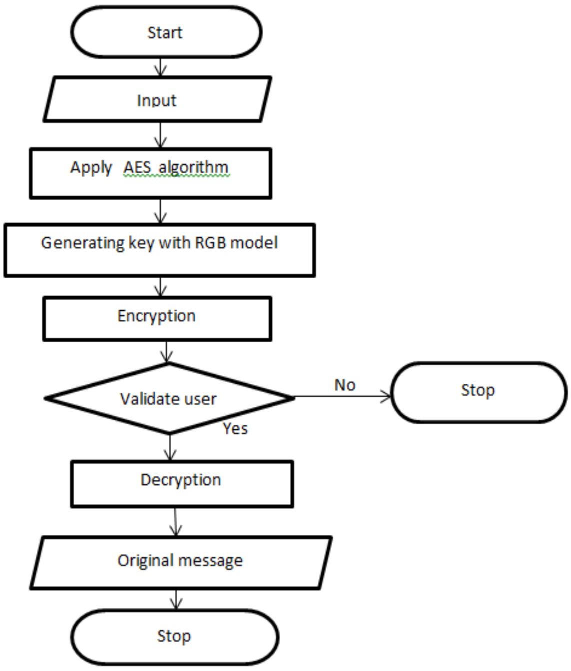


Figure 4.5: Flowchart for AES with RGB model

4.3 Behavioral Modeling through UML Diagrams

In section, the uml diagrams for the proposed solution are listed and explained. The uml diagrams depict the modeling of the proposed solution and helps us to understand the structure of the entire software[7].

4.3.1 Use Case Diagram

A use case diagram[8] for Security of Data with RGB Color and AES Encryption techniques consisting an actors named User and Database Administrator, which performs different activities like Receive Data and RGB Values, Send Data and Query Validation as shown in Fig 4.6.

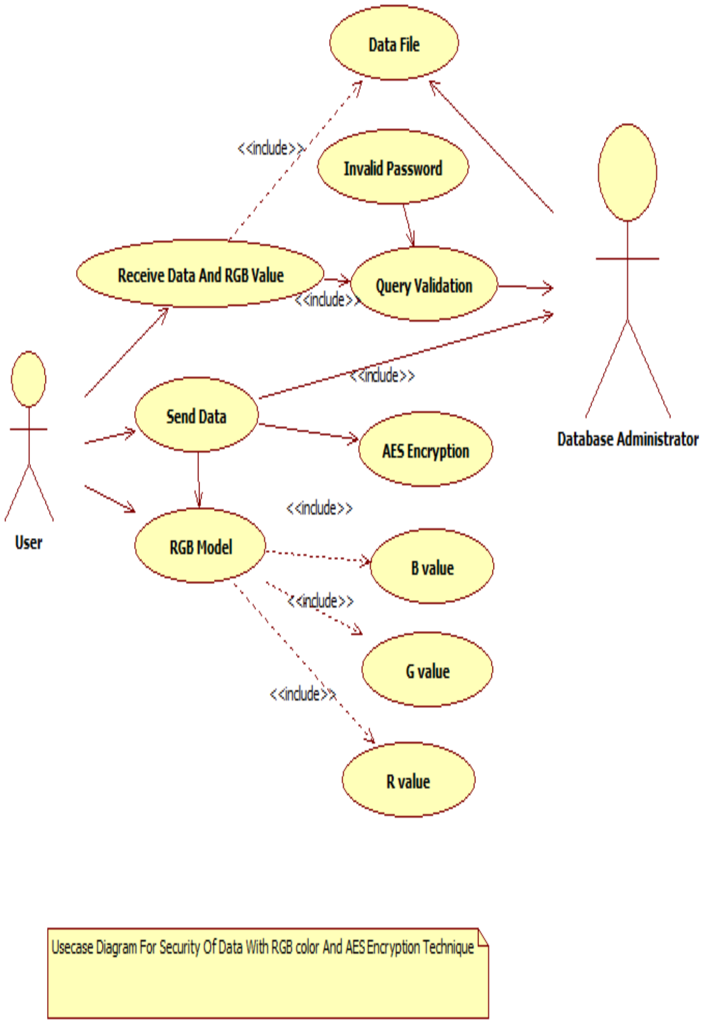


Figure 4.6: UseCase Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.2 Class Diagram

A class diagram[8] for Security of Data with RGB Color and AES Encryption techniques which consist multiple classes such as User, Save image, Receive image and Key In preview class mentioned some attributes such as Data, type, time, name, message, audio file and performed certain operations such as create, update, delete, save, close, get audio, view, get file, get audio. These are all classes as shown in Fig 4.7.

