CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

A Technique to Combine Different Cryptographic Algorithms on Basis of their Metrics and Content to be Encrypted

by

Mudassar Nazir

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2019

CERTIFICATE OF APPROVAL

A Technique to Combine Different Cryptographic Algorithms on Basis of their Metrics and Content to be Encrypted

by

Mudassar Nazir

(MCS173014)

PROJECT EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	Internal Examiner	Zeeshan Qaiser	CUST, Islamabad
(b)	Supervisor	Mr. Qamar Mahmood	CUST, Islamabad

Mr. Qamar Mahmood
Project Supervisor
October, 2019

Dr. Nayyer Masood
Head
Dept. of Computer Science
October, 2019

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
October, 2019

Author's Declaration

I, **Mudassar Nazir** hereby state that my MS project titled "**A Technique to Combine Different Cryptographic Algorithms on Basis of their Metrics and Content to be Encrypted**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Mudassar Nazir)

Registration No: MCS173014

Plagiarism Undertaking

I solemnly declare that research work presented in this project titled "***A Technique to Combine Different Cryptographic Algorithms on Basis of their Metrics and Content to be Encrypted***" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that complete project has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled project declare that no portion of my project has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled project even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Mudassar Nazir)

Registration No: MCS173014

Acknowledgements

I would like to dedicate this project to my parents and teachers because of whom I was able to do it. I would like to specially thanks my supervisor **Mr. Qamar Mahmood** for encouraging and helped me whenever needed and he was always there for any kind of support. I would also like to thanks my friends and family for encouraging me and motivating me for completion of this project.

(Mudassar Nazir)

Registration No: MCS173014

Abstract

Most of the researchers have worked in the field of cryptography to finding out the cryptographic algorithms that provide more security for the data. Many authors have combined different cryptographic algorithms to find out better algorithms for encryption and decryption. We have found that their main focus was only on the algorithms parameters like block size and key size, security and cipher type. They were not considering data content parameters like data nature and data length and data type. In this project, we proposed a rule-based approach that will consider both data content and algorithm parameters for evaluating the algorithms. After performing a comprehensive literature analysis of more than 15 research papers, it was accessed that these research works were missing the data content parameters for evaluation of cryptography algorithms. Considering this viewpoint we proposed our framework that will complete the missing factor. We evaluated our framework on different sizes of text and images files. The results produced by the proposed framework are compared with the existing techniques. This comparison revealed that the proposed framework provides the best solution for encryption and decryption. Hence it can perform the best evaluation of cryptographic algorithms.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advance Encryption Standard
CBC	Cipher Block Chaining
DES	Data Encryption Standard
RC4	Rivest Cipher 4
RSA	Rivest Shamir Adleman
3DES	Triple Data Encryption Standard

Chapter 1

Introduction

Cryptography is the art of protecting information with the process of converting plain text message into unreadable form. It is a method of transmitting information in such form so that only those for whom it is intended can read. Cryptography not only protects data from an unauthorized person, but it also ensures the confidentiality, integrity, non-repudiation, and authentication [1]. Encryption and decryption are the functions of cryptography. In encryption, a simple plaintext is converted into unreadable form which is also called ciphertext while in decryption, a ciphertext is converted into readable form which is called plaintext. Nowadays security is the biggest concern everyone's life. Therefore, the use of cryptography has extended in almost every field of life. Till now, there are many ciphers available for the protection of data.

Cryptography has two general types i.e. Symmetric key cryptography and Asymmetric cryptography [2]. In symmetric-key cryptography, both sender and receiver have the same key for encryption and decryption of the message. The main advantage of the symmetric key is fast speed and high security. The disadvantage of this technique is that the key should be transmitted to the receiving end before the actual message is transmitted. Asymmetric encryption is also called public-key cryptography. Asymmetric encryption uses two keys for encryption as well as decryption that is public key and private key [3]. A public key is available to anyone and the private key is the secret key. In asymmetric encryption there is no

need for exchanging keys and the main advantage of public-key cryptography is that private keys never need to be transmitted. It also provides digital signatures using public and private key. The disadvantage of asymmetric encryption is speed because it takes a lot of time for encryption and decryption.

Till date, multiple approaches have been proposed by researchers based on cryptography techniques. They have implemented different techniques related to symmetric and asymmetric algorithms. All the research which have been done for cryptography, the researchers have tried to combine different algorithms based on different parameters such as block size, key size, the performance of algorithm and security. For example in [8], authors have combined different algorithm together and proposed a system to secure the plaintext as well as key. In [10], authors have discussed the limitation of the different cryptographic algorithm. They have used different parameters like key exchange, flexibility and security. In [11], authors have provided the performance evaluation of different cryptographic algorithms using different parameters like battery power consumption, block size, and encryption/decryption speed. Several other researchers have combined different cryptographic algorithms together based on different parameters such as key size,block size, performance measures, battery consumptions, and security. They have tried to find out the better cryptographic algorithm, however, they have not considered the content of plaintext for the selection of cryptographic algorithms.

Based on this motivation, we proposed a framework in which based on the content of plaintext and algorithm metrics we will check which encryption algorithm should be used. Content of plaintext includes the textual and image data while algorithm metrics contains certain parameters which include key size, block size, security, and cipher type. We will also define the rules such as we may check the length of the data, data nature like data contains alphanumeric data or it contains special characters, data type such as textual or image, data content like file contains online data or offline data, security, and performance of the algorithm. Based on the rules cryptographic algorithm selection will be performed and the data will be encrypted.

In the second chapter, we will discuss the comprehensive literature in the field of cryptography to find out the merits and demerits due to which we are proposing our technique. In the third chapter, we will discuss our methodology and the steps which are involved in our technique. In the 4th chapter, we will discuss the results and the experimental setup. We will compare the results of the proposed technique with the existing technique to find out the better technique among them. In the last chapter, we will conclude our report and we will discuss the future work and enhancements which we will make further.

1.1 Purpose

The purpose of this project is to make the comprehensive framework which is capable to decide encryption algorithm based on the content of plaintext and algorithm metrics. This framework will not use any machine learning technique. However, we are considering some parameters like block size, key size, cipher type, security. and based on the content of plaintext we will define rules which will ensure to select the better algorithm for encryption and decryption.

