Analysis of Data Security Algorithms for Grain Storage Systems

A Thesis report submitted towards the partial fulfilment

of the requirements of the degree of

Master of Engineering

in

Information Security

Submitted by

Ankita Verma

(801433005)

Under the supervision of

Dr. Inderveer Chana
Professor, CSED

Dr. Paramita Guha
Scientist, CSIO-CSIR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

THAPAR UNIVERSITY, PATIALA – 147004

JUNE 2016

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Analysis of Data Security Algorithms for Grain Storage Systems"**, in partial fulfilment of the requirements for the award of degree of Master of Engineering in ***Information Security*** submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Inderveer Channa, Professor, Thapar University.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Ankita

(Ankita Verma)
Roll no. 801433005

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

23/06/16

Dr. Inderveer Chana
Supervisor

Countersigned by

Dr. Maninder Singh
Head
Computer Science and Engineering Department
Thapar University

Dr. S.S. Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

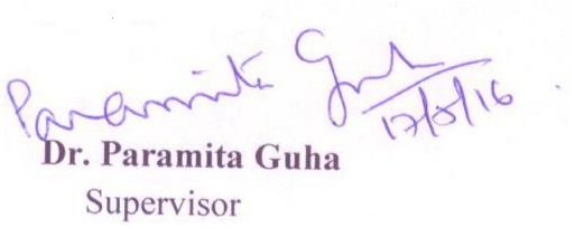
Certificate

I hereby certify that the work which is being presented in the thesis entitled, "**Analysis of Data Security Algorithms for Grain Storage Systems**", in partial fulfilment of the requirements for the award of degree of Master of Engineering in ***Information Security*** submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Paramita Guha, Scientist, CSIO-CSIR.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Ankita Verma)
Rollno: 801433005

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.



Dr. Paramita Guha
Supervisor

Acknowledgement

The real spirit of achieving a goal is through the way of excellence and austere discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities.

With deep sense of gratitude I express my sincere thanks to my esteemed and worthy supervisor, **Dr. Paramita Guha,** Scientist, CSIO-CSIR, Chandigarh and **Dr. Sunita Mishra,** Scientist, CSIO-CSIR, Chandigarh and for their valuable guidance in carrying out this work under their effective supervision, encouragement, enlightenment and cooperation. Most of the novel ideas and solution found in this thesis are the result of our numerous stimulating discussions. Their feedback and editorial comments were also invaluable for writing of this thesis.

I shall be failing in my duties if I do not express my deep sense of gratitude towards **Dr. Inderveer Chana,** Professor, Department and **Dr. Maninder Singh**, Head, of Computer Science and Engineering, Thapar University, Patiala, who have been a constant source of inspiration for me throughout this work. I am also thankful to all the staff members of the Department for their full cooperation and help.

This acknowledgement would be incomplete if I do not mention a helping hand provided by my friends. I had a pleasant enjoyable and fruitful company with them. My greatest thanks are to all who wished me success, especially my parents, my brother whose support and care makes me a person what I am today.

Ankita Verma

(801433005)

Abstract

Large amount of data has been debouched in the coming years therefore data security has become the most important aspect of information sharing. More private data is stored in the cloud. Practically, the quantity of data to be transferred is not the concern. The important factor is the channel, through which the data is transferred, should be secured. Cryptography is one such technique which is can ensure for secure transmission of the data. And, using cryptographic techniques security can be provided to the information.

This research work classifies the types of existing encryption algorithms and presents a comparative analysis on Advanced Encryption Algorithm (AES), Data Encryption Standard (DES), and Blowfish algorithm. These algorithms have been implemented on a Grain depot system dataset which consists of granaries and a server from where the expert system accesses the data. This data from the granaries is transferred to the server which is stored in an encrypted form. The algorithms are compared on the basis of different parameters such as throughput value, avalanche effect, perceived performance, performance based on execution time, convergence (convergent algorithms) and power consumption. Code for all the algorithms is written in MATLAB. Throughput value checks if the algorithm is efficient or not, it tells the amount of text encrypted per unit time. Blowfish Algorithm has the high value of throughput nearly 90% increase in the value in comparison to AES and DES. Performance based on execution time checks the speed if the particular algorithm is suitable enough to use. Its value is inversely proportional to the execution time. More is the execution time of an encryption algorithm, less favorable it would be to use. Here also Blowfish Algorithm has outpaced AES and DES algorithm. Perceived performance tells how quickly encryption task is done. It is directly proportional to the real performance of the encryption algorithm. Convergence is checked through the value of cipher text. Blowfish Algorithm produces different value of cipher text whenever it is run, whereas AES and DES produces the same value of cipher text every time it is run. Further, comparison is made on the amount of energy consumed

by each algorithm. Algorithm which requires low energy and power is favored. Blowfish has nearly 61% decrease in value of power in comparison to AES and DES algorithm. Avalanche effect of an algorithm is calculated by changing a bit in the plain text. After that the value of cipher text is checked. This is again a parameter to check the level of security of an algorithm. Blowfish Algorithm changes the cipher text completely. Hence, it can be concluded that Blowfish algorithm is secure and efficient than the remaining algorithms, therefore it has been used in providing data security to CSIO-CSIR Grain storage data.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the emergence of large amount of data, the need of data security has become primary concern for the users. Ever since conceptualization of cloud, more and more private digital data has been put into the cloud and this data is accessed through many kinds of devices. All this brings into a situation where data security plays a significant role.

1.1 Data Security: An Overview

Data security also known as information security is a practice in which unauthorised users are defended from performing illegal activities like disclosure, modification, access, destruction and perusal of any digital and physical data. Computer attacks which people come across in day to day life include identity theft, masquerading, spoofing, sabotage, software attacks and information extortion. All these attacks must be handled in an efficient way such that only intended users could access the private data and unauthorised users should be blocked from using the data. Due to this renounce need of security, Cryptography [1] came into picture, so that the data in the cloud could be protected and can be read by the intended user only. Cryptography also known as "secret writing" is an art of hiding useful information so that only the intended parties can have access to the private information. It protects the privacy and modification of data which may occur due to active and passive attacks in the channel. Cryptography consists of plain text and cipher text [2]. Plain text in the original data which the sender intends to send and cipher text is the encrypted format of the plain text. The plain text is converted to the cipher text and vice versa with the help of an encryption and decryption algorithm. The encryption-decryption algorithms are mainly classified into two type e.g. symmetric key algorithm and asymmetric key Algorithm. Since database is a collection of large amount of data, its security becomes a primary concern because for some people the data may be as

confidential as their credit cards. Just as credit cards are provided with the security key called pin similarly cryptography provides users with an encryption and decryption algorithm with a key which encrypts the text and converts it into cipher text.

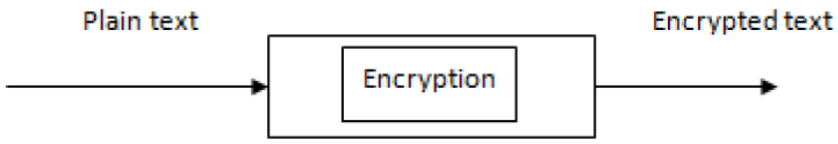


Figure 1.1: Encryption

Only those who have access to the cipher key can easily decipher the text. As shown in Figure 1.1, a plain text is passed through an encryption algorithm which encrypts the text with the help of a unique key. This Encrypted text is sent to the receiver which through the decryption algorithm and key deciphers the text back into plain text. There is a possibility that through cryptanalysis one can easily break the code which may include brute force attack. This is generally termed as code- breaking.

Traditional cryptographic algorithms were breakable therefore modern cryptographic algorithms are introduced because they cannot be easily breakable through human attacks. Electronic communication persists in today's era and is favored till now therefore cryptography has become a primary concern. Pretty good privacy is one of the cryptographic techniques that are preferred because it is secure and effective.

Input data can be in the form of blocks or streams. Hence on the basis of this data ciphers can be of two types. Block ciphers and stream ciphers. In block ciphers the data is divided into fixed size block. Data gets divided into block of given size and then encryption is performed on independent block data. In case of stream ciphers the data is a long stream on which encryption decryption algorithm is performed. AES, DES, Blowfish are the examples of Block ciphers and ECC, RC5 are some of the stream cipher techniques.

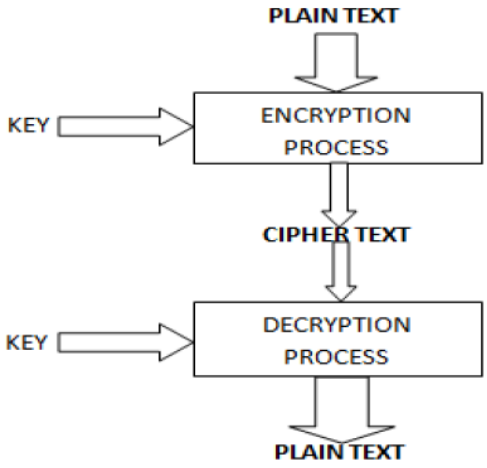


Figure 1.2: Encryption Process

Figure 1.2 shows the flowchart of the encryption process. Main components of cryptography are plain text, cipher text, encryption algorithm, decryption algorithm and keys (private key and public key).

- Plain Text

The original text or message used in communication in called as Plain text. foreg. Hello world is an example of a simple plain text.

- Cipher Text

Any un-readable message that is obtained from a plain text is a cipher text.

- Encryption

Encryption is a process of converting Plain text into cipher text. This un-readable message can be communicated over any communication channel without the fear of the loss of confidentiality and integrity. Encryption process is done using encryption algorithm with the help of a key.

- Decryption

Decryption process is just the opposite of encryption process, i.e. cipher text is converted into plain text using a particular decryption algorithm.

- Key

A key is a numeric or Alpha-numeric text. It acts on the plain text through encryption algorithm to encrypt the text and on cipher text through decryption algorithm to decipher the text. Encryption or Cryptography have some goals that needs to be fulfilled for user benefit. Modern cryptography consists of the following five objectives:

i) Confidentiality

The information cannot be understood by anyone for whom it was unintended. It should only be understandable for those who are authorized to avail the information.

ii) Integrity

The information cannot be changed while being sent over a communication channel between sender and intended receiver.

iii) Non-repudiation

The sender cannot deny that the information sent by him to a particular receiver does not belong to him.

iv) Authentication

The sender and receiver can confirm each other's identity so that the information exchanged should be genuine.

v) Access Control

Only authorised users can access the data. Main objective of access control is to avoid unnecessary access of useful information by unknown users. The plain text is encrypted through encryption algorithm and decrypts the cipher text through decryption algorithm. The key can be either public or private.

The encrypting and decrypting algorithm as discussed above can be categorized into two types based on the number of keys required. They are symmetric encryption algorithms and asymmetric encryption algorithms [2]. These are defined as follows.

i). Symmetric encryption algorithms

Symmetric encryption algorithms are the encryption algorithms in which the same key is used for encryption process as well as decryption process. Different types of symmetric key encryption algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-Data Encryption Standard (3-DES), Blowfish etc. These algorithms used for encryption and decryption involves the generation of public and private keys and decrypt message through private key which is known only to the intended recipient. Message can be easily encrypted with the help of public key but decrypting the private key one should possess the ability of code breaking.

ii). Asymmetric encryption algorithms

Asymmetric encryption algorithms are the algorithms which require different keys to encipher and decipher the text. To encrypt a text public key of the sender is used and to decrypt the text, receiver uses its own private key to decrypt the text. Different types of asymmetric encryption algorithms are Rivest Shamir Adelman (RSA), Diffie-Hellman algorithm and many more. Symmetric key algorithms though require less number of calculations as compared to asymmetric key algorithms. Asymmetric algorithms (also known as public-key algorithms), requires at least a 3,000-bit key to compete with the level of security 128-bit symmetric algorithm provides.

1.2 Forecasting Security Demand

Data security is a critical phenomenon not only for the corporate users but also for the computer users at home. Financial information, employee details, banking details are critical information which can prove to be potentially dangerous if the information falls in the wrong hands. Hence securing information and keeping it confidential must

the prime concern of a security analyst. Data if lost through hacking and malware can cause great consequences.