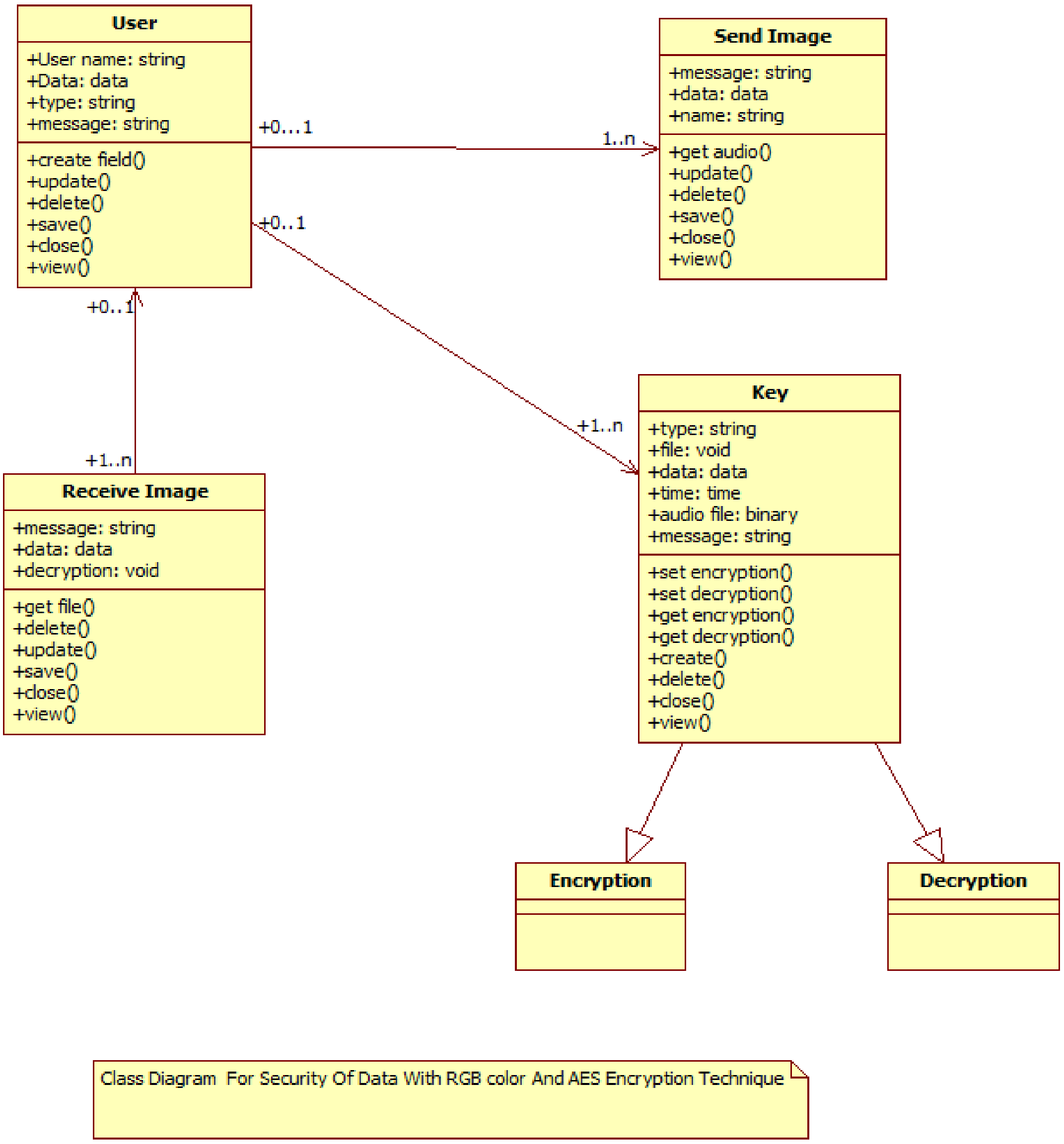


Figure 4.7: Class Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.3 Sequence Diagram

A Sequence diagram[8] is a structured representation of behavior as a series of sequential steps over time. It is used to depict workflow, message passing and how element in general cooperate over time to achieve a result. It is primarily used to show the interaction between objects in the sequential order that those interaction occurs. The sequence flow as shown in Fig 4.8.