1.2 Problem Statement

State-of-the-art cryptographic techniques are focusing on combining different cryptographic algorithms together based on certain parameters to find out the best algorithm. However, there is a lack of technique that considered both cryptographic algorithms parameters and data content parameters for evaluation of cryptographic algorithms.

1.3 Scope

In this research, we propose a framework which will give us a better cryptographic algorithm for encryption/decryption based on the algorithm metrics and rules. Algorithm metrics contains different parameters like block size, key size, cipher type, and security while rules are defined to select the algorithms based on different criteria. For example, if data is of online nature than we will consider the RC4 algorithm likewise if data is offline nature than we will consider some other parameters like block size, key size, security [9] and some data content parameters like data size and data type. After that based on these parameters we will select the best possible cryptographic algorithms. The algorithms selection will be made from both Symmetric and Asymmetric techniques.

1.4 Significance of the Solution

The proposed framework considers the content of plaintext [4] which includes textual and image data. This framework also considers algorithms metrics which contains different parameters of a cryptographic algorithm such as block size, key size, cipher type, and security. This framework will not use any kind of machine learning technique. However, based on rules our framework will select the best possible cryptographic algorithms for encryption and decryption. This framework will not restrict to select one specific algorithm but it will automatically select the best possible algorithm based on data and algorithm parameters.

Chapter 2

Literature Review

There are many approaches proposed by the researchers in the past to combined different cryptographic algorithms together to build a mechanism for finding out the best possible algorithms in terms of block size, key size, and many more parameters. This section provides a comprehensive literature review of the research conducted in this area and provides a critical review of all the proposed approaches. We have divided this chapter into different sections, Section 2.1 shows the related work and Section 2.2 shows the conclusions of the literature review.

2.1 Related Work

Lina Gonga et al. [8] proposed a hybrid technique for encryption and decryption. They have used the 3DES algorithm for plaintext encryption and they have used the RSA algorithm for encrypting the keys. In this paper Firstly, sender uses the DES algorithm for encrypting the plaintext with the symmetric key and then encrypts the symmetric key using the RSA algorithm, after encrypting the plaintext and key sender transfer this to the network for receiver, after receiving the ciphertext information receiver decrypt the key with its own key to obtain the DES key and then decrypts the ciphertext using the key and obtains the plaintext.

Zoran et al. [10] discuss the implementation limitations of cryptography algorithms in which DES, 3DES, CAST-128, Blowfish, IDEA, AES, and RC6 of symmetric technique and RSA of the asymmetric technique. They discussed different parameters such as key exchange, flexibility and security issues of these algorithms. These parameters are major issue of concern in any encryption algorithm. In 1st case, comparison is performed among symmetric algorithms. It is concluded that RC6, Blowfish and AES are secured and efficient based on high security and fewer limitations. In 2nd case comparison performs among symmetric and asymmetric keys and it is concluded that RSA is more efficient than any symmetric algorithm.

Diaa Salama et al. [11] provide the performance evaluation of six algorithms: AES, DES, 3DES, RC2, Blowfish, and RC6. They have performed the comparisons for each algorithm such as data types, different size of a data block, battery power consumption, different key size, and encryption/decryption speed. Following results are shown. There is no significant difference when the results are displayed either in hexadecimal base encoding or base 64 encodings. In case of changing packet size, it was found that RC6 requires less time as compared to other algorithms except Blowfish. When changing datatype such as images instead of text, they found RC2, RC6 and Blowfish have disadvantages over other algorithms in term of time consumption. 3DES still has low performance compare to DES algorithm. In case of changing key size which is only possible in AES and RC6 algorithm higher key size lead to clear change in the battery and time consumption.

Agrawal et al. [12] implement most widely used symmetric encryption technique that is DES, 3DES, AES, Blowfish, and RC4 using MATLAB Software. These techniques are also compared after implementation. These points give the indication of the avalanche effect due to one-bit variation in plaintext. The result shows that the avalanche effect is highest in AES, medium in DES, 3DES and Blowfish whereas smallest in RC4. AES is best option if one desires good avalanche.

Alanazi et al. [13] have done the comparative analysis of three cryptographic algorithms that are DES, 3DES, and AES. They have considered certain parameters such as key length, block size, security, possible keys, possible ASCII printable

character keys and time require for checking all possible keys at 50 billion keys per second. Study shows that AES is better than DES and 3DES.

Nidhi Singhal et al. [14] has done the comparative analysis of AES and RC4 for better utilization. They have done the experiments on a laptop 2.99 GHz CPU and 2GB RAM. The laptop encrypts different file sizes ranger from 100Kb to 50MB. They have used different parameters to find a better algorithm based on performance metrics Encryption/ Decryption time, Throughput, CPU Process time and Memory Utilization. Their experiment shows that RC4 is fast and energy-efficient for encryption and decryption and based on their research RC4 is better than AES.

Jawahar Thakur et al. [15] has done the analysis of DES, AES, and Blowfish for finding our the best algorithm from these three in terms of performance. They have conducted the analysis by running several encryptions setting to process different sizes of data to evaluate the algorithms speed. They have retrieved the data from different text files to calculate the time consumed by the algorithms to process the data. Their results showed that blowfish has better performance than the other two algorithms. AES showed poor performance than other algorithms since it requires more processing power.

Anand Kumar et al. [16] have performed the performance evaluation of AES and Blowfish algorithm. They have used different algorithm parameters like key size, block size and security. They have used different experimental procedures like different encryption and decryption encodings techniques such as base64 and hexadecimal. They have used a different packet size of data ranging from 0.5MB to 20MB. They have used different data types such as documents and images. Their experimental results show that Blowfish has better performance than AES. Their results also show that Blowfish is good for textbase encryption whereas AES is better for Images encryption. They have examined that AES can be used when there is a need for high security and in case of performance aspects, Blowfish can be used.

Singhal et al. [17] have performed a comparative analysis of AES and RC4 algorithms for better utilization. They have used different performance metrics to evaluate the results. Performance metrics which they have used in their techniques are encryption/decryption time, throughput, CPU process time and memory utilization. Their experimental results show that RC4 is fast and energy-efficient for encryption and decryption. Based on their performance metrics results they have concluded that RC4 is better than AES.

Seth et al. [18] have performed the comparative analysis of AES, DES, and RSA. They have used different parameters such as computation time and memory usage. Their experimental result shows that DES Algorithm consumes least encryption time than AES and AES algorithm has least memory usage than DES. RSA consumes more time than AES and DES and memory usage is also very high.