Following are the reasons why there is a great need for data security.

i. To avoid any kind of risk to the corporate or the organization

The organization keeps certain kind of information confidential for a specific purpose. If the information gets leaked it can jeopardize the company as well as its employees to a large extent.

ii. Protection against identity theft

To avoid identity theft physical and logical access controls are introduced. Physical access controls are the countermeasures that restrict any user for accessing a sensitive data. Example biometrics, Scanners which allows only authorized users to access data. In case of unaccredited employee the access controls can warn people about any unauthentic user.

iii. To avoid phising and targeted attacks

Phising is a malicious way of obtaining confidential information such as credit card information, username passwords, banking details. The emails sent to the target person are infected with a malicious code. If the person opens the email his computer is compromised with virus and malwares resulting in information breach.

iv. To avoid employees from harassment

When an unethical hacker gets access to a company's sensitive data he may blackmail the organization in doing wrong things harassing the victim by keeping his life at stake. He may lose his job.

v. Implemented in any system which requires data security

There are many working systems like Password Management systems, Grain depot Systems, Hospital management systems, banking management systems and many more where data security can be enhanced by implementing different encryption

algorithms. Algorithms like Data Encryption standard (DES), Advanced Encryption Standard (AES), Blowfish Algorithm have already been implemented in such systems providing efficient security in the respected areas.

Data security therefore is highly important in today's era where cyber attacks are highly common. Figure 1.3 gives you a better view of a security tree.

Figure 1.3: Security tree [3]

1.3 Challenges Faced During Data Security

There are multiple challenges of data encryption for security. Not only problems are faced in data base security, big data also faces challenge with encryption. Database is a place where company's mandatory data is accumulated and is accessible by the employees in the organisation. If database is provided security at the lowest level

called as the storage level such as disk media or tape, the level of protection is very little as compared to application and logical level. There are many risk involved at the database level which are discussed as follows.

i) Hackers who gains privilege in a database can access encrypted keys through which they can extract any kind of sensitive information.
ii) Applications that are infected through a virus can easily access confidential data. There are chances that the database keys to decrypt the data are lost. Here large amount of data will be lost as data would become unavailable.
iii) Since there is a large amount of data in the database, the person who has the access to this wide data can lose control and unintentionally make changes which cannot be reverted back.

Big data also faces challenges while securing the data. The majority of them includes key management, access policy based encryption, communication protocols, big data privacy which can affect end to end privacy of the data. All these factors are the key factors for hampering data integrity. There are cases where users store images, video data on the cloud. To perform encryption in which mathematical calculations are involved cannot be performed on images. In that case document containing both images and data is difficult to encrypt simultaneously. It is definitely a big challenge for security coders.

Access policy is also a big problem. Many scientists say that access controls must be applied irrespective of the host system. If data is encrypted based on the host system, there is some access policy based with system, so that policy will be applied with respect to the host system while accessing the data. Hence Data security is not a simple task. All the policies and encryption must be applied based on the system requirements.

1.4 Research Motivation

Large amount of data is stored in the cloud which means there is a high possibility of attacks. The cost of data stealing is rising globally which needs to be addressed. Recently vulnerability is observed in facebook wherein an attacker can read personal

chats between the people and even changed the written conversation causing threat to the person's life. There are many such attacks which gain a lot of attention and need to be taken care of but even if the attacks are not popular they can be equally dangerous and impactful. Therefore data security must provide a solution by providing correct security controls and end to end approach for safeguarding the data. Many security algorithms have also been implemented so as to store the encrypted data on the server.

The motivation of this research work arises from data security as it is an important issue. Highly secure encryption algorithms if applied to any application can prevent data loss and leakage. It protects the organization from data breaches. Research on data security algorithms is not an easy task. In this work, existing security algorithms namely AES, DES and Blowfish algorithms have been analyzed for their security solutions by applying them on a grain storage data set.

1.5 Organization of Thesis

The rest of thesis is organized as follows:

Chapter 2- This chapter deals with the review of literature survey on different encryption algorithm.

Chapter 3- The problem statement about the research work along with the objectives is stated in this chapter.

Chapter 4- This chapter deals with the Case study for evaluation of the algorithms. It discusses the proposed method and methodology used for carrying out the research work

Chapter 5- This chapter deals with software and hardware methodologies.Software methodology, covers the software used during the project development like MATLAB on which the code for all the algorithms is written and different conclusion have been drawn. Experimental results have been stated in this chapter.

Chapter 6- In this chapter conclusion followed by future work has been discussed.

Chapter 2

Literature Review

In the last chapter, needs for data security has been introduced and challenges faced in the data security are discussed. Encryption Algorithms for ensuring data security are of utmost importance. In this chapter literature survey of different cryptographic algorithms for security has been done. The new generated cryptographic security algorithms have been characterized and discussed in detail.

2.1 Research Questions

This literature review incorporates the existing security algorithms to answer various present research questions.

i) How secure are the existing data security algorithms?

ii) How these algorithms are different from previously generated encryption algorithms?

iii) Which algorithm is most favored and provides justice for the security of organizations data. This literature review starts systematically with appropriate research questions. Various security algorithms have been categorized on the basis of different techniques and are discussed below.

2.2 Existing Security Algorithms

There are many security algorithms that have been developed due to the increasing attacks on the data of an organization. Figure 2.1 shows the different data security algorithm based on encryption, database techniques, and audibility and stegnographic techniques. These algorithms are currently being used for the integrity and confidentiality of data.

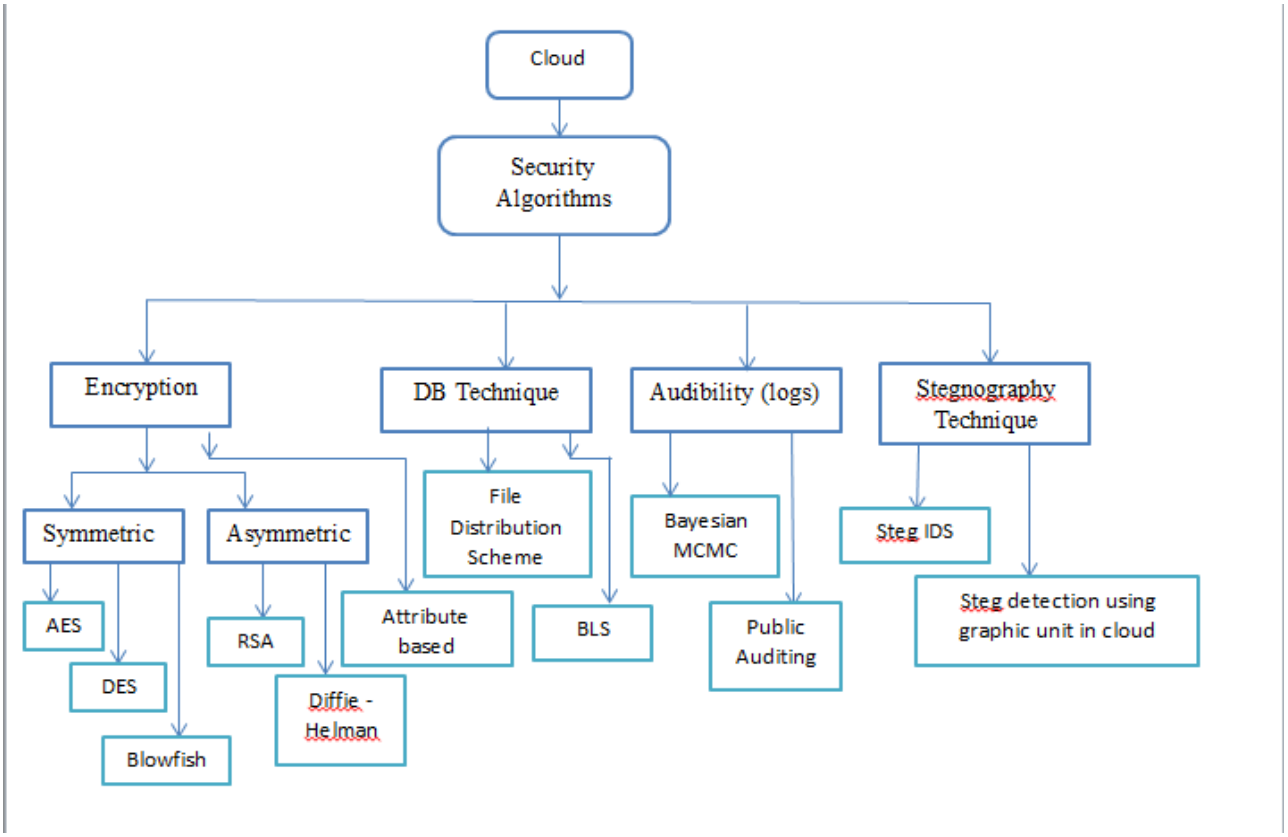


Figure 2.1 Different security algorithms

Existing security algorithms used for the integrity and confidentiality of the data have been discussed below.

2.2.1 Encryption Techniques

The algorithms which are defined under this category follow encryption process.in encryption techniques algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish, Rivest Shamir Adlemen (RSA), Diffie-Helman and attribute-based encryption algorithms have been defined**.** Since DES is vulnerable to brute force attacks therefore it is proven inadequate in terms of security. In [4], the DES algorithm has been modified (called M-DES) Modified- Data Encryption Standard, to improve the Bit Error Rate (BER) rate caused due to avalanche effect and is made more secure so that it can be used in wireless

communication. To carry out this modification the authors have made use of S-box mapping tables. The second modification has been done from the work in [5] where the authors have shown that DES can be cracked from the differential cryptanalysis attack if 247 pairs of plain text and cipher text are present. After the simulation the author in [4] observed that BER rate is much better than DES because there is no avalanche effect in Modified Data Encryption Standard (M-DES) and as expected the algorithm came out with good results. After plotting and comparing the values of throughput obtained in [4] and [5], it has been observed that the proposed algorithm outperforms the use of the fixed 256-AES algorithm. It proved be powerful when the channel conditions were worst. Apart from BER rate throughput of the encryption algorithm must also be kept in mind so, in [6] the author maintained a tradeoff between security and throughput.

AES algorithm is comparatively more secure and has a strong avalanche effect. Attackers cannot easily decrypt the encrypted text by the brute force attack. Therefore AES has been used in many applications. In [7], the implementation of AES for PDA secure communication has been described. The author introduces a linear complexity in the design of AES to make it more secure. There are many attacks the AES algorithm has undergone. An attack which is a combination of boomerang and rectangle attack with related key differentials introduced in [7]. This attack can break the round versions of AES. In [8] short cut attacks have been defined which are dangerous to the three AES block ciphers. There are attacks which occur due to the vulnerability of Substitution-Box (S-box) in AES algorithm. In [9], authors have introduced a new way of generating S-box which can help from the algebraic attack. Authors also added their contribution to make up for the weakness of S-box and introduced an iterated hill climbing algorithm for the design of S-box [10]. After further discussions new algorithms were proposed to overcome the weakness in S-box design [11], [12]. In [13] author describes the security that AES Algorithm provides in accounting information where Accounting Information Security System (AISS) protect the accounting information data. The design of AISS based on AES is made which provides security from both internal and external attacks. Data security with steganography and AES is also discussed [14]. Since AES algorithm is secure, it

is used in hybrid form with other encryption algorithm, forming an onion layered structure and providing more security [15]. A modified version of AES was introduced to carry out MPEG video encryption. The algorithm was modified just to overcome calculations and computer overhead. A drastic improvement in the speed and encryption performance has been observed [16].

Blowfish is a strong encryption algorithm so it has been used in many applications. In [17], the author has shown nested watermarks which are embedded in a main image and these watermarks are encrypted before embedding using blowfish algorithm. Results show a remarkable embedded capacity and security in the watermarks. Tests are done to check the performance of blowfish algorithm by increasing the file size and the key length [18]. The equations derived from the result are kept for evaluating future performances. The design and implementation of password management system is also based on Blowfish algorithm [19].The algorithm has also been used in bitmap image plotting instead of using secret algorithm like skipjack algorithm in the clipper and capstone chips [20], [21]. Blowfish algorithm has been used with other encryption algorithms in hybrid form to enhance security and performance [22], [23]. Performance is also evaluated by modifying its function which brought up subsequent impressive results [24]. In the next section, different asymmetric algorithms available for the cryptography along with their applications are discussed in detail.

In [25], the author has introduced an improved version of RSA which is based on complex numeric operation resulting in comparatively low computational power. The authors have proposed a mechanism to speed up large mathematical calculations by implementing the numeric operation on the array resulting in a low computational power. With this the loop time is decreased and the calculation speed is improved greatly. Although RSA is a secure algorithm, but in [26] an experiment was done in the application of low private exponent attack in RSA where the author found out that there can be some new weak keys in RSA. Therefore, digital signature concept was introduced in combination with RSA [27]. Keeping all the flaws in mind, in [28] an algorithm implementing Digital Signature with RSA Algorithm was proposed to double the security of the algorithm. The RSA has been used in various applications

like in electronic commerce trade which ensures integrity, confidentiality, authentication and non-repudiation. This algorithm is also used in the construction of mercurial commitments and with this it has shown its contribution in zero knowledge databases as well [29].