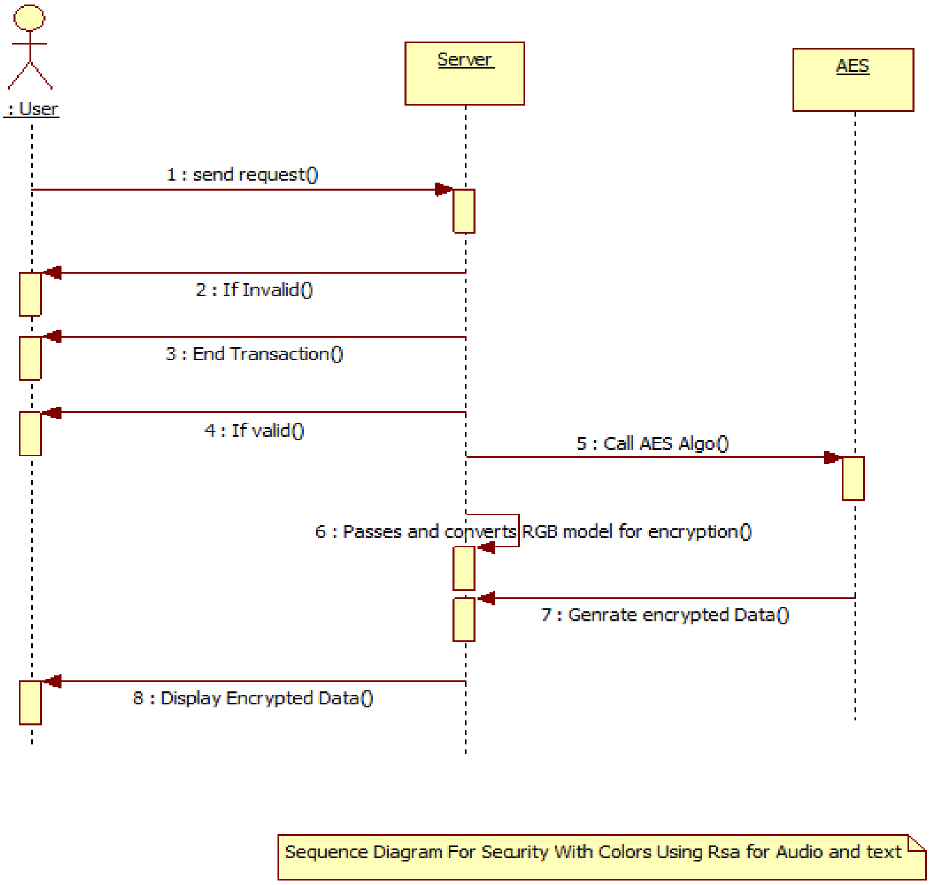

: User
Server
AES
1 : send request()
2 : If Invalid()
3 : End Transaction()
4 : If valid()
5 : Call AES Algo()
6 : Passes and converts RGB model for encryption()
7 : Genrate encrypted Data()
8 : Display Encrypted Data()
Sequence Diagram For Seaurity With Colors Using Rsa for Audio and text

Figure 4.8: Sequence Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.4 State Transition Diagram

State transition diagram[8] for Security of Data with RGB Color and AES Encryption techniques which provides a way to model various states in which the object is exists. They are used to model more dynamic behavior of system. The diagram shows the behavior of an object. A condition enclosed in square box is called as 'Guard' condition. Black dot indicates start point and black dot with circle indicates stop i.e. terminate state. In the state transition diagram etc. various states are illustrated in Fig 4.9.