Abdul. Elminaam et al. [19] have performed the evaluation of six of the most common encryption algorithms which are DES, AES, 3DES, Blowfish, and RC6, RC2. They have used different parameters for evaluation of results such as different sizes of data blocks, different data types, battery power consumption, different key size, and encryption/decryption speed. Experimental results show that RC6 requires less time than all algorithms except Blowfish. In the case of changing data type such as image instead of text, it was found that RC6, RC2, and Blowfish has a disadvantage over other algorithms in terms of time consumption. 3DES still has low performance as compared to DES algorithm. In case of key size it can be seen that higher key size leads to change in the battery and time consumption.

Md. Alam Hossain et al. [20] have performed the analysis of different cryptographic algorithms which are symmetric and asymmetric algorithms. They have described different cryptographic parameters like key length, block size of symmetric and asymmetric algorithms. They have performed the evaluation on Intel core i5 fourth-generation processor with 4GB Ram. They have used different text files as input. Their evaluation results show that AES consumes less encryption time than RSA. Their results also show that AES is better than DES and RSA.

Rihan et al. [21] have performed the performance comparisons of AES and DES. They have performed the performance evaluation in terms of processing time, CPU Usage and encryption throughput. They have performed their analysis on two different platforms, A laptop core i5 and 2.5 GHz with operating system windows 7. The other platform they have used is Apple mac book inter-core i5 with mac operating system. Their experimental result shows that AES is faster than DES in terms of execution time. AES has also high throughput and DES consumes less CPU than AES.

Sombir et al. [22] have performed the analysis of DES and RSA algorithms. They have used different features for the evaluation of algorithms that are the speed of encryption and decryption for input text files. They have different sizes of file as an input to measure the encryption and decryption time. They have discovered that DES consumes less time as compared to RSA algorithms for encryption and decryption. They have figured out that performance of DES is better as compared to the RSA.

Abdullah Al Hasib et al. [23] have performed the comparative analysis of performance and security issues of AES and RSA. Their main focus was to discuss the basic encryption and decryption method and to discuss the mathematical and security aspects. Their experimental results show that AES provides better security and its implementation is easy as compared to RSA, however they considered key distribution is critical for AES like other symmetric encryption algorithm. As RSA is asymmetric cryptographic algorithm so it solves this issue but the major drawback of RSA is its greater computation cost because of a large key.

Aamer Nadeem et al. [24] have performed the performance comparisons of the DES, Triple DES, AES and BLOWFISH algorithms. They have used different file formats and sizes as input data. They have implemented all four cryptographic algorithms using java language. They have compared the results using two different hardware platform to compares the results. Their experimental result shows that Blowfish is the fastest algorithms but only in terms of performance. They have ignored the security issues while their experiments.

2.2 Synopsis

From the analysis of literature, it has been observed that all the techniques are trying to combine different algorithms for evaluation of better algorithms in terms of security and performance. All the techniques which we have discussed are trying to compare different algorithms to find a better solution for encryption and decryption. Most of the techniques have used different parameters of the cryptographic algorithms for evaluating their performance. Few of the techniques used different file sizes as an input to evaluate the time consumption of cryptographic techniques. Few of them used different hardware to compare the results, however, we have discovered that researchers have not focused on the content of the data while evaluating the algorithms for encryption and decryption.

From the research which has already been done, we have discovered that their focus was only on the different parameters of cryptographic algorithms. One of the parameters which have figured out that they were missing is the data content. They were not considering the parameters of data content for evaluation of the cryptographic algorithms. Therefore, we are proposing a technique in which we will take the data content parameters such as data nature, data type, data size and also we will check the data is online nature or offline nature. We will also take the algorithm metrics that include block size, key size, performance measure, and security. Based on the rules this framework will provide us the better possible cryptographic algorithms for encryption and decryption.

Chapter 3

Methodology

In this chapter, we will discuss our proposed framework. This framework focuses on protecting the information of the users. In this research work, we have developed a framework which selects the cryptographic algorithms dynamically while considering the data nature, data type and some other important parameters which we will discuss further in this chapter. We developed this framework for client/server model [25] for securing the data that needs to be transmitted over the network. We have divided this chapter into different sections. Section 3.1 describes the Sender, Section 3.2 describes the Receiver, Section 3.3 describes the Algorithm Selection, Section 3.4 describes the Rule-based approach and Section 3.5 describes the conclusion of this chapter.

We have done a comprehensive literature review to identify the merits and demerits of existing cryptographic techniques. We have developed a rule-based approach [26] which requires less human effort and it can be made easily using a small dataset. This approach consists of two phases (1) Encryption and (2) Decryption.

In the encryption process, this approach the consists of four phases: (1) Check data type and data nature, (2) Apply Rules on data, (3) Select Cryptographic Algorithm, (4) Perform Encryption. These phases provide the encrypted messages as well as code which is concatenated with the encrypted message. The concatenated code contains the information of rule which is used to select the algorithms and

data nature. This code is concatenated with the encrypted message so that when it will reach the destination end, the receiver can get to know the information of how the message was encrypted and what was the rules behind the selection of algorithms. The decryption process of this approach consists of three different phases: (1) Separate Message and Code, (2) Select Cryptographic Algorithm and (3) Perform Decryption. In the first phase our framework separates the code and message that needs to be decrypted. In the second phase it will find out the algorithms through which the encryption was performed with the help of code and in the last phase we get the plaintext.