In [30] the author has shown a round addition attack in Triple DES using Differential analysis [31]. The secret key extracted by the attack can easily obtain one correct Cipher text and two incorrect cipher text. Since triple DES is used in many applications today counter measures must be taken to implement a modified algorithm. In [32] the application of the triple DES has been discussed in the implementation of (Very-large-scale integration) VLSI. Three different hardware implementations have been proposed where the first two are related to pipeline techniques and the third one is used for consecutive iterations for data transformations. T-DES has been implemented by look up tables and ROM blocks providing information regarding throughput and design area. With these implementations simulation was done to check out for the correct functionality. It was found that the result was validated by the know answer test vector mentioned in [33]. The authors have shown that ROM blocks provide better performance and throughput results as compared to the look up tables.

2.2.2 Database Techniques

Based on database techniques, file distribution scheme and BLS algorithm have been proposed. In [34] the authors have proposed file distribution scheme in which third party auditor checks for integrity of the data that is stored on the server. It consists of a verification system which includes operations like block addition and deletion which is absent in existing systems. It also includes update; append operations for ensuring remote data integrity. This scheme is resilient to a failure called the byzantine attack. The only disadvantage of this scheme is that the latest dynamic operations like add, delete, update etc. are not so popular and therefore their applicability is comparatively limited. In [35, 36] BLS scheme have been presented. In [37] Reed Solomon Scheme has been proposed. The authors have stated that the probability of error pertaining to in reed solomon technique is very low. It is an error

correction as well as error concealment technique. This algorithm has been used in satellite broadcasting, spread spectrum systems, telecommunication systems and any more. The main disadvantage of this scheme is that it requires lot of processing in encoding and decoding processes.

2.2.3 Audibility Techniques (Logs)

In [38, 39] Bayesian MCMC algorithms have been discussed by the authors. It is through the logs that the user can come to know about the probability of the attacks. It gives the belief about the hypothesis after the data collection. The disadvantage of this technique is that it is very difficult to keep the log of all the lost data. This technique is definitely not feasible in large organizations. And therefore in [40] authors introduced a public auditing technique. It involves a special standard to be followed for keeping the logs of all the data and maintain data privacy.

2.2.4 Stegnographic Techniques

In [41-44] the authors have introduced steg intrusion detection system which ensures security of the data by hiding the data in audio, videos or any kind of music files. Through the knowledge of LSB it searches if there is any change in the bits. If any change found data integrity can be easily checked out. The only disadvantage with this algorithm is that if any component of stegIDS that is the analyzer, detector system, if fails, it would be impossible for the user to find out and data loss and intrusion will not be identified. There is another technique called stegnographic detection through graphic processing in the cloud unit [45-47]. Here also the data intrusions are find out through the graphic processing. Any change in the graphics could easily make out that the integrity of the data has been hampered.

2.2.5 Analysis of Algorithms

Table 2.1 presents an analysis of the existing data security algorithms categorized on the basis of different techniques.

Table 2.1: Analysis of Existing Algorithms Categorized under different Techniques

Data Security techniques	Algorithms based on the techniques	Future Scope	Discussions
Encryption Techniques	Modified Data Encryption Standard (M-DES)	M-DES is being favored in 4G wireless technologies. Also been used in the wireless fading channels.	i) Des algorithm has been modified to improve the bit error rate caused due to Avalanche effect. ii) Differential Cryptanalysis attack has been eliminated. iii) Is more secure and favored in wireless communication.
	Advanced Encryption Standard (AES)	AES can be used in fusion with the M-DES algorithm for better security. Can be used with Stegnography to provide image encryption.	i) Used for PDA secure Communication. ii) AES algorithm has undergone and eliminated rectangle and boomerang attacks. iii) Vulnerability in S-box can crack AES algorithm hence s-box has been generated through hill climbing algorithm to prevent the attack on AES.
	Blowfish Algorithm	ii) Blowfish function can be modified and can be used in fusion with AES and DES algorithm along with digital signatures.	i) The algorithm has been used in password management system. ii) Used as a replacement of skipjack algorithm in bitmap image plotting iii) DES-Blowfish fusion data techniques have been used to check the performance of the encryption process.
	Attribute-Based Encryption	Attribute based encryption to be applied on multimedia files.	i) Provides access control by providing only a specific attribute to be encrypted. ii) It has been implemented in data sharing techniques along with the technique of attribute revocation.
Database techniques	File Distribution scheme	Research in coding is done for elevating the distribution security.	i) TPA checks the integrity of the server data. ii) Consists of verification system including updating, appending operations for existing data integrity. iii) Resilient to byzantine attack. iv) Add, delete, update not popular hence applicability is limited.
	Reed Solomon	RS decoder can be	i) An error correction and

	Scheme	designed in MATLAB and detect the error even if it is present in the form of symbols. Similar implementation can be done using FPGA.	concealment technique used in satellite broadcasting, spread spectrum and telecommunication system. ii) Requires a lot of processing in encoding and decoding process.
Auditability (Logs)	Bayesian MCMC	The scheme is generally not favored due to maintenance of logs.	i) Analysts come to know about the attack through logs. ii) Since probability of the attacks can be judged through logs, this scheme cannot be used in large organization as it is difficult to keep log of large data
	Public auditing		i) This scheme is used remove the problem faced Bayesian MCMC. ii) It follows a special standard of keeping logs and maintains privacy.
Stegnographic Techniques	Stegnographic intrusion detection system.	This technique in fusion with Blowfish and DES algorithm can be used. Some of the experiments have been done using AES and stegnography in combination.	i) Through the knowledge of LSB it checks the change in the bit and ensures data security in audio, video and image files. ii) If any of StegIDS components, the analyzer and the detector system fails bugs will not be identified.
	Stegnographic detection through graphic processing in the cloud unit		i) This scheme detects the data integrity through the change in the graphics of the data. ii) This technique is limited only to audio, video and image file.

2.3 Conclusion

In this chapter different types of data security algorithm have been categorized based on different techniques. Based on each technique, recent algorithms along with their practical applications have been discussed.

Next chapter discusses about the problem statement, objectives and objectives methodology.

Chapter 3

Problem Formulation

In previous chapter different data security algorithms have been discussed. This chapter focuses on problem statement which has been taken up in the thesis.

3.1 Problem Statement

Data security to CSIO-CSIR organisation's critical data is to be provided with the help of DES, AES and Blowfish encryption algorithms. To evaluate which algorithm is to be used to provide data security to organization's data, MATLAB environment has been used. Implementation of Blowfish algorithm is to be done in MATLAB to make a comparative analysis with AES and DES algorithms that are already implemented in MATLAB.

3.2 Objectives

The objectives of present work are as follows:

- Study different data encryption algorithms.
- Implement the best three algorithms in MATLAB environment.
- Make a comparative analysis of the algorithms based on different parameters like throughput, performance based on execution time, perceived performance, avalanche effect, convergence and power consumption for a dataset.

3.3 Methodology

Methodology implemented to carry out the above objectives have been discussed below

Obj1: According the literature survey, existing data security algorithms based on different techniques will be classified.

Obj2: Through the survey conducted, the best three algorithms suitable for providing data security to CSIO-CSIR grain storage data sets will be implemented in MATLAB environment.

Obj3: After running the algorithms in MATLAB environment based on the values of the experimental results, a comparative analysis will be to decide which algorithm to be used for securing CSIO-CSIR grain storage data.

3.4 Conclusion

The problem statement and objectives of the thesis have been discussed in this chapter. The objective of comparing Blowfish algorithm with AES and DES has also been discussed.

Next Chapter discusses a case study for the evaluation of the algorithms.

Chapter 4

Case Study for the Evaluation of Algorithms

4.1 Case Study

The case study summarizes the work done in this thesis. An attempt to provide encryption to the CSIO-CSIR grain storage data has been done as per the requirement. The encryption has been carried out through the symmetric encryption algorithms, DES AES and Blowfish algorithm. A comparative analysis is done based on the results produced after running each encryption algorithm. The motive of using these algorithms for protecting the organization's data is because these algorithms can be implemented in MATLAB. As per the survey conducted, it has been observed that DES and AES algorithms have already been implemented in MATLAB. Implementing Blowfish Algorithm in MATLAB is definitely a new task, thus providing add-on explanation which algorithm to be used out of the three after the comparison is being carried out. Through the comparative analysis it has been observed that blowfish algorithm is highly secure than DES and AES and therefore has been used as an encrypting algorithm in CSIO - CSIR organisation for providing encryption on the grain storage data when stored on the server.

4.2 Grain Depot Systems

Attacks of insects, mites and fungi are the most concern for the health of stored grains. Control of storage temperature can prevent the insect development [48] and controlled humidity can control mite and fungi growth [49, 50]. Hence, storage temperature and humidity are most important factors that determine the quality of stored grain [51, 52]. After obtaining the data from the sensors, a proper actuator (e.g. AC, humidifier etc.) can be operated. Traditionally, a large number of cables are used in order to transmit the collected data back to control centre. These kinds of cables may result in lighting strike, interference, large cable coverage etc. Too many joints may also cause diffusion corrosion and accidents along with a vast maintenance cost. For these reasons, in recent years, wireless sensor network along with zigbee have

gained popularity for data transfer and control large scale grain depots. These chambers are generally built above the ground and kept at remote locations. The recent grain depot systems are formulated into a tiered structure which consists of smart, sink and sensor nodes at the upper level, server in the middle level and remote management centre at the lowest level. Sensor nodes are present within the granaries which collect the data about the environment. The data obtained from sensor node is forwarded to the server with the help of smart node. The server is localized where the management is realized. This data in the server is huge which can be protected through various mechanisms. One of them is cryptographic techniques.

4.3 Proposed Method

The proposed method consists of the following steps. Figure 4.1 gives a brief overview of what the dataset consists of.

Step 1: The data consists of humidity and temperature values which is obtained from grain depot systems. This data is collected on a server which is basically handled by an administrator.

Step 2: This data is encrypted using an encryption algorithm which runs on the server. Here the algorithms used are AES, DES and Blowfish algorithm.

Step 3: After the Encryption of data, this data can be decrypted by the user who is authenticated with a user name or password. The execution of the complete project methodology is being discussed in detail in the methodology section.

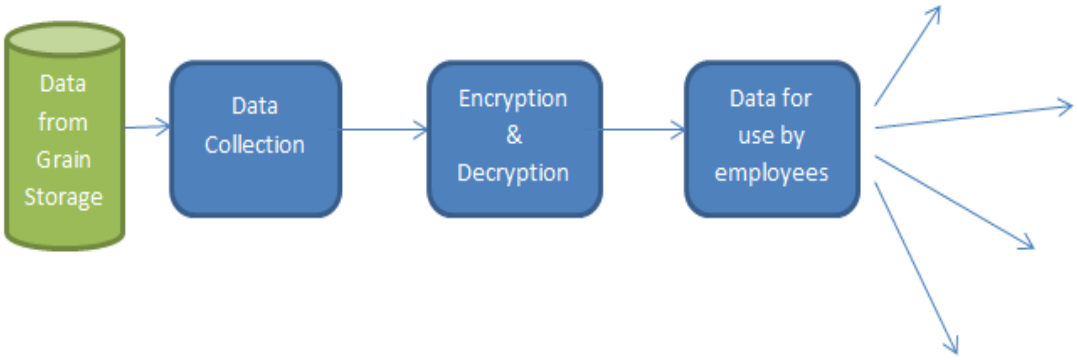


Figure 4.1 Execution of the Proposed Methodology

Figure 4.3 shows the actual grain storage in the CSIO laboratory where the grains are kept under specific temperature and humidity and further experiments are performed. The data from this grain storage is stored in a server for further examinations.

Figure 4.2: Grain Storage System in CSIO

4.4 Methodology

The methodology can be explained with the help of Figure 4.3. Several grain storage chambers as shown are placed at remote locations. The data from these chambers are collected wirelessly by sensors and sink nodes and sent to an expert system via server. The data obtained from each storage is huge, sensitive and vital and should be controlled by the expert only. Hence, a proper security algorithm is needed for the protection of cloud and the encryption process is done so that only the registered users can decrypt and access the data As shown in Figure 4.4, the data first goes through the encryption algorithm using sender's public key and gets converted into cipher text. This cipher text when accessed by the registered user gets converted to the original text through decryption algorithm using Sender's private key. The encryption process takes place at the server end and decryption process takes place at the client's end. Here the three symmetric algorithm DES, AES and Blowfish algorithms are applied. After the comparative study it has observed that Blowfish algorithm outpaced every other algorithm. The parameters have been discussed in the later sections.