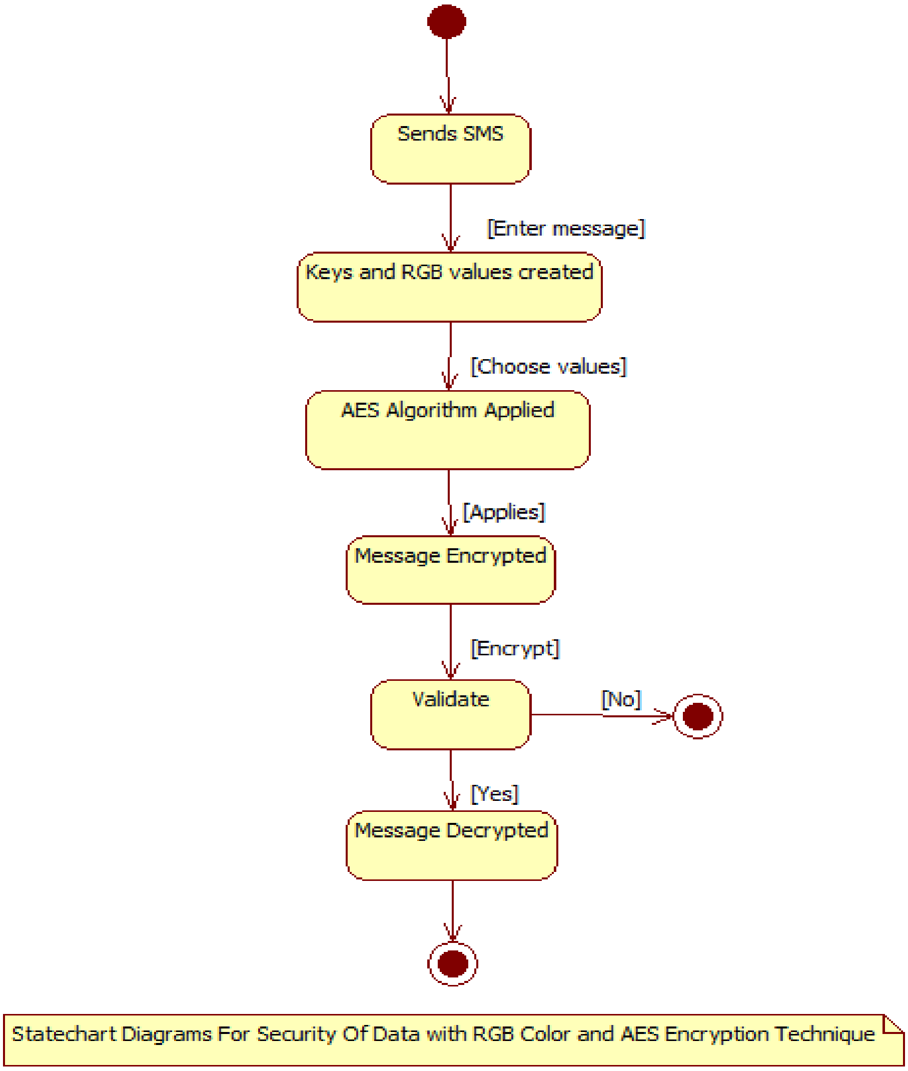


Figure 4.9: Activity Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.5 Activity Diagram

Activity diagram[8] for Security of Data with RGB Color and AES Encryption techniques which provide a way to model various states and one more addition is decision making in states (initial and final states) in which the object is exists. The diagram is used to express dynamic behavior of system. The diagram shows the behavior of an object. A condition enclosed in square box is called as "Guard" condition. A diamond shape is called "Decision Making" condition. Black dot indicates start point and black dot with circle indicates stop i.e. terminate state. In a activity diagram contains Send SMS, Register account online, furnish details, submit, enter data and RGB value, generate key using RGB value, RSA algorithm, AES algorithm, Response to user. It is shown as in Fig 4.10.