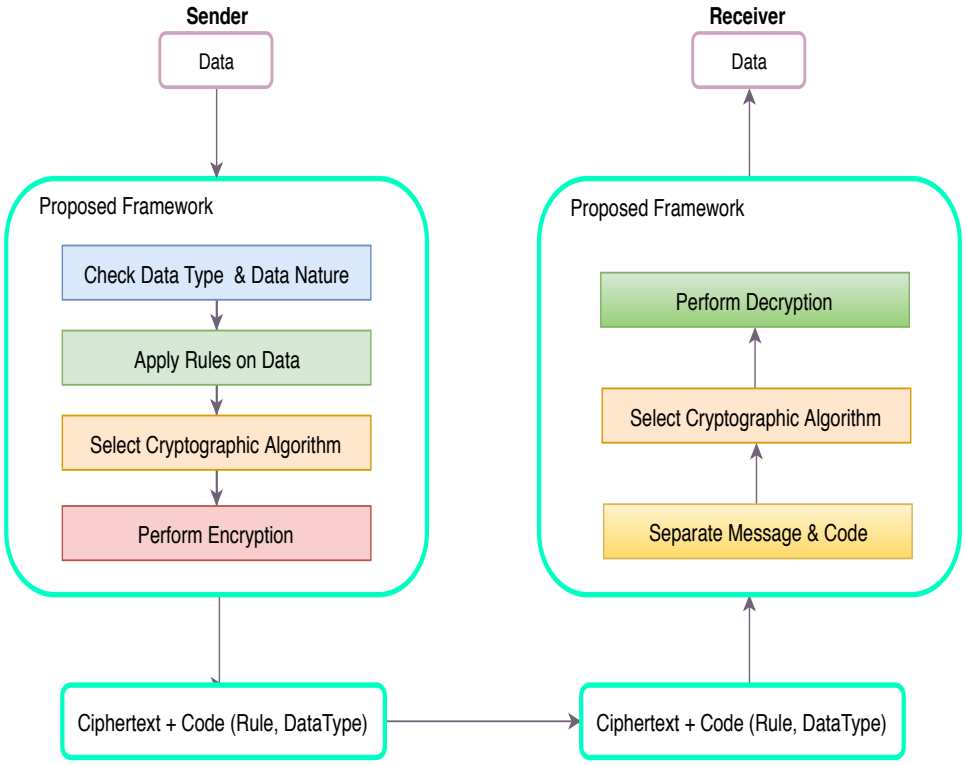

FIGURE 3.1: Architecture diagram of methodology.

3.1 Sender

This is the first phase of our proposed framework in which sender pass the data to our framework for encryption. Our framework process the data in different steps. In the first step, it checks the data type like String, Number, and Image than it checks the data nature like data contains the only number, alphanumeric

or it contains some special characters. In the second step, we apply the rules on data which we have defined. Based on the rules cryptographic algorithm selection is performed. After selecting the algorithms our framework performs the encryption and generate the ciphertext and after that a specific code is attached with ciphertext generated by the algorithm. This code contains all information regarding algorithm selection rule and data type which helps at the receiver side for selection of algorithm. Figure 3.2 indicates the complete flow of the encryption process.

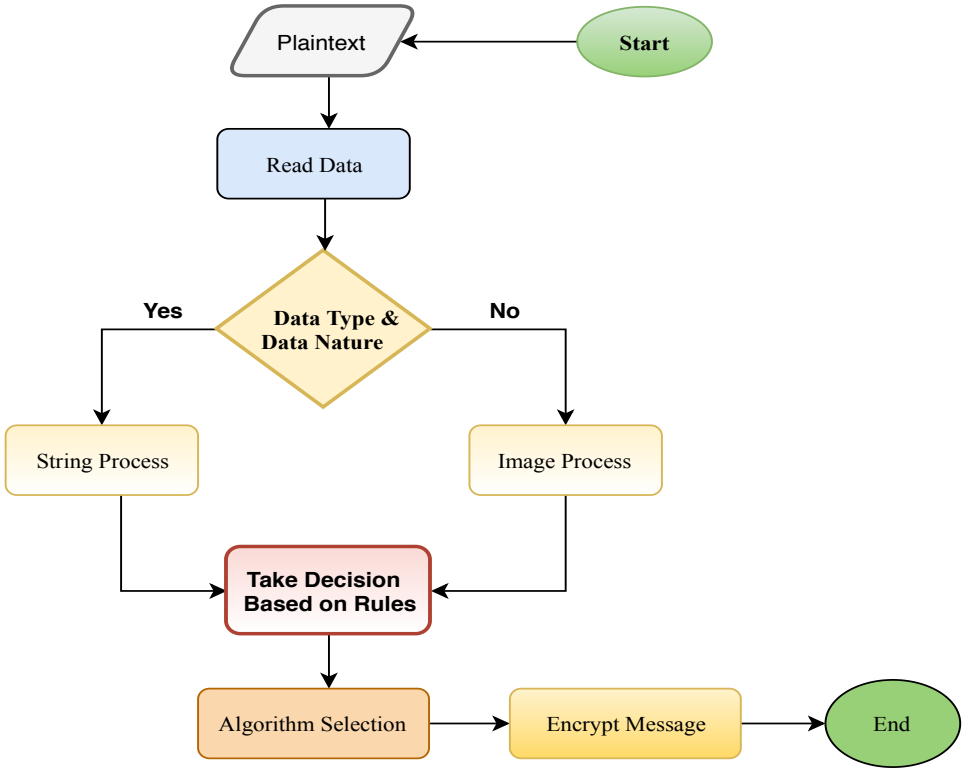

FIGURE 3.2: Encryption Diagram.

3.2 Receiver

This is the second phase of our proposed framework in which receiver pass the data to our framework for decryption. Our framework process the data in different steps. In this first step, it separates the code and the encrypted message so we get the information about how the rules are applied at the sender side for encryption. In the next phase we get the Algorithms through which encryption is performed. In

the last phase decryption is performed and it generates the plaintext. In this phase we don't check the data type and its nature because we already get this information in the form of code. Figure 3.3 shows the complete flow of the decryption process.