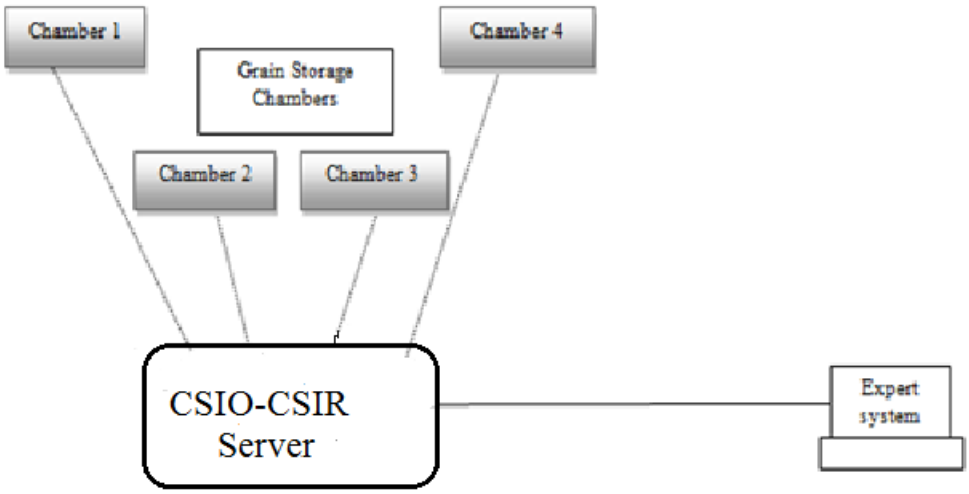


Figure 4.3: Architecture of the Methodology Stated

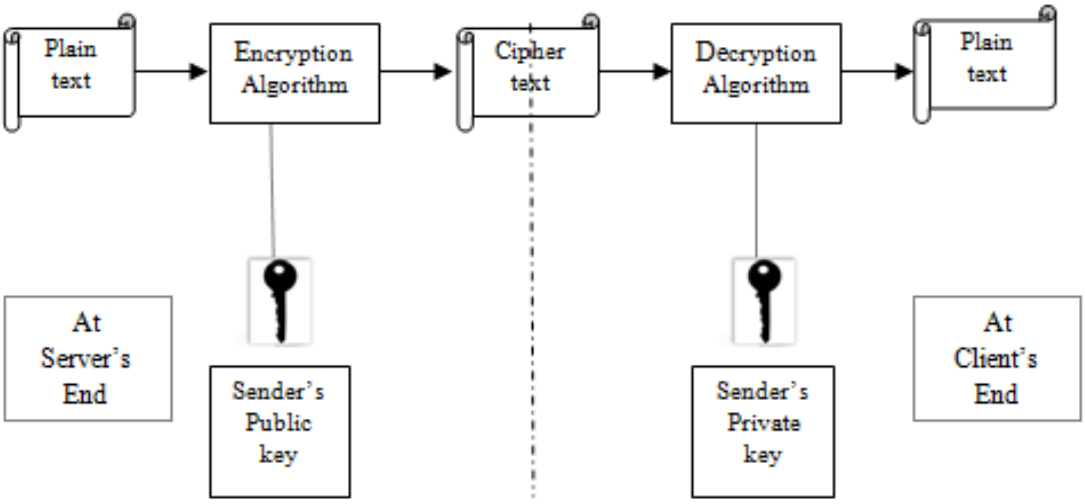


Figure 4.4: Encryption and Decryption Process in Grain Deports system.

4.5 Conclusion

The data from the grain storage that is brought to the remote system is encrypted with the help of DES, AES and Blowfish. After following the above methodology numerical calculations are performed.

The results after performing these numerical operations have been discussed in the next chapter.

Chapter 5

Implementations and Results

Security and performance are used to evaluate the cryptographic algorithms. To reach out to a conclusion that Blowfish algorithm is an efficient security algorithm than AES and DES, various tests are carried out. These include the throughput value, perceived performance, performance based on execution time, convergence of the encryption algorithm and power evaluation. All these parameters have been discussed in detail later.

5.1 Tools for Experimental Setup

For carrying out encryption on the grain storage data, different tools have been used to carry out experiments and each value of the parameter have been calculated based on the experimental results.

i. MATLAB – A matrix library is a programming language which is developed by math works. It is basically used for matrix multiplication, implementation of algorithms and creating other user interfaces. MATLAB is similar to C language, differ in syntax and functions used. The algorithms being compared here have been written in MATLAB to carry out necessary comparison. Main objective is to test the amount of security and efficiency Blowfish algorithm provide in comparison to AES and DES.

ii. Digital Multimeter – Digital multimeter is used to calculate the values of different current and voltage to evaluate value of power consumption for different algorithms.

The rest of the tools consist of Computer system which consists of MATLAB software where there all the data from the grain storage system is brought and encrypted. Different parameters are calculated according to the experimental results obtained.

5.2 Implementation of the Algorithms in MATLAB

Encryption of the data in blowfish algorithm takes place for a 64-bit data and transform into a 64-bit cipher text. The initial part consists of splitting of 64-bit data into two halves. The first p-array (P1) is Ex-OR with the left half of 32-bit data. The result after the Ex-OR operation is passed through the function which is again Ex-OR with the right half of the data. After the completion of Ex-OR operation, the values of the right and left half are swapped. The left half becomes the new right half and the right half becomes the new left half. As shown in the block diagram XL and XR are the left and the right halves of a 64 bit data. X is the input 64-bit data. P1, P2 …. P18 are the P-arrays. The decryption process is just the reverse of the encryption process instead of P1, P18 is used as the input text and they are simply swapped, the rest of P16 to P1 follows the same operation in the reverse direction. The F- function part of the blowfish algorithm is complex part because it involves the use a substitution box. After the 32- bit data passes through the function, splits into 8-bit data each. This 8-bit data passes through four respective S-box and gets converted to 32- bit data after passing their respected S-boxes. As a result after Ex-OR operation 32-bit data is obtained at the end. All the additions are modulo 232 [53]-[55].

i. *P*-arrays are initialized with a fixed string. Here the fixed string used is the hexadecimal digits of pi. S-box is also randomly generated.

ii. Ex-OR *P1* with first 32 bits data, Ex-OR *P2* with its second 32 bits, and so on till *P16*. This cycle is repeated till all the *P*-arrays are Ex-OR.

iii. The output after Ex-OR *P1* and 32-bit data is passed through the function which is again Ex-OR with *XR*.

iv. New *XL* and *XR* are swapped after performing the operation till step 3.

v. Same steps are followed till P*16.*

P17 and *P18* don't require *fiestal* structure mechanism. This round doesn‟t contain F function. The values are Ex-OR with the output generated in previous rounds and are simple swapped.

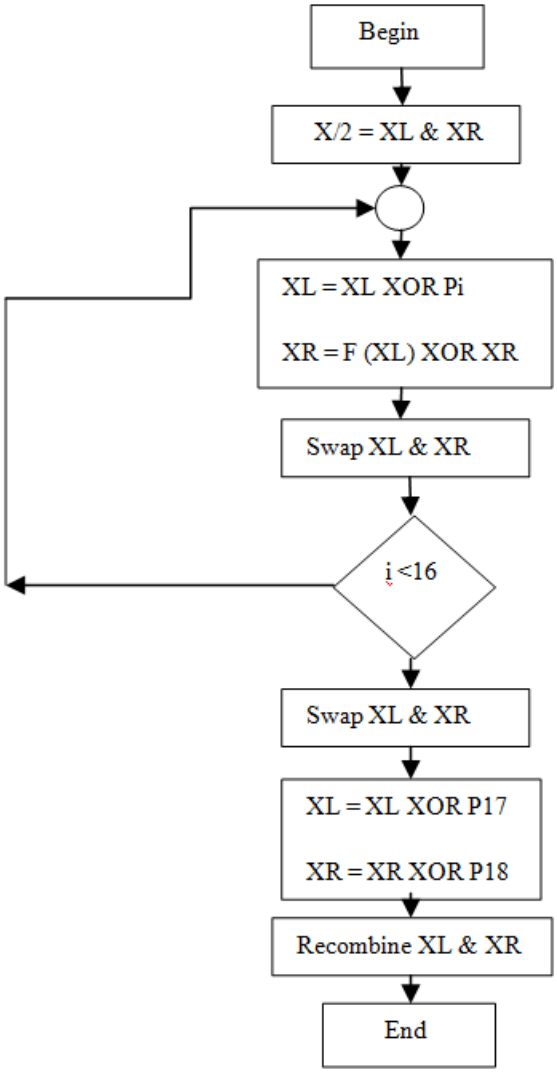


Figure 5.1 Block Diagram of Blowfish Algorithm

Following is the code of Blowfish algorithm which is implemented in MATLAB. The code has been written according to the block diagram of the blowfish algorithm [56] as shown in Figure 5.2

P1 = sscanf(sprintf('%u',14159265),'%2d')'; // Converts the value of Pi to hexadecimal

P2 = sscanf(sprintf('%u',35897932),'%2d')'; numbers.

```
…… it goes till P18
S = sprintf( '%08x',uint32(rand(1,ceil(1024/8)) * 2^32)); // Generates a random S-box
S = S(randi(128,4,256));                                    matrix
text = double('hey what');
half = size(text,2)/2;            // Divides the data into two equal halves
L1 = (text(1:half));
R1 = text(half + 1 : end);
R2 = bitxor(P1,L1);                                  // L1 becomes the new right half
Func = rem(S(1,1) + S(2,1),S(3,1))+ S(4,1);
L2 = bitxor(R1,Func);
R3 = bitxor(P2,L2);
Func = rem(S(1,2) + S(2,2),S(3,2))+ S(4,2);
L3 = bitxor(R3,Func);
R4 = bitxor(L3,P3);
Func = rem(S(1,3) + S(2,3),S(3,3))+ S(4,3);
L4 = bitxor(Func,R4);
R5 = bitxor(L4,P4);
Func = rem(S(1,4) + S(2,4),S(3,4))+ S(4,4); // Swapping goes till P16
L16 = bitxor(Func,R16);
R17 = bitxor(L16,P16);
Func = rem(S(1,16) + S(2,16),S(3,16))+ S(4,16);
L17 = bitxor(Func,R17);
Cipher = cat (2, newL, newR);   // Required cipher text.
```

This code is run in the MATLAB software. Depending upon the input the data can be changed and encrypted to the required form. The user get the Corresponding values of left half and right half by just applying the operations as been discussed in the blowfish block diagram. At the end the user get a cipher text which is in the form of

matrix. The input data cannot be easily obtained by just brute force attack on the algorithm. This algorithm is way too secure and cannot be easily cracked. The codes of AES and DES algorithm have already been implemented on MATLAB. Therefore these algorithm codes were just directly run on the software. A brief idea of the codes of AES and DES algorithm has been shown below.

- DES Algorithm Code

```
mydata='E:\DES\mydata.txt';// For reading the data user enter for encryption
%text1 = fileread('mydata')
fid = fopen(mydata, 'r');
M = fread(fid,'*char')'
fclose(fid)
mydata1='E:\DES\mydata1.txt';
fid1=fopen(mydata1,'w');
fwrite(fid1,M).
times = data_length/8;          // for encrypting the data block by block.
for i = 0:times-1
for j = 1:8
tempdata(j) = data(8*i+j);
end
encrydata = char(tempdata);
encrydata = des(encrydata,ki);
for k = 0:7
temp = encrydata(k*8+1:(k+1)*8);
data_encrypt(i*8+k+1,1) = bin2dec(temp);
end
end
```

- AES Algorithm Code

```
plaintext_hex = {'01' '11' '22' '33' '44' '55' '66' '77' ...  // arbitrary series of 16 plaintext
'88' '99' 'aa' 'bb' 'cc' 'dd' 'ee' 'ff'};

%plaintext_hex = {'32' '43' 'f6' 'a8' '88' '5a' '30' '8d' ...

                '31' '31' '98' 'a2' 'e0' '37' '07' '34'};

 //Convert plaintext from hexadecimal (string) to decimal representation

plaintext = hex2dec(plaintext_hex)

//Convert the plaintext to ciphertext, using the expanded key, the S-box, and the
polynomial transformation matrix

ciphertext = cipher(plaintext, w, s_box, poly_mat,1);

// Convert the ciphertext back to plaintext using the expanded key, the inverse S-box,
and the inverse polynomial transformation matrix

re_plaintext = inv_cipher (ciphertext, w, inv_s_box, inv_poly_mat,1);
```

To make a comparison on different symmetric encryption algorithm data obtained from the grain storage chamber is used. This data is transferred to the main expert system which is basically a Compaq computer with Core i5 processor, GB RAM with MATLAB 2016a installed into it. The data is then encrypted with three different algorithms and performance parameters are evaluated to make necessary comparisons.

5.3 Experimental Results

Following are the parameters on which the comparisons regarding which algorithm to be used are discussed. The experimental results after running each algorithm and calculating the value of each parameter make a fine comparison among the algorithms which have been discussed.