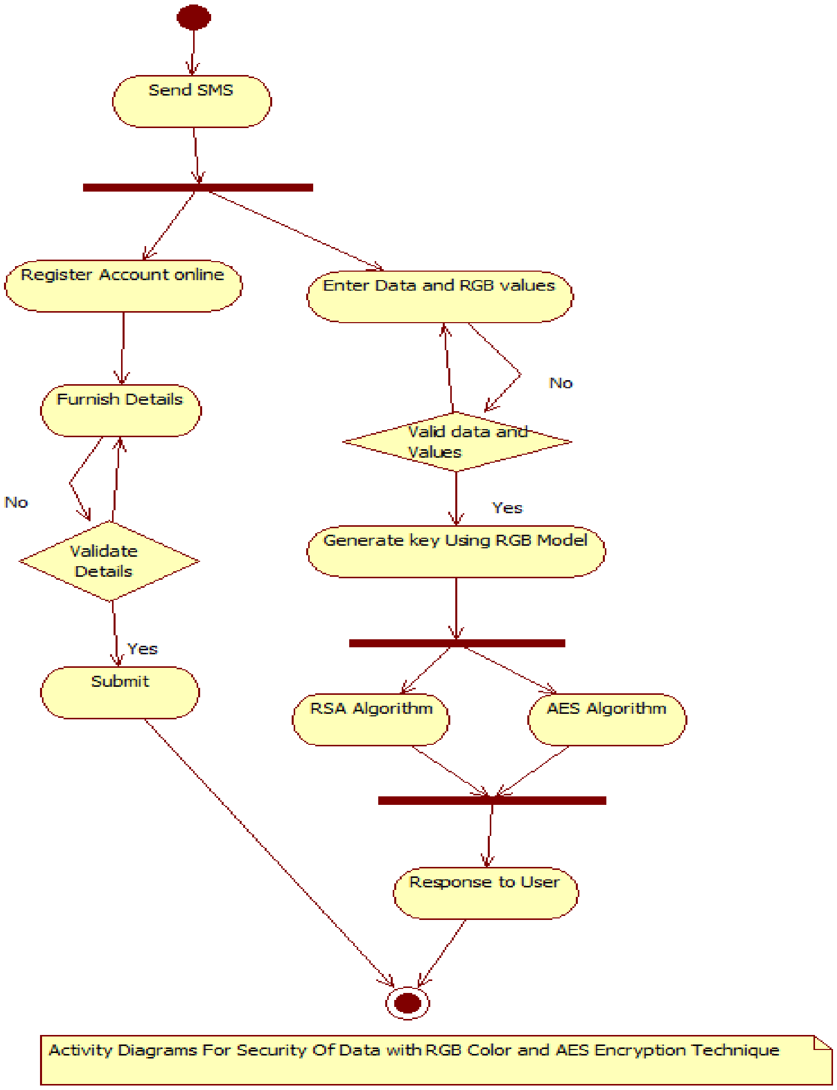


Figure 4.10: Activity Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.6 Component Diagram

Component diagrams[8] are used to represent the implementation view of a system. They represent various components of the system and their relationships as shown in Fig 4.11. Component Diagram describes the physical component.

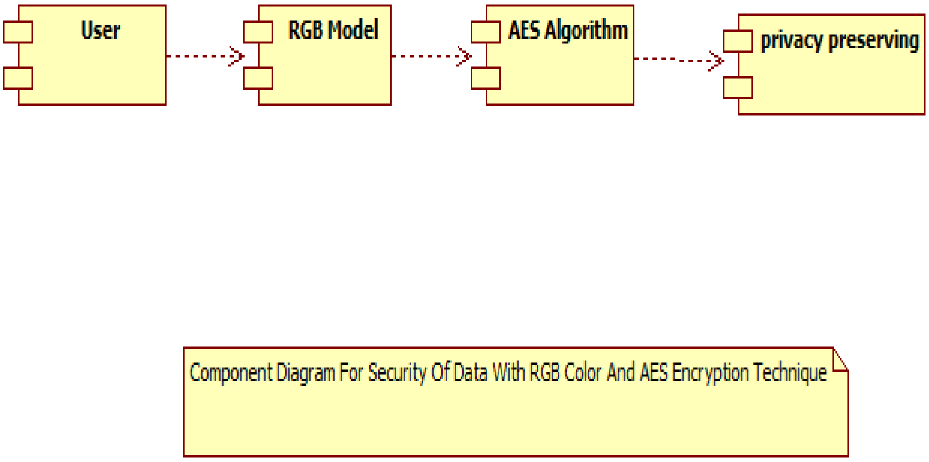

User
RGB Model
AES Algorithm
privacy preserving
Component Diagram For Security Of Data With RGB Color And AES Encryption Technique

Figure 4.11: Component Diagram for Security of Data with RGB Color and AES Encryption techniques

4.3.7 Deployment Diagram

Deployment diagram[8] for Security of Data with RGB Color and AES Encryption techniques which shows the physical structure of system. By using diagram user can easily understand the physical layout of system. Deployment diagram contain nodes like Caching Server, Server1, Server2 and Server3. Deployment of a system as shown in Fig 4.12.