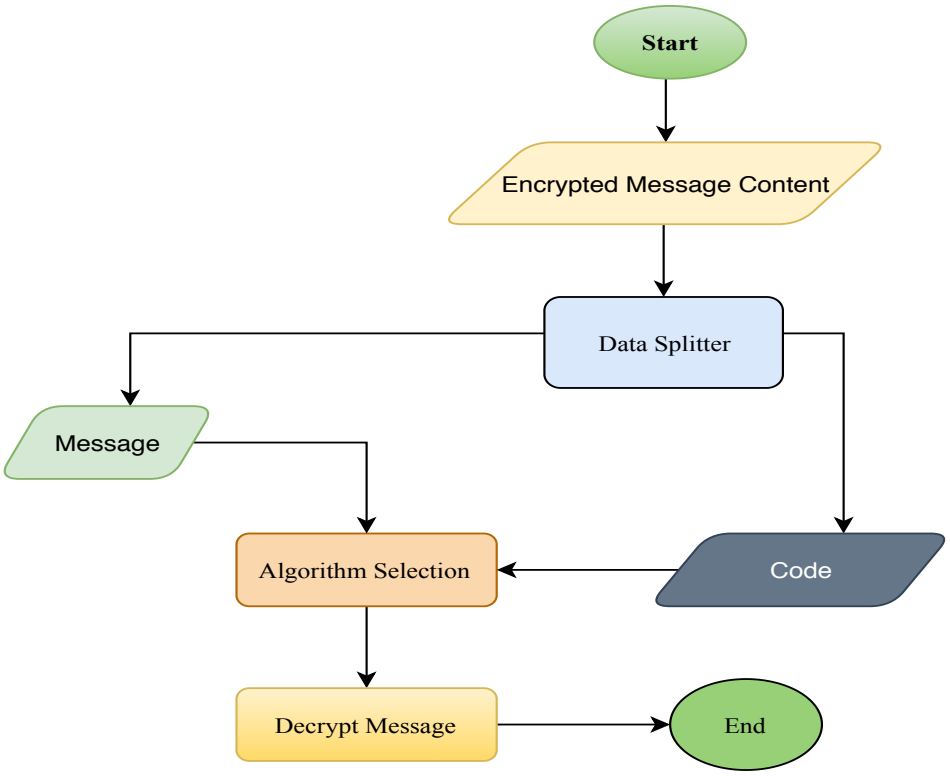

FIGURE 3.3: Decryption Diagram.

3.3 Algorithm Selection

In this phase, algorithm selection is performed. Firstly data type, data size, and data nature are provided to our framework, based on algorithm metrics our framework decides whether the data is String or Image Data type. After checking data nature and datatypes rules are applied for the selection of cryptographic algorithms as shown in Figure 3.4. For example, we have provided a message to our framework whose length is 200 and its data type is string. Our framework checked the data nature, data type, and length of the data. After checking these parameters rules are applied for the selection of cryptographic algorithm based on algorithm parameters like key size, block size, cipher type, security, and power consumption parameters. As we have selected six different algorithms for this framework

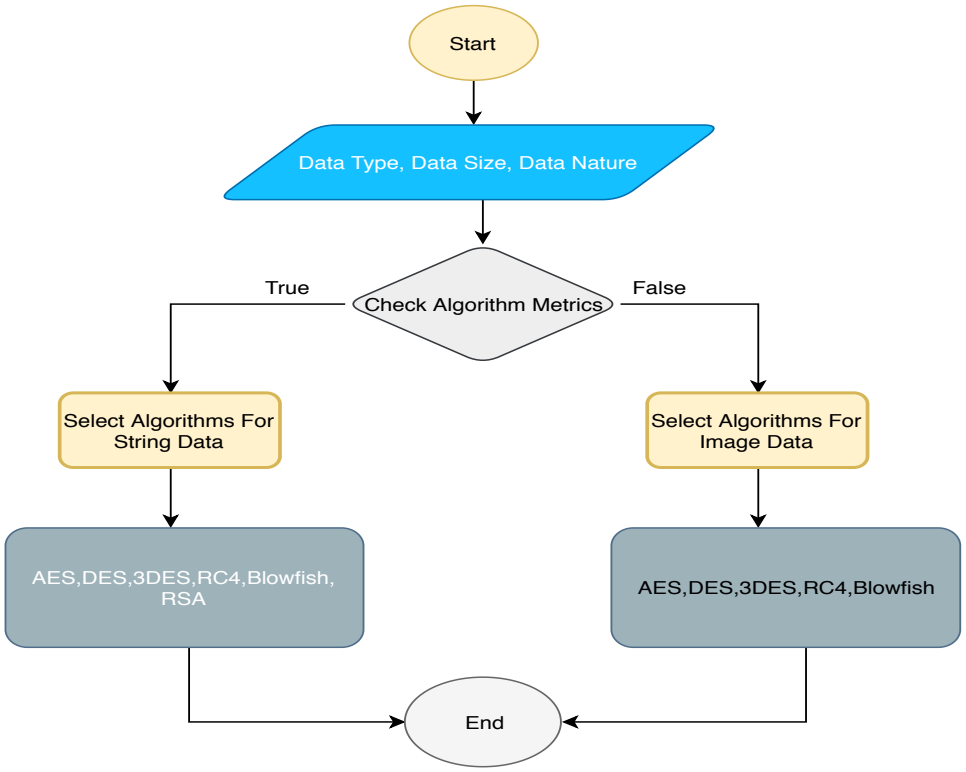

FIGURE 3.4: Algorithm Selection Diagram.

like AES, DES, 3DES, RSA,RC4 and Blowfish [**?**] - [28]. Our framework will automatically select the algorithms in this case.

3.4 Rule Based Approach

In this phase, we will discuss the rules which we have defined in our framework. We have defined our rules considering data content parameters as well as cryptographic algorithms parameters. Data content parameters contain parameters like data size, data type, data nature and content type like data contains online data or offline data. Algorithm parameters contain the parameters like block size, key size, cipher type, and security. 3.5 shows how rules are executed in our framework.