5.3.1 Algorithms Analysis through Throughput

Throughput value of any encryption algorithm is the size of the file encrypted per unit time as shown in Eq.(5.1) [57]. If the value of the throughput is high it means that the algorithm is fast and efficient to encrypt.

$$Throughput = \frac{File \quad Size}{Time} \qquad (5.1)$$

After writing the code in MATLAB for each algorithm, the throughput values are calculated. It is observed that Blowfish algorithm has a high value of throughput for every different value of file size as seen in the table given below. In Table 5.1 as calculated different throughput value based on different file size and corresponding execution time. From the results, it is observed that the Blowfish Algorithm has the highest throughput value and DES algorithm has the least value. More is the throughput, more is the speed of the algorithm and less will be the power consumption. This proves that the Blowfish Algorithm is a highly efficient algorithm with a high speed of encryption. DES and AES have comparatively low speed of encryption hence not as efficient algorithm as Blowfish algorithm. A separate comparison of the algorithms on the basis of power has been done in detail in this thesis.

Table 5.1: Throughput value corresponding to different file size

File size(bytes)	**Time taken to Encrypt (DES) (s)**	**Time taken to Encrypt (AES) (s)**	**Time taken to Encrypt (Blowfish) (s)**	**Throughput (DES) (B/s)**	**Throughput (AES) (B/s)**	**Throughput (Blowfish) (B/s)**
8	0.713	0.132	0.01308s	11.220	60.606	611.246
9	0.872	0.380	0.01249	10.321	23.684	720.115
12	0.918	0.873	0.01369	13.071	13.745	876.104

Grain storage data is encrypted and necessary observation that are made proved that Blowfish algorithm has higher value of throughput. These results are plotted on the graph as seen in the figure. Figure 5.2 shows the throughput value of DES algorithm.

Figure 5.3 & 5.4 shows the throughput value of AES and Blowfish algorithm respectively. From the graph in each figure it is clear that Blowfish has a rising graph and highest value of throughput. AES algorithm shows an increase in the throughput value but as soon as the no of bytes is increased the graph of the algorithm decreases. In case of DES algorithm the throughput value increases, then decreases and then remains constant.

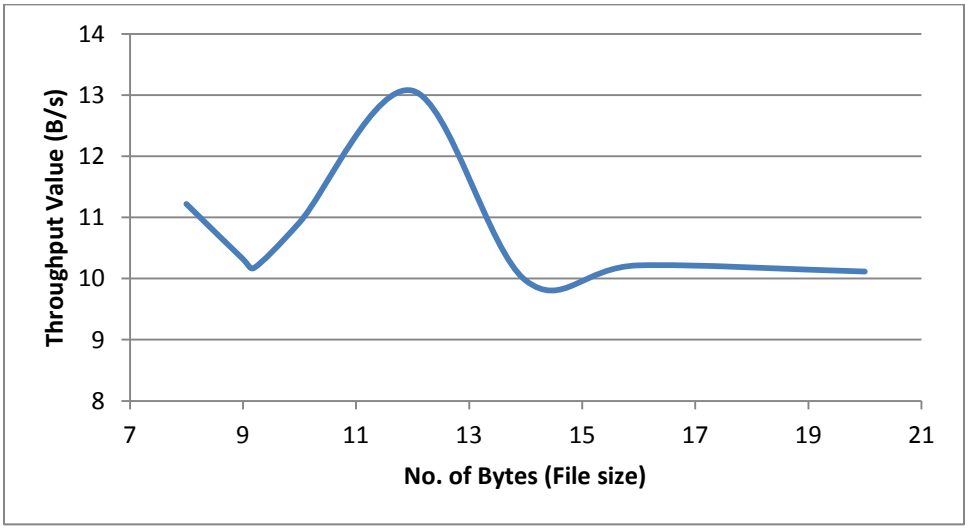


Figure 5.2: Throughput of DES Algorithm.

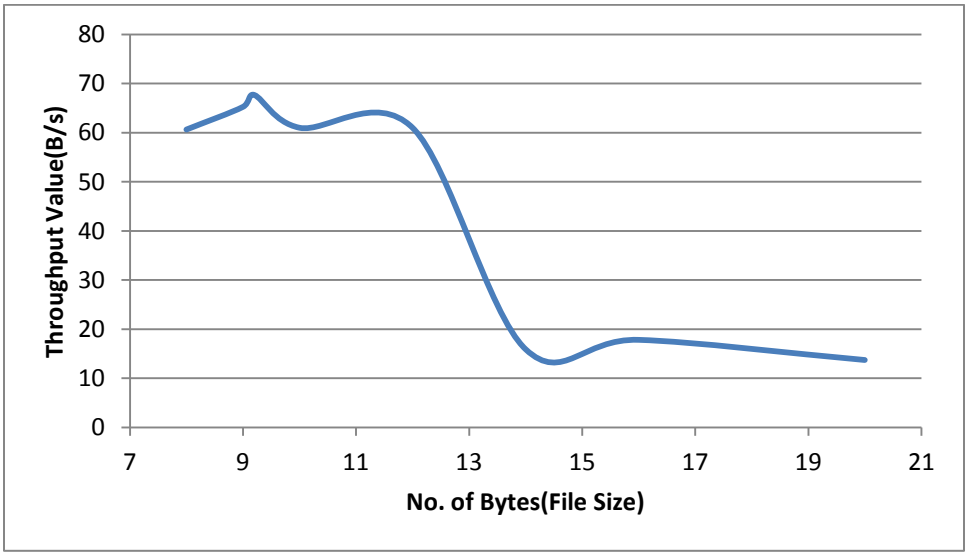


Figure 5.3: Throughput of AES algorithm.

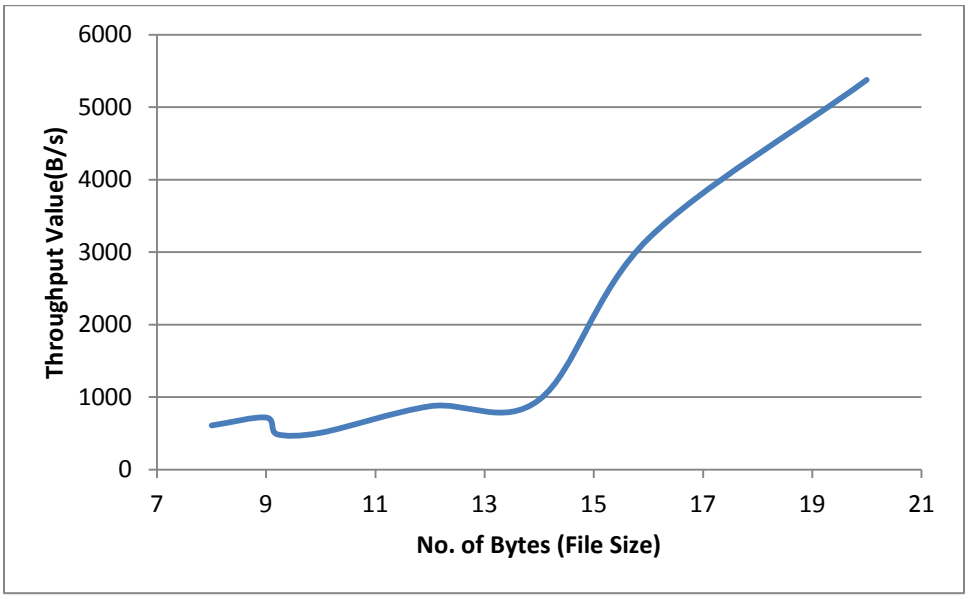


Figure 5.4: Throughput of Blowfish algorithm.

5.3.2 Algorithms Analysis through Performance based on Execution Time

The performance of DES, AES and Blowfish algorithm is evaluated on the basis of execution time. Here performance is inversely proportional to the time taken to encrypt the file [58, 59] as shown in Eq. (5.2). Lesser the execution time, higher will be the performance of the encryption algorithm. Here, the speed of each algorithm is obtained and based on that its performance is evaluated.

$$Performance = \frac{1}{Execution \quad Time} \qquad (5.2)$$

Different performance values based on execution time have been evaluated as shown in the Table II.

Table 5.2: Performance based in Execution Time

Execution Time(DES)(s)	**Execution Time(AES)(s)**	**Execution Time(Blowfish)(s)**	**Performance (DES) (s^{-1})**	**Performance(AES) (s^{-1})**	**Performance(Blowfish) (s^{-1})**
0.713	0.132	0.01308	1.402	7.575	76.452
0.872	0.380	0.01249	1.467	2.631	80.645
0.918	0.873	0.01369	1.089	1.145	73.046

As shown in the Table 5.2, performance for each algorithm based on their execution time is evaluated. It is found that the Blowfish Algorithm has the highest performance as compared to AES and DES algorithm. DES algorithm has overall the lowest value of performance.

5.3.3 Algorithms analysis through Convergence

Convergent of an algorithm implies that the encryption algorithm should produce same cipher text for the same plaintext. If the cipher text remains same for the same plaintext, it means that the algorithm can be cracked easily. But if the cipher text varies for the same plain text it means that the algorithm is highly secure. Since Blowfish algorithm has a random P–array matrix of size 4 X 256 that generates random value matrix, the values of cipher text will vary each time. In the code different values of cipher text have been generated from the same plaintext. It can be concluded that every time the Blowfish algorithm is executed on the plaintext, different value of the cipher text is produced whereas in case of DES and AES same cipher text was produced for the same value of plaintext.

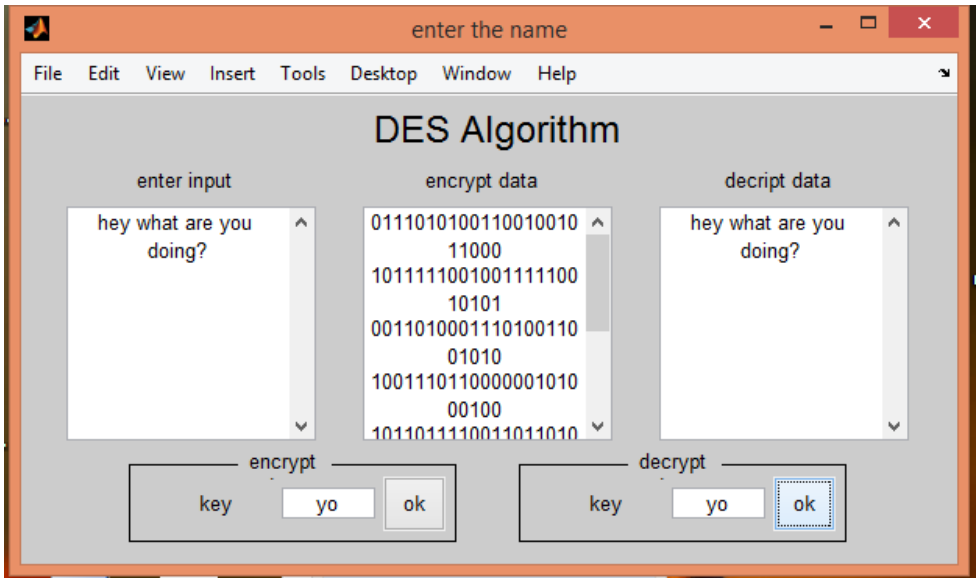


Figure 5.5: Encryption in DES

```
After add_round_key :              5f 57 f7 1d
                                   72 f5 be b9
                                   64 bc 3b f9
                                   15 92 29 1a

State at start of final round :    63 09 cd ba
                                   53 60 70 ca
                                   e0 e1 b7 d0
                                   8c 04 51 e7

After inv_shift_rows :             63 09 cd ba
                                   ca 53 60 70
                                   b7 d0 e0 e1
                                   04 51 e7 8c

After inv_sub_bytes :              00 40 80 c0
                                   10 50 90 d0
                                   20 60 a0 e0
                                   30 70 b0 f0

Round key :                        00 04 08 0c
                                   01 05 09 0d
                                   02 06 0a 0e
                                   03 07 0b 0f

Final state :                      00 44 88 cc
                                   11 55 99 dd
                                   22 66 aa ee
                                   33 77 bb ff

Elapsed time is 3.124481 seconds.
```