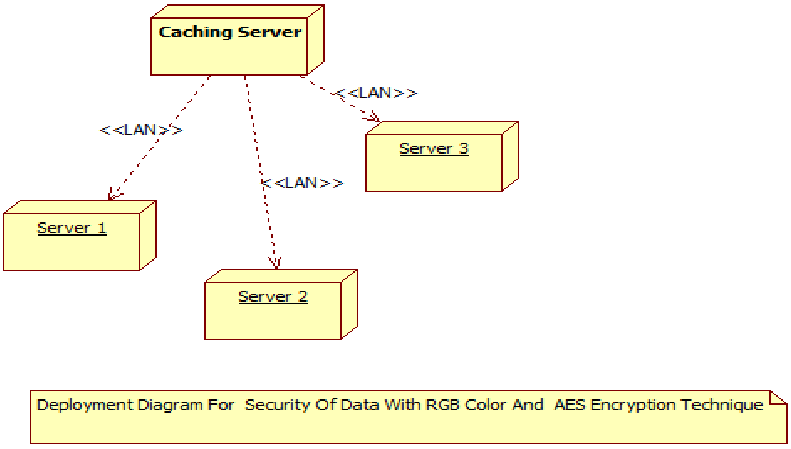

Caching Server
<<LAN>>
<<LAN>>
<<LAN>>
Server 3
Server 1
Server 2
Deployment Diagram For Security Of Data With RGB Color And AES Encryption Technique

Figure 4.12: Deployment Diagram for Security of Data with RGB Color and AES Encryption techniques

4.4 Summary

In this chapter, “System Design” is described is described. In next chapter “Conclusion” of project is concluded as well as future work also forecasted.

Chapter 5

Conclusion

AES encryption technique is used with RGB Color model to provide security. The confidential areas like military, governments are targeted by the system where data security have more importance. Colors, AES are the two main factors in proposed system which makes sure that there is secured message or data transmission and also it is available to authorized person. Hence in the proposed system we provide both authentication and confidentiality with more accuracy.

Bibliography

[1] G. Sankara Rao et al. “Data Security With Colors Using RSA”, Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 9(Version 3), September 2014, pp.95-99.

[2] Nentawe Y. Goshwe “Data Encryption and Decryption Using RSA Algorithm in a Network Environment” IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.

[3] Prof. Manoj Dhande, Akshaya Sawant, Nidhi Pandey, Pooja Sahu, “Secure Data Communication using AES Algorithm, Palindrome Number and Color Code”, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 4 IJRITCC April 2016.

[4] M.Renuga Devi, S.Christobel Diana, “Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers”, International Conference on Computing and Control Engineering(ICCCE 2012), 12 and 13 April, 2012.

[5] AbdulkarimAmerShtewi, BahaaEldin M. Hasan, Abd El fatah, A. Hegazy, “An Efficient Modified Advanced Encryption Standard (AES) Adapted for Image Cryptosystems”, International Journal of Computer Science and Network Srecurity, Vol. 10, No. 2, 2010, pp. 226-232.

[6] Zhang Zhao, Sun Shiliang, “Image Encryption Algorithm Based on Logistic Chaotic System and S-Box Scrambling”, International Congress on Image and Signal Processing, IEEE, 2011, pp. 171-181.

[7] Roger Pressman, “Software Engineering: A Practioner’s Approach”, McGraw-Hill, Seventh Edition, pp.449-490. ISBN-10: 0073375977 ISBN-13:978-007337597, retrieved 2 September, 2016.

[8] Grady Booch, James Rumbaugh, Ivar Jacobson, “The Unified Modeling Language User Guide”, Pearson, Second Edition, 2005, pp. 225-284. ISBN: 978-03-2126-79-79, retrieved 5 September, 2016.