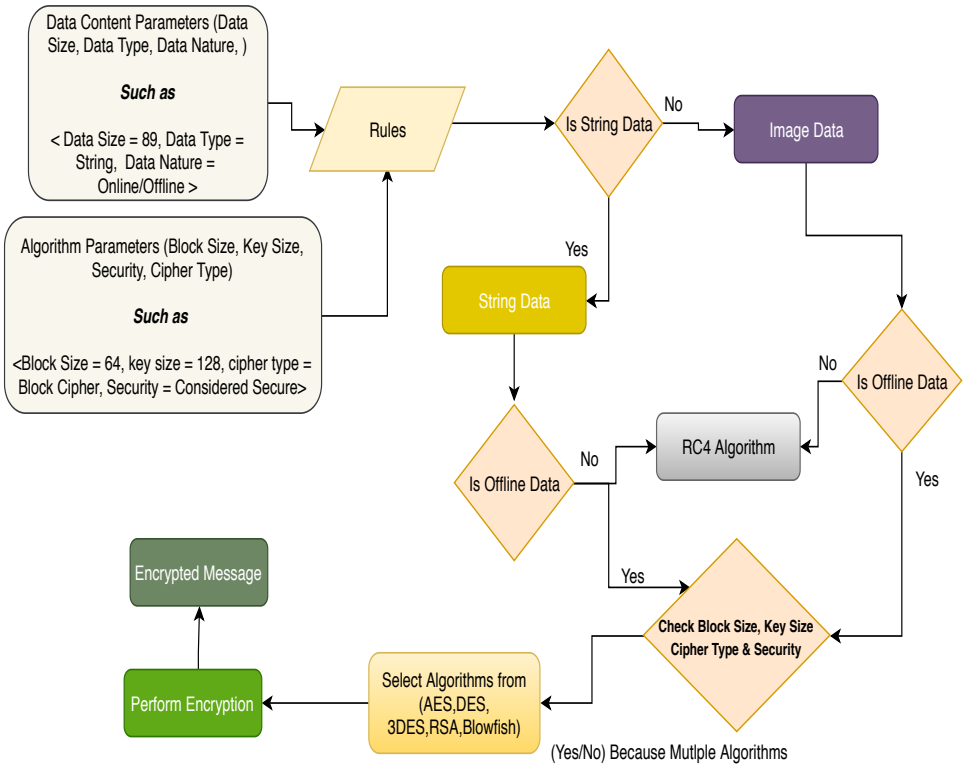

FIGURE 3.5: Rules Based Approach Diagram.

3.5 Synopsis

In this chapter, we have discussed the methodology of our framework. Now we can perform the experiments to validate the better performance of this technique as compared to the existing techniques. In the next chapter we will perform the experiments and we will evaluate the results of our techniques with other existing techniques.

Chapter 4

Experiments and Results

This chapter presents the results obtained from the adopted methodology. We compare the results of our framework with different cryptographic algorithm results. The evaluation of the technique is performed on the basis of encryption and decryption time. This results chapter is divided into different sections. Section 4.1 describes the dataset information. Section 4.2 describes the Experimental Setup. Section 4.3 describes the Textual data results. Section 4.4 describes the Image data results and Section 4.5 discusses the conclusion of this chapter.

4.1 Dataset

This project focuses on providing better cryptographic algorithms for encryption and decryption, For this purpose, we have developed a set of generalized rules. Creating generalize rules is only possible if the data is diverse. There were different websites available for collecting the dataset for images and textual data but we have collected our dataset from [30]. This data is freely available for demo purposes.

4.2 Experimental Setup

This section contains the information of the experimental setup which we have used to get the results. As we know while getting the results system specification matters a lot. We have used a system whose processor Intel(R) Core(TM) i5-5200 CPU @ 2.20 GHz, 4 GB Ram, and 64-bit operating system. We have used java version 1.8 [31] and eclipse oxygen version [32].

4.3 Textual Data Results

We have compared the textual data results of our framework with different algorithms and we have found that our framework takes slightly more time as compared to other techniques. The reason behind this the implication of multiple cryptographic algorithms in our framework. These multiple algorithms selection depends on the rules. We have used different file sizes for getting the results as shown in Table 4.1.

Table 4.1 shows that our framework is taking slightly more time than the other algorithms. Our main goal was to provide more security for the data that cost us increase in encryption and decryption time.

Figure 4.1 indicates the time taken by the algorithms for encryption and decryption with respect to filing sizes given to our framework and other cryptographic algorithms. This shows that our framework is taking slightly more time than others in few cases. This is due to the implication of multiple algorithms in some cases to overcome the security concerns of the standard algorithm which are proven inadequate. As our main focuses were to provide a framework which will select the algorithms based on data content parameters as well as algorithm parameters. Therefore, we believe that we can bear this cost of time.

TABLE 4.1: Textual Data Results in Milliseconds

File Size	RC4	Blowfish	AES	DES	3 DES	Our Framework
10kb	662	634	667	617	605	805
100kb	625	676	710	646	716	872
500kb	688	725	810	780	784	995
1000kb	628	909	880	785	844	975
5000kb	744	963	1108	1100	1876	2505
10000kb	812	1389	1273	1859	3597	3922
20000kb	1084	1858	1503	2853	6401	9526
40000kb	2974	4096	2448	4546	15394	13867

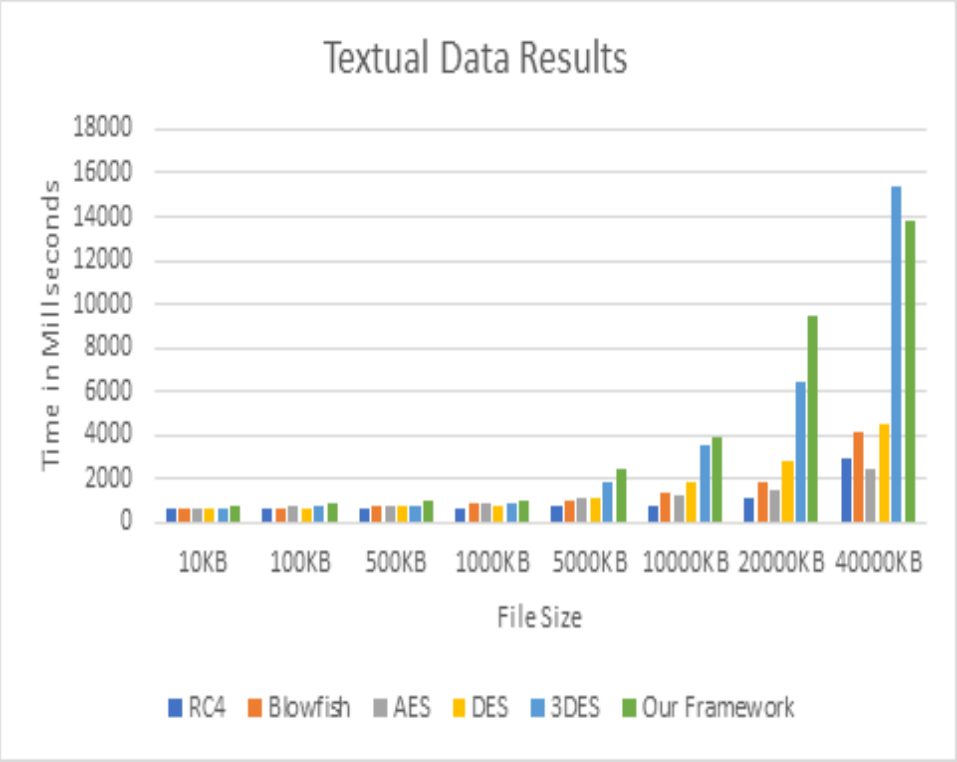

FIGURE 4.1: Textual Data Result Chart.