Figure 5.6: Encryption in AES

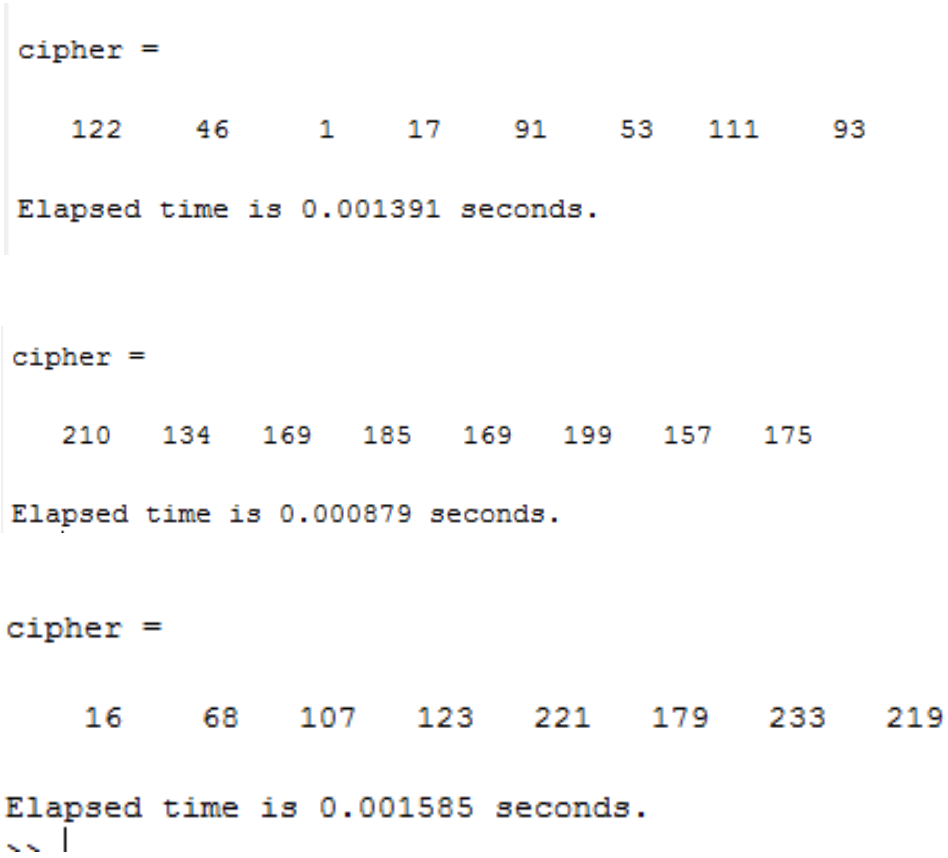


Figure 5.7: Encryption in Blowfish

Some tests have been conducted to check for the convergence of the algorithms. Figures 5.5-5.7 shows the encryption of DES, AES and Blowfish Algorithm respectively. It is observed that when DES algorithm code is run in MATLAB, after encrypting 'hey what are you doing' same value of cipher text was produced every time the algorithm is run. Similar observations are made while running AES algorithm. In case of Blowfish algorithm the results are slightly different as every time the algorithm is run, different value of cipher text is obtained. The advantage here is that the hacker cannot easily crack the text through brute force attack. Each value of plaintext produced different value of cipher. Hence, it can be concluded that Blowfish algorithm is a highly secure algorithm as compared to the other two

algorithms. Since the grain depot data is checked for each algorithm, Blowfish algorithm proved out to be more effective than AES and DES.

5.3.4 Algorithms Analysis through Perceived Performance

Perceived performance means how quickly an algorithm appears to perform a particular encryption or task without any hindrance. Generally real performance increases the perceived performance. It is observed that when the grain storage data is run through the all the three algorithm the data takes time in DES algorithm whereas in case of Blowfish algorithm, the algorithm run fast and encrypt the data in less execution time.

Table 5.3: Execution time for each Algorithm

File size (bytes)	**Time taken to Encrypt (s)**		
	DES	**AES**	**Blowfish**
8	0.713	0.132	0.01308
9	0.872	0.380	0.01249
12	0.918	0.873	0.01369

As seen from the Table 5.3, the execution time for Blowfish is the lowest as compared to DES and AES. The perceived performance of the Blowfish algorithm is therefore higher. Execution time for this algorithm is consistent every time the algorithm is run. The perceived performance of DES and AES are also good but not better than Blowfish.

5.3.5 Algorithms Analysis through Power Consumption

Power Consumption is an important factor for evaluating performance of different Encryption Algorithm. A lot of methods have been proposed to evaluate the power consumption [60]. The method used here to evaluate power is through Powerscope.

Powerscope is a tool which is used to characterize power consumption values of different cryptographic algorithm. Author here proposed that the method combines hardware instrumentation to calculate different current values using some statistical analysis. The power *E* is calculated through the product of current *I* with voltage *V* in a given time interval *I.*

Powerscope is able to calculate fractions of energy consumed in a given time interval. As calculated in the Eq. (5.3) the amount of power consumed is given by the summation of the product of voltage and current in a given time interval. Here suppose there are n samples, so the power calculated over n samples is given below. The advantage of this tool is that a single measured value of the voltage is taken to evaluate power consumption. Here, V_{means} is that voltage of *n* samples.

$$E \cong V_{means} \sum_{t=0}^{n} I_t \, \Delta t \qquad (5.3)$$

where *E* is the Energy evaluated for each Encryption Algorithm, *I* is the value of current calculated for Δt time interval.

Some of the components of Flinn's architecture are profiling computer, data collection computer and energy analyzer are shown in the Figure 5.8. It consists of two phases. First phase is the data collection phase and the second phase is the data analysis phase. During the data collection phase the tool records all the system activity of the profiling computer. It includes the amount of power consumed by the system, the PC/Pid samples, symbol tables, concurrent current levels etc. According to all these system activity an energy profile is generated which is analyzed during the data analysis stage. Since the analysis is done offline there is a least possibility of the profiling overhead. Generally it is zero. Profiling computer here is the mobile or may be a PC on which the application is running and the algorithm is being run. Digital multimeter has been connected here to note the values of voltage and current when the algorithms execute. Energy monitor note the respective current and voltage levels through which a statistics is made by analyzing different values. System monitor is a

user-level daemon process whose structure is similar to that of continuous profiler structure components Morph and DCPI. Energy analyzer communicates with the digital multimeter just to sample different values of current and voltage. Thi architecture is shown in the form of a block diagram in Figure 5.9. It consists of a multimeter which records the value of current in a given interval time *t*. The probes of the multimeter are connected in such a way that the connection is in series. The data collection computer shown in the diagram is the required PC where the program in MATLAB is running. The peaks of the CPU utilization can be viewed from the task manager which changes when the algorithm is executed. Multimeter shows the change in values of voltage and current.

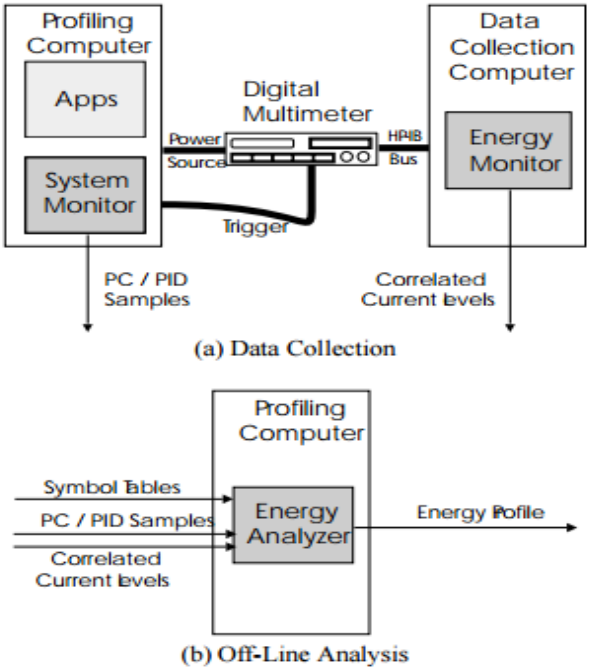


Figure 5.8: Powerscope Architecture [60]

Multimeter is connected to the CPU in series so that current and voltage values can be known once the PC is running. PC has different power consumption and once the application runs it has different power consumption value. All these values are noted to generate an energy profile which is obtained through the analysis of the values

obtained through calculation of different algorithms. First the power is evaluated when the system is idle without running the algorithm. After all the current values are noted for a given time interval the power value is evaluated from the formula given in Eq. (5.3). This will be subtracted from power evaluated while running the algorithm with the same formula [61]. The result gives the value of the power which a particular encryption algorithm requires while running. All the unnecessary power of the unused applications will be eliminated as given in Eq. (5.4).

$$E \cong V_{means} \sum_{t=0}^{n} I_t \, \Delta t \tag{5.3}$$

$$E_{task} = \sum_{t=0}^{n} [P(t_i) - P_{idle}] * T \tag{5.4}$$

where E is the Energy evaluated for the cipher run only. $P(t_i)$ *is* the power evaluated during the execution of algorithm and P_{idle} is the power evaluated when the system is idle for a time interval T .

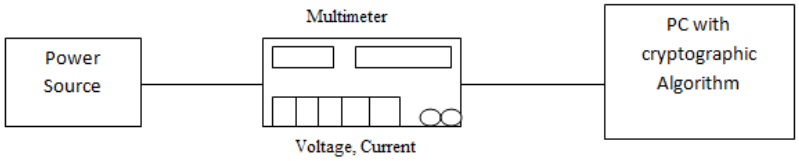


Figure 5.9: Architecture for Power Measurement

According to the block diagram shown connections were made as displayed in Figure 5.10. The power consumption is calculated for different cryptographic algorithms. The experimental results are shown in the Table 5.4.

Figure 5.10: Power Evaluation Setup

Table 5.4: Power Consumption for Symmetric Ciphers

Cipher	**Power Consumption (System and cipher run) (watt)**	**Power Consumption(cipher Run) (watt)**	**Total Energy Consumption (joules)**
DES	745.903	77.92	823.823
AES	736.564	68.59	805.154
Blowfish	641.974	26.227	668.201

Hence from the results it is concluded that Blowfish Algorithm runs fastest and consumes least power that AES and DES algorithm. It is obvious from the result that Blowfish consumes less power because it runs faster and consumes system resources for a short interval of time. DES is least power-effective encryption algorithm. It

consumes large amount of power and therefore it can be said that the algorithm is highly slow. Similar observations can be made for AES which consumes power slightly less than DES but comparatively more than Blowfish. Hence, among the symmetric encryption algorithm, Blowfish algorithm is the most preferred one.

In Figure 5.11 power consumption of Blowfish and DES is shown. Blue line indicates the power consumption of Blowfish algorithm and red line indicates the power consumption of DES algorithm. The average power of blowfish algorithm is 49.10 watt whereas average power consumption of DES algorithm is 50.36 watt. From the figure also it can be concluded that Blowfish algorithm consumes less power. Horizontal axis in the figure is the time in seconds. Power is evaluated for the algorithm in 1 sec interval. Similarly power consumption of Blowfish and AES are also evaluated as shown in Figure 5.12. Blue line indicates the power consumption of Blowfish algorithm and red line indicates the power consumption of AES algorithm. The average power consumption of AES algorithm is 52.63 watt. It can also be clearly seen from the graph that blow fish consumes less power as compared to the DES algorithm.

