A CLOUD COMPUTING MODEL FOR SECURE AND DATA STORAGE IN WIRELESS SENSOR NETWORKS.

FORTINE MWIHAKI MATA

MASTER OF SCIENCE

(Software Engineering)

JOMO KENYATTA UNIVERSITY OF AGRICULTURE ANDTECHNOLOGY

2017

A Cloud Computing Model For Secure And Data Storage In Wireless Sensor Networks.

Fortine Mwihaki Mata

A thesis submitted in partial fulfillment for the Degree Masters Software Engineering of Jomo Kenyatta University of Agriculture and Technology.

2018

DECLARATION

I declare that this thesis is my own original work and has not been presented for award of a Degree in any other university.

Signature _____ Date_____

Fortine Mwihaki Mata

This thesis has been submitted to the School of Computing and Information Technology in partial fulfillment of Jomo Kenyatta University of Agriculture and Technology with our approval as the University supervisors:

Signature_____ Date_____

Dr. Michael Kimwele

JKUAT,Kenya.

Signature_____ Date_____

Dr.George Okeyo

JKUAT,Kenya.

DEDICATION

This thesis is dedicated to my husband and daughter who have been my constant source of inspiration. They have given me the drive and discipline to tackle any task with enthusiasm and determination. Without their love and support this thesis would not have been made possible.

ACKNOWLEDGEMENT

I would like to register my gratitude and appreciation for the significant contribution made by all those who in one way or another supported me during the process of preparing the thesis. Special thanks to: my supervisors Dr. George Okeyo and Dr. Michael Kimwele who gave me the moral support throughout the study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

DTN Delay Tolerant Networks

IOT Internet of Things

EFS Encrypted File System

ISP Internet Service Provider

WSN Wireless Sensor Networks

DAS Direct Attached Storage

SAN Storage Area Networks

CAS Content Attached Storage

RAID Redundant Array of Independent Disks

TLS Transport Layer Security

AES Advanced Encryption Standard

ABSTRACT

Effortless data storage ―in the cloud is gaining popularity for personal, enterprise and institutional data backups and synchronization as well as for highly scalable access from software applications running on attached compute servers. The data is usually access-protected, encrypted and replicated depending on the security and scalability needs. Despite the advances in technology, the practical usefulness and longevity of cloud storage is limited in today‘s systems. This study proposed to provide a solution to the problem of securely storing the client‘s data by maintaining the confidentiality and integrity of the data within the cloud. This study addresses the problem of ensuring data confidentiality (protection against disclosure to unauthorized individual information) against cloud and against accesses beyond authorized rights. To resolve these issues, we designed a data encryption model using hybrid symmetric cryptographic techniques(AES and BLOWFISH) that is in charge of storing data in an encrypted format in the cloud. To improve the efficiency of the designed architecture, the service allows the users to choose the level of severity of the data (which lacks in existing models) and according to this level different encryption algorithms are employed.

Key words*: Data storage, Security, Confidentiality*

CHAPTER ONE:

INTRODUCTION

1.1 Background of the Study

Since its emergence around 2007, cloud computing has become an important part within the IT infrastructure and service-provisioning domain. One of its main pillars is data storage. Due to the ubiquitous accessibility of cloud services, the capability to share data with different stakeholders is becoming an important feature in ICT systems and enables new user participation models.(Gubbi & Buyya, 2013)

The convergence of technologies such as cloud computing, Internet of Things (IoT) and big data will give rise to novel (relatively long experiments) smart applications that regard security and data storage. (Friess, 2013).Monetary and scalability benefits have driven the adoption of cloud storage solutions while their security still remains questionable in terms of being weak and secure. Recent leaks about espionage affairs and large-scale data breaches increased the public perception of the importance of data privacy and security. Both issues are paramount for achieving users‘ acceptance. (Suciu & Vulpe, 2013).

Approaches to strengthen the security of cloud-storage solutions and thus increase user‘s trust have already been proposed but open issues remain. (Birk & Wegener, 2011)

Several trends are opening up the era of cloud computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the Software as a Service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high

quality services from data and software that reside solely on remote data centers. (Buyya & Ranjan,2010)

A cloud computing platform provides easy access to a company‘s high-performance computing and storage infrastructure through web services. With cloud computing, the aim is to hide the complexity of IT infrastructure management from its users. At the same time, cloud computing platforms provide massive scalability, 99.999% reliability, high performance, and specifiable configurability. (Wu & Ping, 2010).These capabilities are provided at relatively low costs compared to dedicated infrastructures.