4.4 Image Data Results

We have compared the performance of our framework on image data with other cryptographic techniques. The evaluation results depict that our framework is taking less time for encryption and decryption as compared to others. We have also evaluated that the behavior of different algorithms varies depending upon the size of input like Blowfish and AES at some instance Blowfish is working better than AES likewise at some instance AES is behaving better than Blowfish. Our framework is performing better as compared to other cryptographic algorithms in terms of performance. Our framework is using multiple algorithms together to maintain security as well. Table 4.2 shows the results for the dataset which we have evaluated.

TABLE 4.2: Image Data Results in Milliseconds

File Size	RC4	Blowfish	AES	DES	3 DES	Our Framework
50kb	1054	912	1102	1036	1008	975
100kb	1110	956	1225	1218	1032	998
500kb	1305	1628	1535	1448	1307	1345
1000kb	1809	1688	1685	1481	1557	1774
5000kb	3013	3259	3914	3412	3734	3477
10000kb	4266	4844	4646	4918	5642	5112
20000kb	5543	6379	6020	6614	8050	6120
30000kb	8140	9144	8622	9706	12819	8666

Figure 4.2 indicates the time taken by the algorithms for encryption and decryption with respect to the image sizes given to our framework and other cryptographic algorithms. This shows that our framework is working efficiently as it is taking less time than other cryptographic algorithms in terms of performance. Also,

we are using multiple algorithms together to enhance more security. We have also evaluated that our framework is working more efficiently on image data as compared to textual data.

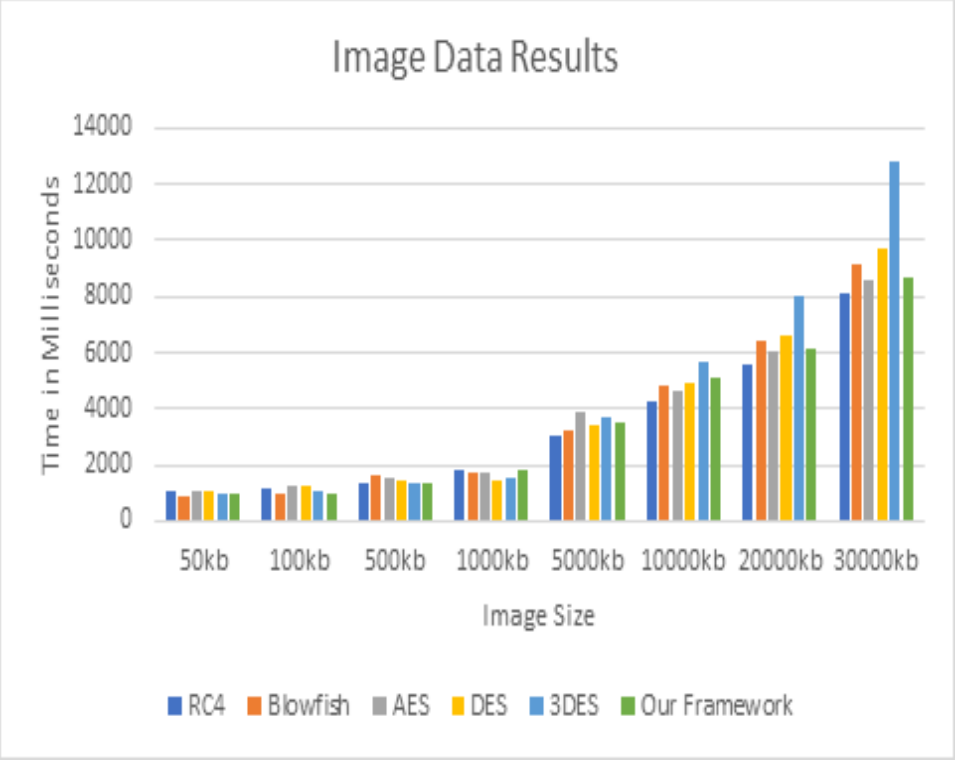

FIGURE 4.2: Image Data Result Chart.

4.5 Synopsis

In this chapter, we have done a comparison of results on image data and textual data. We have evaluated that our approaches have performed significantly well as compared to other techniques in terms of performance. We have also evaluated that our textual based approach took more time in few cases of file sizes but our image-based approach performed efficiently in terms of performance. As our main goal was to provide the evaluation criteria of the cryptographic algorithms on the basis of data content parameters as well as cryptographic algorithms parameters. Based on this factor such kind of cost can be tolerated. In the next chapter, we will conclude our report and we will discuss our future work.

Chapter 5

Conclusion and Future Work

Selecting the Algorithm dynamically from a set of cryptographic algorithms is a very challenging task due to the security concern of the data. Multiple approaches have been identified for selecting the cryptographic algorithm. From the comprehensive literature review, we have identified different approaches for selecting cryptographic algorithm based on different algorithm parameters like security, block size, and key size. This project focuses on making rule-based approach. we have not identified any rule-based approach in this area in our literature review.

In this project, we proposed a generalize rule-based approach that decides the algorithm selection based on data nature, data type and algorithm parameters. It will help the users to import the library and just passed their data to the library and it will automatically decide what type of cryptographic algorithm should be used and then it will perform encryption on the data. User will not be able to judge from which algorithm encryption is performed at the sender end. In the receiver end, user passed the data to our library and that will automatically decrypt the data without any information given by the receiver.

We have compared the results of our approach with different cryptographic algorithms and we have evaluated that our textual data took more time for encryption and decryption as compared to other cryptographic algorithms but considering security as a priority we can bear this kind of lost that provides us more security.

Also, our framework uses multiple algorithms together based on rules which itself considered as an efficient solution. The results which we have evaluated of other algorithms were not creating much difference of time between our framework and other cryptographic algorithms. We have also evaluated that Image-based data took less time as compared to other cryptographic algorithms which are also a plus point of our framework.

Our future work includes the addition of more algorithms and we will consider a few more parameters of the algorithm to get more accurate results in terms of security and efficiency. We are also considering to generate the code dynamically which contains the information of the rules which have been applied at the sender end so that will also enhance the security. We will also consider making this more generalize for the user so user can decide which type of algorithms should be considered for their library like they would be able to decide the algorithms that they want to used and reject the others algorithms.