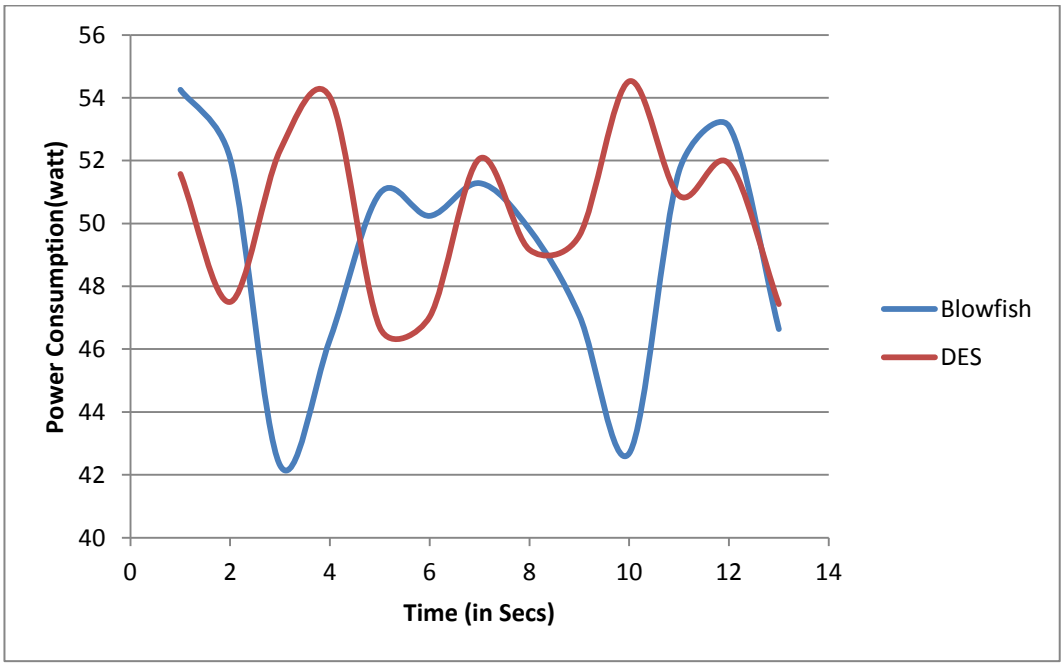


Figure 5.11: Power Consumption of system with Blowfish and DES

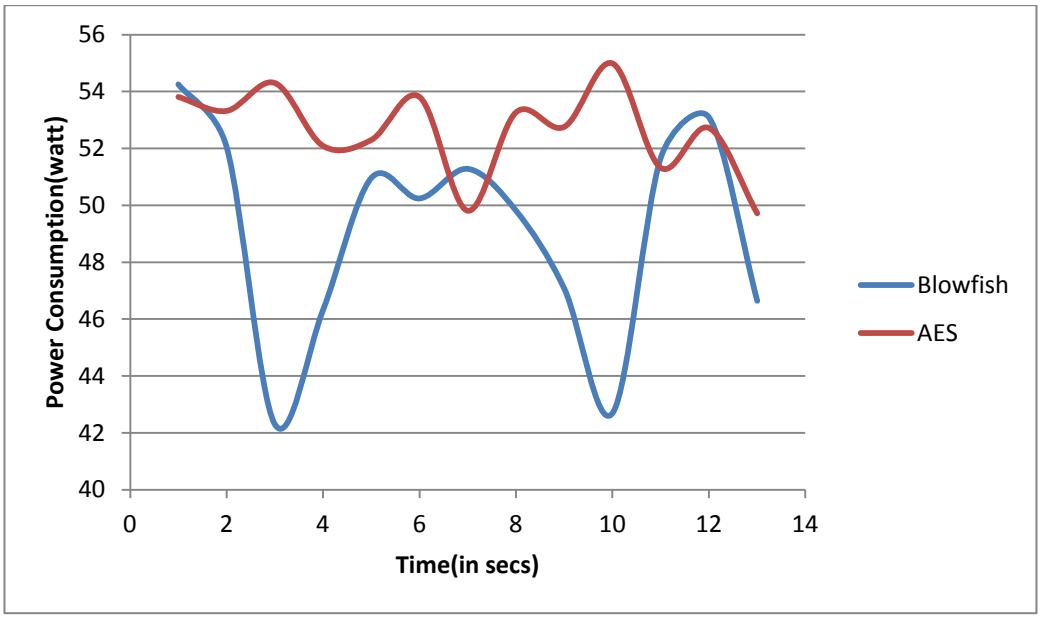


Figure 5.12: Power Consumption of system with Blowfish and AES

5.3.6 Algorithms Analysis through Avalanche Effect

Avalanche effect is the property in which slightly change in the plain text bits makes a huge change in the cipher text bits. It is an attractive property of block cipher and cryptographic hash functions. The avalanche effect is checked in each of the cryptographic algorithm. If the change in the bits is not good enough it can be said that the algorithm is not highly secure. Cryptanalyst can easily figure out the input through his calculations and brute force attacks. This is a property which if present in the algorithm may reduce the effect of any code-breaking attacks. Below Figures.5.13-5.18 show the avalanche effect in AES, DES and Blowfish.

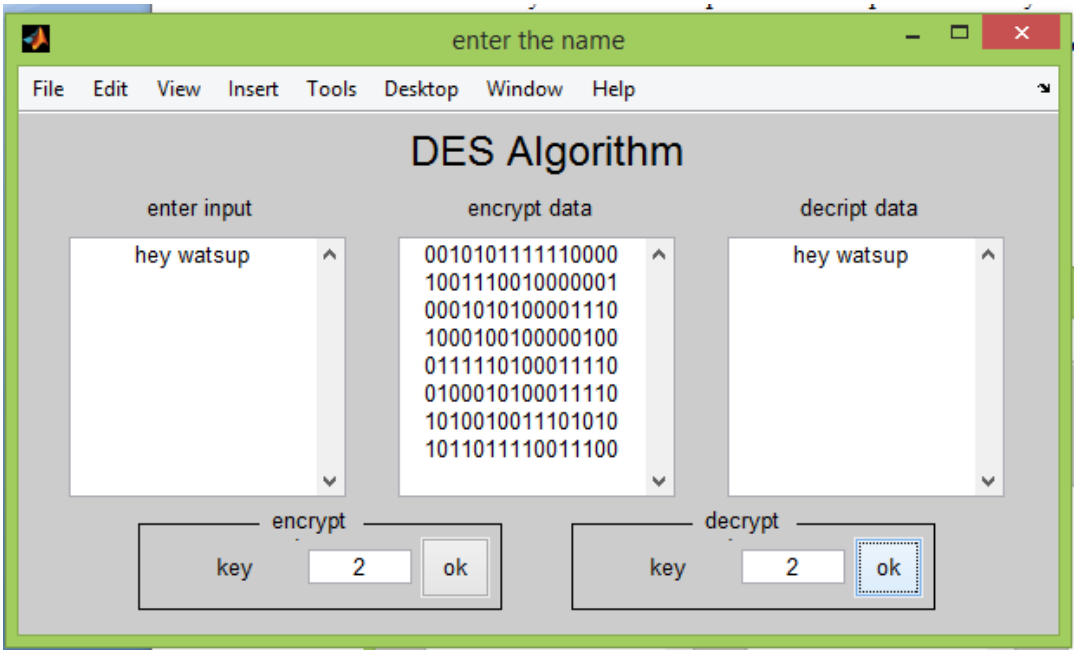


Figure 5.13: DES algorithm before Changing Bit

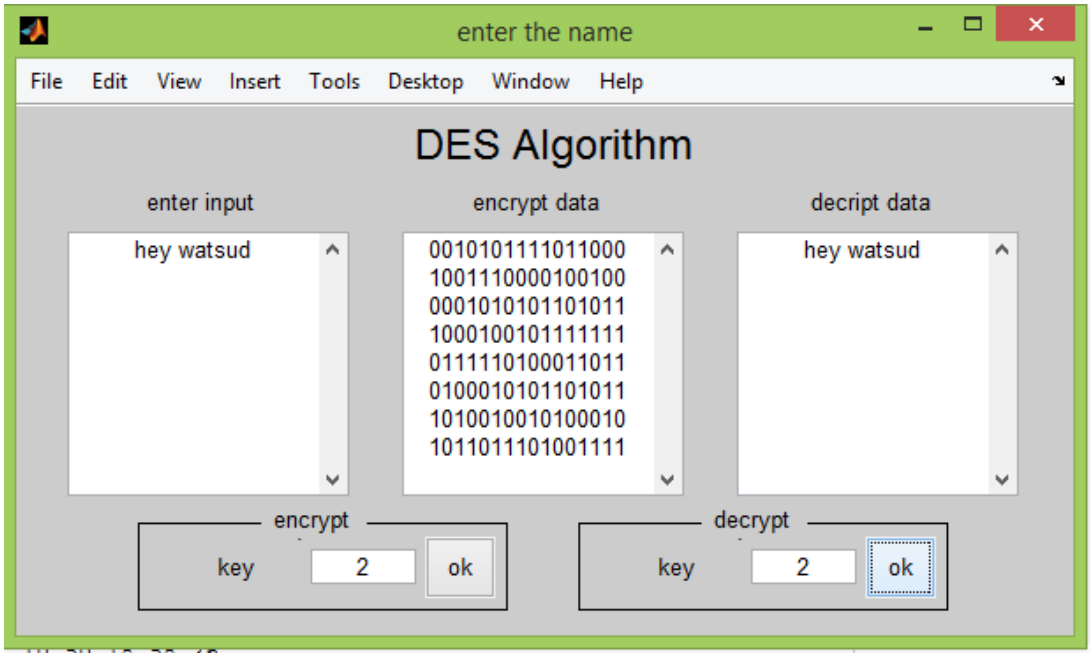


Figure 5.14: DES algorithm after Changing Bit

As shown in the figure above the DES algorithm was run with the text ‘hey watsup’. The bits as can be seen from the tests only the last 4 bits changed. Figure 5.13 shows the tests of the DES algorithm when the bits were not changed. Figure 5.14 shows the tests conducted for DES algorithm after the changing of a bit. The remaining bits remained the same. This shows that the algorithm is not that secure since there is no large change in the number of bits. The same procedure was followed by AES algorithm. The algorithm was run without changing any bit the output in shown in the Figure 5.15. After changing 1 bit there is no change in the output cipher matrix. Figure 5.16 shows the AES algorithm after changing the bit. Here also since the change in the bit is not much AES algorithm is not secure enough.

```
State at start of final round :  63 09 cd ba
                                 53 60 70 ca
                                 e0 e1 b7 d0
                                 8c 04 51 e7

After inv_shift_rows :           63 09 cd ba
                                 ca 53 60 70
                                 b7 d0 e0 e1
                                 04 51 e7 8c

After inv_sub_bytes :            00 40 80 c0
                                 10 50 90 d0
                                 20 60 a0 e0
                                 30 70 b0 f0

Round key :                      00 04 08 0c
                                 01 05 09 0d
                                 02 06 0a 0e
                                 03 07 0b 0f

Final state :                    00 44 88 cc
                                 11 55 99 dd
                                 22 66 aa ee
                                 33 77 bb ff
```

Figure 5.15: AES algorithm before Changing Bit

Figs. 5.17 - 5.18 show the avalanche effect in Blowfish algorithm. It can be said after looking at the snapshot that the algorithm is highly secure as the change in the bits after change in 1 bit has entirely changed the cipher text. Hence avalanche effect also proved that Blowfish algorithm is highly secure algorithm.

```
State at start of final round :  7c 09 cd ba
                                 53 60 70 ca
                                 e0 e1 b7 d0
                                 8c 04 51 e7

After inv_shift_rows :           7c 09 cd ba
                                 ca 53 60 70
                                 b7 d0 e0 e1
                                 04 51 e7 8c

After inv_sub_bytes :            01 40 80 c0
                                 10 50 90 d0
                                 20 60 a0 e0
                                 30 70 b0 f0

Round key :                      00 04 08 0c
                                 01 05 09 0d
                                 02 06 0a 0e
                                 03 07 0b 0f

Final state :                    01 44 88 cc
                                 11 55 99 dd
                                 22 66 aa ee
                                 33 77 bb ff
```

Figure 5.16: AES algorithm after Changing Bit

```
cipher =

   237   185   150   134   148   250   160   146
```

Figure 5.17: Blowfish Algorithm before Changing Bit.

```
cipher =

   137   222   241   225   246   155   193   243
```

Figure 5.18: Blowfish Algorithm after Changing Bit.

5.4 Conclusion

In this chapter Experimental implementations and results that have been carried out in MATLAB environment have been discussed.

In the next chapter, thesis contribution and future work have been discussed.

Chapter 6

Conclusions and Future Work

The thesis presents a comparative analysis of DES, AES and Blowfish algorithm on grain storage data based on different set of parameters. It is observed from the results that Blowfish algorithm is highly efficient algorithm with a high value throughput and performance based on execution time. It is highly secure and the most power effective algorithm as compared to AES and DES. It is a high speed algorithm yet it is cryptographically secure. Therefore, Blowfish algorithm is favored and is used in many applications in the field of information security.

The code has been written according to the block diagram of the blowfish algorithm and efforts have been made to bring out the best solution to the problem. Results were satisfactory as the comparison made between the algorithms AES, DES, and Blowfish algorithm gave the results as expected.

6.1 Thesis Contribution

i. Implementation of AES, DES and Blowfish algorithm in MATLAB has been done to make a comparative survey on these algorithms.

ii. Encryption CSIO-CSIR grain storage data has been taken to provide security to the data and evaluate which algorithm is to be used.

iii. According to the results Blowfish algorithm has outpaced AES and DES algorithm in each and every parameter.

iv. This proposed method is a contribution for CSIO-CSIR organization to provide data security to their personal and critical data.

6.2 Future work

Future work has been discussed as follows

- Blowfish algorithm is a security algorithm and can be used in any field. In any application which requires data to be protected, Blowfish algorithm can be used.
- Blowfish algorithm has been modified by some of the authors. This modification has been done in the implementation of *F* function in the algorithm. It can be checked if the parameters discussed in this thesis affect the performance of the modified algorithm.
- The modified version of the Blowfish algorithm can be compared with AES, DES and original Blowfish algorithm and check if the modified Blowfish algorithm can be implemented in the field of information security.

References

[1] T. Bala and Y. Kumar, "Asymmetric Algorithms and Symmetric Algorithms: A Review," *International Journal of Computer Applications (ICAET),* pp.1-4, 2015.