The fast progression of digital data exchange information security has become an important issue in data communication. Encryption algorithms play animportant role in information security system. These algorithms use techniques to enhance the data confidentiality and privacy by making information indecipherable which can only be decoded or decrypted by party those possesses the associated key. (Madhumita Panda, 2016)

1.2 Problem statement.

Data stored in third party storage systems like the cloud might not be secure since confidentiality and integrity of data are not guaranteed. (Subashini & Kavitha, 2011).

Though cloud computing provides cost-effective storage services, it is a third party service and so, a client cannot trust the cloud service provider to store its data securely within the cloud .Unencrypted data of the client cannot be stored in the cloud because the cloud provider will have access to the data and hence the confidentiality of the data will be lost. Also, amalicious cloud provider (system administrator) can modify the client‘s data and hence, the integrity of the data will be lost. (Neal & Rahman, 2012).

To achieve confidentiality and integrity of the data, cryptographic techniques can be used to encrypt data. Encrypted file systems (EFS) can be used to encrypt the client‘s data within the cloud (Damgard & Jakobsen, 2013). Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating.

As the cloud has matured, reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility.

1.3 Justification of Study.

1.3.1 Justification

The study findings and conclusions will benefit Database designers and administrators in organization, Companies that manage huge amounts of data and potential Database Engineers when formulating strategies and implementing intelligent databases as they will have a clear reflection on improving security and confidentiality of their data. The study findings will serve as an eye opener to Database Engineers and designers who may have existing databases and need to enhance their security. They will be able to see the opportunities provided by this solution. This study will give them alternative strategies in form of confirm results and theirs will be to pick and implement reasonably.

1.3.2 Policy Justification

So far, there is no Company, organization or government outright an ICT policy that governs address impacts of Employing of cloud computing towards secure and robust data storage in wireless sensor networks(Ezell& Atkinson,2013), this study will be a catalyst in helping formulate a policy that will be biased towards address challenges security in data stored in the cloud.

1.4 Research Objectives

1.4.1 General Objective

The general objective of this study was is to investigate a data storage security system that provides solution to factors affecting performance, security and reliability in the cloud computing domain. It was done with the aim of designing the model for securely storing data in the cloud.

1.4.2 Specific Objectives

The specific objectives of this study were:

i. To study the various approaches on secure and robust data storage in wireless sensor networks.

ii. To offer a controlled approach for the problem of security issues from the end users of cloud services.

iii. To design a model that will help organizations encrypt their data before storing them in the cloud.

iv. To test the effect of Cloud computing model towards secures data storage in wireless sensor networks.

1.5 Research Questions

To address the above objectives, the following research questions were used:

i. What are the current mechanisms of distributed storage in wireless sensor networks?

ii. What is the best approach to address data security and confidentiality in cloud computing?

iii. How do we design a data encryption model that will help to secure data in cloud computing?

iv. What are the impacts of the new encryption model on data security in Cloud computing?

1.6 Scope of the Study

The research will focus only on Impact of cloud storage towards secure and robust data storage in wireless sensor networks within an organization.

1.7. Limitation of the study.

i).Robust Data Storage

A sensing system stores the raw data collected from different types of sensors, or the information derived from them, in its distributed database on the Internet. The database may be deployed on nodes under a single, loose administration or multiple cooperative administrations like today‘s ISPs. In such large systems, failures of system components (e.g., nodes or links) are the norms, rather than the exceptions. The database needs to be highly available and durable in the face of such failures.

ii).Robust Data Collection

Robust collection of aggregate data from wireless sensors is challenging due to the following factors:

a). High transient loss rates: Due to their harsh deployment environment and low- power radio hardware, sensors experience high communication loss rates

b). Long-term dynamics: The operating condition of a long-running wireless sensor network may change over time.