Bibliography

[1] "Crypto Mathic", https://www.cryptomathic.com/, accessed on 25 Feburary 2019.

[2] "Symmetric Vs Asymmetric Cryptography", https://www.ssl2buy.com/, accessed on 25 Feburary 2019.

[3] "Public and Private Key Cryptography",https://searchsecurity.techtarget.com/, accessed on 27 Feburary 2019.

[4] "Plaintext",https://www.open.edu/, accessed on 28 Feburary 2019.

[5] Mahajan, Prerna, and Abhishek Sachdeva. , "A study of encryption algorithms AES, DES and RSA for security." *.Global Journal of Computer Science and Technology* , 2013.

[6] Kumar, Yogesh, Rajiv Munjal, and Harsh Sharma. , "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures." *.International Journal of Computer Science and Management Studies* , 11(03), pp. 60-63. 2011.

[7] Kader, H. M., and M. M. Hadhoud. ,"Performance evaluation of symmetric encryption algorithms." *.Performance Evaluation*, 58-64. 2009.

[8] Gong, Lina, Li Zhang, Wei Zhang, Xuhong Li, Xia Wang, and Wenwen Pan., "The application of data encryption technology in computer network communication security," *.In AIP Conference Proceedings* , (Vol. 1834, No. 1, p. 040027), 2017.

[9] Mushtaq, Muhammad Faheem, Sapiee Jamel, A. Hassan Disina, Zahraddeen A. Pindar, N. Shafinaz Ahmad Shakir, and Mustafa Mat Deris., "A Survey on the cryptographic encryption algorithms," *.International Journal of Advanced Computer Science and Applications* , 8(11), pp. 333-344, 2017.

[10] Hercigonja, Zoran., "Comparative analysis of cryptographic algorithms.," *.International Journal of Digital Technology and Economy*, 1(2) pp. 127-134. 2016.

[11] Elminaam, Diaa Salama Abd, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. , "Evaluating the performance of symmetric encryption algorithms.," *.IJ Network Security*, 10(3) pp. 216-222. 2010.

[12] Agrawal, Himani, and Monisha Sharma. , "Implementation and analysis of various symmetric cryptosystems.," *.Indian Journal of science and Technology*, 3(12) pp. 1173-1176. 2010.

[13] Alanazi, Hamdan, B. Bahaa Zaidan, A. Alaa Zaidan, Hamid A. Jalab, M. Shabbir, and Yahya Al-Nabhani. , "New comparative study between DES, 3DES and AES within nine factors.," *.arXiv preprint*, 2010.

[14] Singhal, Nidhi, and J. P. S. Raina. , "Comparative analysis of AES and RC4 algorithms for better utilization.," *.International Journal of Computer Trends and Technology*, 2(6) pp. 177-181. 2011.

[15] Thakur, Jawahar, and Nagesh Kumar. , "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis.," *.International journal of emerging technology and advanced engineering*, 1(2) pp. 6-12. 2011.

[16] Kumar, M. Anand, and S. Karthikeyan. , "Investigating the efficiency of Blowfish and Rejindael (AES) algorithms.," *.International Journal of Computer Network and Information Security.*, 4(2) 2012.

[17] Singhal, Nidhi, and J. P. S. Raina. , "Comparative analysis of AES and RC4 algorithms for better utilization.," *.International Journal of Computer Trends and Technology.*, 2(6) pp. 177-181. 2012.

[18] Seth, Shashi Mehrotra, and Rajan Mishra. , "Comparative analysis of encryption algorithms for data communication 1." 2(2) pp. 292-294,2011.

[19] Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms." *IJCSNS International Journal of Computer Science and Network Security*, 8(12) pp. 280-286. 2008.

[20] Hossain, Md Alam, Md Biddut Hossain, Md Shafin Uddin, and Shariar Md Imtiaz. , "Performance analysis of different cryptography algorithms" *.International Journal of Advanced Research in Computer Science and Software Engineering*, 6(3) pp. 659-663. 2016.

[21] Rihan, Shaza D., Ahmed Khalid, and Saife Eldin F. Osman., "A performance comparison of encryption algorithms AES and DES." *.International Journal of Engineering Research and Technology (IJERT).* , 4(12) pp. 151-154. 2015.

[22] Singh, Sombir, Sunil K. Maakar, and Sudesh Kumar., "A performance analysis of DES and RSA cryptography." *.International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, 2(3) pp. 418-423. 2013.

[23] Al Hasib, Abdullah, and Abul Ahsan Md Mahmudul Haque., "A comparative study of the performance and security issues of AES and RSA cryptography." *.Third International Conference on Convergence and Hybrid Information Technology, Vol. 2 pp. 505-510 IEEE*, 2008.

[24] Nadeem, Aamer, and M. Younus Javed., "A performance comparison of data encryption algorithms" *. International conference on information and communication technologies. IEEE*, pp. 84-89 2005.

[25] Pujol, F. A., Mora, H., Luis Sánchez, J., Jimeno, A., "A client/server implementation of an encryption system for fingerprint user authentication.," *.Kybernetes*, 37(8) pp. 1111-1119. 2008.

[26] "Rule-Based Approaches", https://gregstanleyandassociates.com/, accessed on 10 March 2019.

[27] Yu, Qian, and Chang N. Zhang. , "RC4 state and its applications," *.IEEE*, pp. 264-269. 2011 .

[28] Zhou, Xin, and Xiaofei Tang., "Research and implementation of RSA algorithm for encryption and decryption.," *Proceedings of 2011 6th International Forum on Strategic Technology. IEEE*, Vol. 2. pp. 1118-1121. 2011.

[29] "Diagrams", https://www.draw.io/, accessed on 1 May 2019.

[30] "Dataset", https://sample-videos.com/, accessed on 24 April 2019.

[31] "Java SE 1.8", https://www.oracle.com/technetwork/java/javase/downloads/index.html, accessed on 5 May 2019.

[32] "Eclipse Oxygen", https://projects.eclipse.org/releases/oxygen, accessed on 5 May 2019.

[33] "RC4 Algorithm", https://www.vocal.com/cryptography/rc4-encryption-algoritm/ , accessed on 7 May 2019.