[2] W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall, 2005.

[3] "Securitytree"[online].Available:http://www.fotosearch.com/CSP387/k31187726/. [Accessed 11 May 2016].

[4] W. Zibideh and M. Matalgah, "Modified-DES Encryption Algorithm with Improved BER Performance in Wireless Communication," *IEEE Radio and Wireless Symposium (RWS) Phoenix*, pp. 219-222, Jan 2011.

[5] H.Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki, "Round addition DFA for microcontroller implemented the Triple DES," *IEEE Consumer Electronics (GCCE) Tokyo*, pp. 538-539, October 2013.

[6] W. Zibideh. And M. Matalgah, "An Optimized Encryption Framework based on the Modified-DES Algorithm:A Trade-Off between Security and Throughput in Wireless Channels," *IEEE Radio and Wireless Symposium (RWS) CA*, pp.419-422, Jan 2012.

[7] L. Niansheng, G. Donghui, and H. Jiaxiang, "AES Algorithm Implemented for PDA Secure Communication with Java," *IEEE Anticounter. Sec. Ident. Fujian*, pp. 217-222, April 2007.

[8] E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks*," Lecture Notes in Computer Science*, vol. 3494, pp. 507-525, Berlin: Springer-Verlag, 2005.

[9] Y. Zhang and D. Feng, "Equivalent Generation of the S-box of Rijndael," *Chinese J. Computers*, vol. 27, no.12, pp. 1593-1600, December 2004.

[10] W. Millan, "How to Improve the Nonlinearity of Bijective S-boxes," *Lecture Notes in Computer Science*, vol. 1438, pp.181 - 192, Berlin: Springer-Verlag, 1998.

[11] H. Chen and D. Feng, "An Evolutionary Algorithm to Improve the Nonlinearity of Self-inverse S-Boxes," *Lecture Notes in Computer Science*, vol. 3506, pp. 352 - 361, Berlin: Springer-Verlag, 2005.

[12] J. Liu, B. Wei, and X. Cheng,"An AES S-Box to Increase Complexity and Cryptographic Analysis, " *IEEE Proc. of the 19th International Conference on Advanced Information Networking and Applications China*, vol. 1, pp. 724-728, March 2005.

[13] Q. Zhu, L. li, J. Liu, N. Xu, "The analysis and design of accounting information security system based on AES algorithm," *IEEE Machine Learning and Cybernetics Boading*, vol. 5, pp. 2713 -2718, July 2009.

[14] S. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using Steganography, AES and RSA," *IEEE Design and Technology in Electronic Packaging (SIITME) Timisoara*, pp.339-344, October 2011.

[15] V. Mahalle, A. Shahade , "Enhancing the Data Security in Cloud by Implementing Hybrid(RSA & AES) Encryption Algorithm," *IEEE Power, Automation and Communication (INPAC)Amravati*, pp. 146149,October 2014.

[16] P. Deshmukh and V. Kolhe, "Modified AES Based Algorithm for MPEG Video Encryption," *IEEE Information Communication and Embedded Systems (ICICES) Chennai*, pp.1-5, Feb 2014.

[17] J. Bhalla, P. Nagrath, “Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm,” *ISSN International Journal of Scientific and Research Publications*, vol. 3, pp.1-6,April 2013.

[18] A. Mousa, “Data Encryption Performance Based on Blowfish,” *IEEE ELMAR Symposium Zadar*, pp.131-134, June 2005.

[19] M. Wang and Y. Que, “The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm,” *IEEE Computer Science-Technology App. IFCSTA Chongqing*, vol. 2, pp.24-28, December 2009.

[20] N. Palaniswamy, D. Dugar, D. Jain, R. Sarabhoje, “ Enhanced Blowfish Algorithm using Bitmap Image Pixel Plotting for Security Improvisation,” *Education Technology and Computer (ICETC) Shanghai*, vol.1, pp.V1-533 - V1-538, June 2010.

[21] National Institute of Standards and Technology, "Clipper Chip Technology," 30 Apr 1993.

[22] R. Rivest, A. Shamir, and L. Adleman, “A Method For Obtaining Digital Signatures and Public Key Cryptosystems,” *ACM Transactions on Communications*, vol. 21, pp. 120-126, 1978.

[23] T. Nie and T. Zhang “A Study of DES and Blowfish Encryption Algorithm,” *IEEE TENCON Singapore*, pp.1-4, Jan 2009.

[24] G. Krishnamurthy, V. Ramaswamy, G.H. Leela “Performance Enhancement of Blowfish Algorithm By Modifying Its function,” *SPRINGER Innovative Algorithms and Techniques in Automation Industrial Electronics Telecom. Netherlands*, pp 241-244, 2007.

[25] Hongwei Si, Youlin Cai, Zhimei Cheng, “An Improved RSA Signature Algorithm based on Complex Numeric Operation Function,” *IEEE*

Challenges in Environmental Science and Computer Engineering (CESCE) China, Vol.2, pp.397-400, March 2010.

[26] Y. Zheng, Y. Zhu, Hong Xu , "An Application of Low Private Exponent Attack on RSA," *IEEE Computer Science & Education(ICCSE) Nanning* ,pp.1864-1866, July 2009.

[27] U. Somani , K. Lakhani , M. Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," *IEEE Parallel Distributed and Grid Computing (PDGC) Solan* , pp.211-216, October 2010.

[28] LIU Dong- liang, CHEN Yan-ping, Z. H, "Secure Applications of RSA System in the Electronic Commerce," *IEEE Future Information Technology and Management Engineering (FITME) Changzhou*, Vol. 1, pp.86-89, Oct. 2009.

[29] H Zhu, "Mercurial Commitments from General RSA Moduli and Their Applications to Zero knowledge Databases/Sets," *IEEE Computer Science and Engineering WCSE Qingdao*, Vol. 2, pp.289- 292, Oct. 2009.

[30] H.Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki,"Round addition DFA for microcontroller implemented the Triple DES," *IEEE Consumer Electronics (GCCE) Tokyo*, pp. 538-539, October 2013.

[31] E.Biham and A.Shamir, "Differential Cryptanalysis of the Full 16- Round DES," *Proceedings of Crypto'92*, vol. 740, Santa Barbara, CA, December 1991.

[32] P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSI implementations of the triple-DES block cipher," *IEEE Electronics Circuits and Systems*, Vol. 1, pp.76- 79, December 2003.

[33] NIST Special Pubilication 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm," National Institute of Standard and Technology, 2000.

[34] A. I. Pamintuan and G. Daniel, "File replication and distribution system for low bandwidth networks," *in Proc. 2002 International Symposium on Parallel Architectures, Algorithms and Networks*, May 2002, pp. 133.

[35] N. Praveen and D. Sareesha, "Ensuring Data Integrity in Cloud Computing", *IJCSNS International Journal of Computer Science and Network Security*, Vol.14 No.9, Sept 2014, pp.34-38.

[36] Liu Hongwei, Zhang Peng, Liu Jun, "Public data integrity verification for secure cloud storage" *Journal of Networks*. 2013, pp. 373-380.

[37] "Reed Solomon Error correction scheme" [online]. Available: https:// tools.ietf.org/pdf/rfc5510.pdf. [Accessed 11 April 2016].

[38] "Markov Chain Monte Carlo and Applied Bayesian" [online]. Available: http://www.stats.ox.ac.uk/~cholmes/Courses/BDA/bda_mcmc.pdf. [Accessed 15 April 2016].

[39] "Introduction to Markov Chain Monte Carlo" [online]. Available: http://www.mcmchandbook.net/HandbookChapter1.pdf. [Accessed 14 March 2016].

[40] C. Wang , Q. Wang , K. Ren , W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing", *Proceedings of the 29th conference on Information communications*, p.525-533, March 2010.

[41] H. Sharma and M. Arya , "Secure Image Hiding Algorithm using Cryptography and Steganography", *IOSR Journal of Computer Engineering,* Volume 13, Issue 5, pp.1-6, aug 2013.

[42] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to Steganography" *IEEE Computer Society IEEE Security & Privacy*.

[43] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", *IEEE* 2001.

[44] Kelvin Curran, "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence Fall*, vol. 2, Issue 2, 2003.

[45] M. Chen, S. Agaia etal. , "Alpha-trimmed image estimation for JPEG steganography detection," *Systems, Man and Cybernetics IEEE International Conference* pp. 4581, 4585, Oct. 2009.

[46] "Break our watermarking system, second edition" [online]. Available: http://bows2. gipsa-lab. inpg. fr/ [Accessed 14 May 2016].

[47] M. Tiwary, R. Priyadarshini and R. Misra, "A faster and intelligent steganography detection using Graphics Processing Unit in cloud", *Proceedings of International Conference on High Performance Computing and Applications (ICHPCA)*, pp. 1-6.

[48] D. Sun, J. Woods, "Low temperature moisture transfer characteristics of barley: thin-layer models and equilibrium isotherms", *Journal of Agricultural Engineering Research*, vol. 59, no. 4, pp. 273-283, 1994.

[49] D. Sun, "Comparison and selection of EMC/ERH isotherm equations for rice", *Journal of Stored Products Research*, vol. 35, no. 3, pp. 249-264, 1999.

[50] D. Sun, "Selection of EMC/ERH isotherm equations for shelled corn based on fitting to available data", *Drying Technology*, vol. 16, no. 3-5, pp. 779-797, 1998.

[51] D. Sun, J. Woods, “Low temperature moisture transfer characteristics of wheat in thin-layers”, *American Society of Agricultural and Biological Engineers*, vol. 37, no. 6, pp. 1919-1926, 1994.

[52] P. Mandal, “Evaluation of performance of the symmetric key algorithms,” *Jour. of Global Research in Computer Science*,vol. 3, pp.67-70, August 2012.

[53] “Two notions of performance” [online]. Available: https://www. courses.engr.illinois.edu/cs232/sp2009/section/Discussion6/disc6.pdf.

[54] S.Bruce, "Applied Cryptography: Protocols, Algorithms and Source Code in C," *2nd edition, New York: Wiley*, 1996.

[55] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish),” *Fast Software Encryption, Cambridge Security Workshop proceedings* (December 1993), Springer-Verlag, pp. 191-204, 1994.

[56] J. Daemen, V. Rijmen, editors, *Fast Software Encryption, 9th International Workshop,* FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers. Springer, 2002.

[57] A. Hashim” Type-3 Feistel Network of The 128-bits Block Size Improved Blowfish Cryptographic Encryption,” *IJCSNS International Journal of Computer Science and Network Security*, vol.8 No.12, pp. 280-286, December 2008.

[58] S. Eyerman and L. Eeckhout, “System-level performance metrics for multiprogram workloads,” *IEEE Micro*, pp. 42-53, 2008.

[59] B. Amanulla, S. Chakrabarti, S. Singh, "Reconfiguration of Power Distribution Systems Considering Reliability and Power Loss," *IEEE Trans. on Power Delivery*, vol. 27, no. 2, pp. 918-926, 2012.

[60] J. Flinn, M. Satyanarayanan, "PowerScope: a tool for profiling the power usage of mobile applications", *Proc. Second IEEE Workshop on Mobile Computer Systems and Applications*, pp. 2-10, 1999.

[61] L. Zhou, Z. Lu , "Power evaluation methods for data encryption algorithms**"**, *IET software*, vol. 8 , issue 1, pp. 12-18, Feb 2014.

List of Publications

1. A. Verma, P. Guha, S. Mishra, I. Chana, "Performance analysis of Blowfish Algorithm" in Chandigarh science congress Chascon'2016 Punjab University, Feb 2016.[Accepted]
2. A. Verma, P. Guha, S. Mishra, I. Chana, "Comparative Study of Different Cryptographic Algorithms", Volume 5, Issue 2, March-April 2016, 58-63.[Accepted]
3. A. Verma, P. Guha, S. Mishra, I. Chana, "Development of a Cryptographic Algorithm Based on Blowfish for Grain Storage Systems" in IEEE/CAA Journal of Automatica Sinica, May 2016.[Communicated]

Video Presentation

Video URL: https://youtu.be/edQqHh-5R0g

Ankita_thesisF.pdf

ORIGINALITY REPORT

12%	10%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.thapar.edu:8080 Internet Source	2%
2	Submitted to CSU, Fullerton Student Paper	1%
3	www.sersc.org Internet Source	1%
4	Submitted to Thapar University, Patiala Student Paper	1%
5	www.kia.or.jp Internet Source	<1%
6	Submitted to Higher Education Commission Pakistan Student Paper	<1%
7	Lu, Zhe-Ming, Lijian Zhou, and Tingyuan Nie. "Power evaluation methods for data encryption algorithms", IET Software, 2014. Publication	<1%
8	Submitted to Panjab University Student Paper	<1%