1.8 Structure of thesis

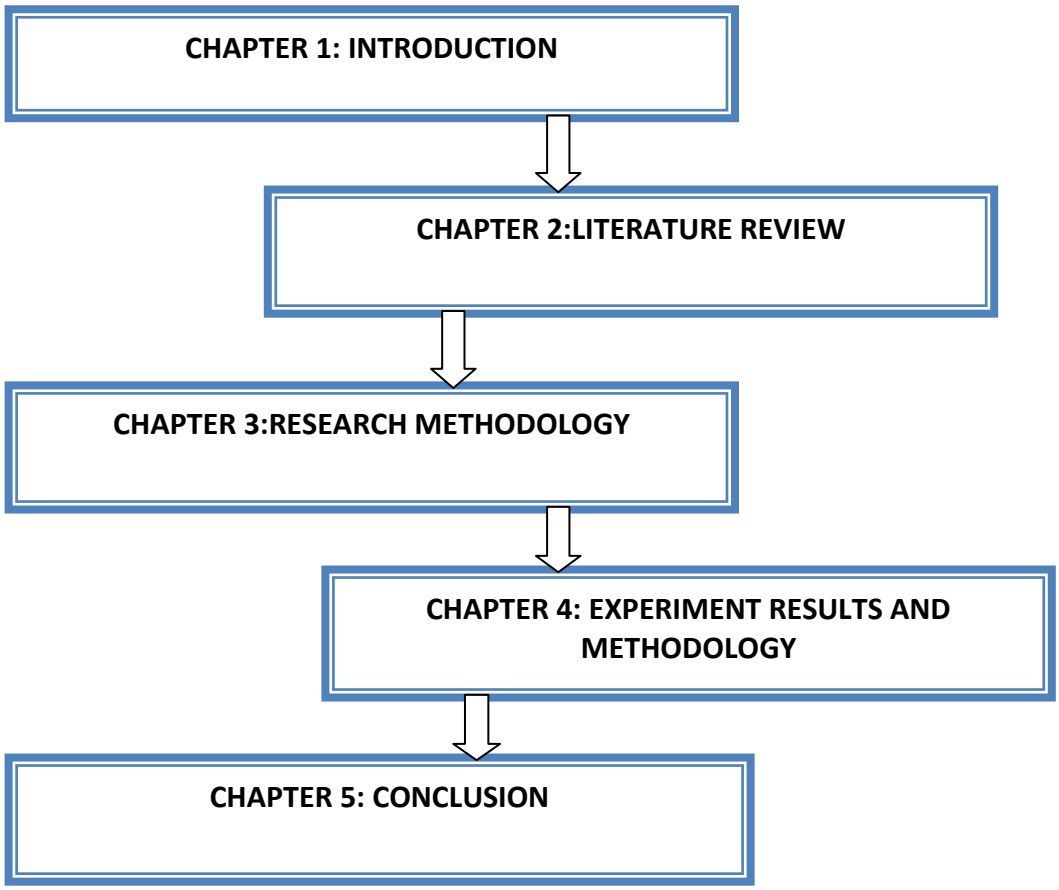


Figure 1.Structure of the Thesis

.

CHAPTER TWO:

LITERATURE REVIEW

2.1*:* Introduction.

In this chapter, the research focuses on theoretical framework, existing theories relating to the impact of employing various data storage systems towards robust data storage in wireless sensor networks. The research will mainly focus on Cloud data storage.

2.2: Wireless Sensor Network

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.

Most of the research done in the field of wireless sensor networks focused in-network support and disregard the backend that has to deal with the immense storing and processing requirements.

This section shows that although there are studies involving the integration of WSN with the Cloud, transparent integration with heterogeneous Cloud computing systems is still a recent topic.

Wireless sensor networks are becoming increasingly common and we believe they are an important part of the future of machine-to-machine communication and the Internet of Things.(Wan & Zou, 2013)

Nowadays, acquiring the required infrastructure and programming the backend to deal with all the requisites of a WSN is a cumbersome task at best. (Conzon &Brizzi, 2015)

The best way of implementing the backend is to take advantage of the emerging Cloud Computing paradigm. The future state described as the Internet of Things will become a reality provided by the proliferation of WSN. For that end, perhaps the most important part of WSN, the backend, needs to be seriously addressed. In the next section, we detail the architecture for our proposed cloud middleware solution that will tackle this issue. . (Wan &Zou, 2013)

Experience on building applications is showing several common properties of wireless sensor networks.

First, with a range of only a few hundred feet at most, sensors often use multi-hop communication; i.e., they relay data through neighboring nodes to the base station.

Second, battery is generally the only source of energy, and it is not feasible to re- place batteries in most sensor deployments. Therefore, it is necessary to minimize energy consumption in order to maximize sensors‘lifetime.

Third, although communication, processing, and sensing, all consume energy, communication is the single most expensive operation. (Younis et al 2006)

A key shortcoming of current research efforts is a lack of consideration of the WSN backend.

Since the nodes of a sensor network have very limited storage and processing capabilities,

sensor networks rarely, if ever, operate in isolation and are usually connected to a backend

modeling infrastructure.(Lee& Murray, 2010)

Even if the WSN is being designed in a special-purposed way to allow some processing within the network, the results are usually stored outside the network where they can also be further

analyzed. A recent literature is an example of the previously mentioned type of network where the concept of collector nodes is introduced.

These nodes are better equipped with processing, storage and battery capabilities compared to the ordinary sensors. The collector nodes receive the data from the spatially distributed sensors and perform complex in-network computations according to the application needs. (Younis et al 2016).

The integration of Sensor Networks with Internet is one of the open research issue in Wireless Sensor Networks. Although it makes a lot of sense to integrate sensor networks with the Internet, there is need to consider that the number of sensor nodes could be so large that it becomes impossible to allocate a MAC address for each one of them. (Yang,2014).

2.3 Data storage

Data storage is a general term for archiving data in electromagnetic or other forms for use by a computer or device. Different types of data storage play different roles in a computing environment. In addition to forms of hard data storage, there are now new options for remote data storage, such as cloud computing, that can revolutionize the ways that users access data.

2.3.1Direct-attached storage (DAS)

Direct attached storage is a digital storage directly attached to the computer accessing it. (Prahlad & Schwartz 2009). Most PCs and many servers come with DAS already installed, and if there is a need to add more direct attached storage, generally all that is required is to purchase is a storage device and possibly a cable. Examples of DAS include had drives, solid-state drives,optical disc drives, and storage on external drives.

DAS is used if you only need storage attached to one server or workstation. DAS is not networked and therefore is accessed through the server or workstation that it is attached to

through a host bus adapter. The main downside to directly attached storage is that it‘s a dedicated resource for (usually) a single computer, and it can‘t be managed over a network. (Velte et al 2010)

2.3.2 Storage area Network

This refers to a network of storage devices that provides block-level storage for servers in a data center. (Therrien et al, 2007) For large organizations with many servers, SAN offers better performance and flexibility than DAS, along with potential cost savings, although SAN hardware can be costly.

SANs are complex because computer networks are (usually) complex. This is especially true in environments where SANs are commonly needed. SANS will need dedicated IP addresses. Multiple addresses, probably going to different switches. SAN implementations sometimes involve virtual networks, switching rules, and planning for the physical wiring.

Storage area network is mainly used in defining the current user applications and supporting storage resources and mapping those to new infrastructures. This in turn provides a comprehensive overview of customer storage requirements and options and can be used as a blueprint for further development of the network. (Velte et al 2010)

2.3.3: Content-addressable storage,

Content addressable storage is a mechanism for storing information that can be retrieved based on its content, not its storage location.(Koller&Rangaswami,2010).It is typically used for high-speed storage and retrieval of fixed content, such as documents stored for compliance with government regulations. Roughly speaking, content-addressable storage is the permanent-storage analogue to content-addressable memory.

Content management systems have traditionally been based on computer systems and programs adapted to solely manage contents that already exist, such systems commonly being referred to as asset management systems. These asset management systems are capable of managing and providing long-term archival of large number of documents and various content objects and the systems are typically used by e.g. advertisement agencies or large enterprises. Also, systems for management of contents including the tasks of planning, creating and organizing contents for electronic publication e.g. on the Internet have been on the market. The search logic was incorporated into the disk controller. A query expressed in a high-level query language could be compiled into a search specification that was then sent to the disk controller for execution. (Sclater 2008).

2.3.4: RAID (redundant array of independent disks)

RAID is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both. (Call et al 2014)

Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemas, or data distribution layouts, are named by the word RAID followed by a number, for example RAID 0 or RAID 1. Each schema, or a RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity. RAID levels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives. According to support.microsoft.com (2014) Microsoft Windows NT Advanced Server supports only RAID 0, RAID 1, and RAID 5. Fault tolerance and disk array implementations, while generally based on the design described here, vary considerably among manufacturers.

2.3.5 Cloud Data Storage

Cloud storage refers to saving data to an off-site storage system maintained by a third party.(Dunham, 2013). Instead of storing information in the computer's hard drive or other local storage device, you save it to a remote database. The Internet provides the connection between the computer and the database. On the surface, cloud storage has several advantages over traditional data storage. For example, data is stored in cloud storage system; you'll be able to get to that data from any location that has Internet access. You wouldn't need to carry around a physical storage device or use the same computer to save and retrieve your information. With the right storage system, you could even allow other people to access the data, turning a personal project into a collaborative effort.

Therefore cloud storage is convenient and offers more. With cloud storage, data is stored on multiple third-party servers, rather than on the dedicated servers used in traditional networked data storage(Rosenthal & Mork, 2010).When storing data, the user sees a virtual server- that is, it appears as if the data is stored in a particular place with a specific name. But that place doesn‘t exist in reality. It‘s just a pseudonym used to reference virtual space carved out of the cloud. In reality, the user‘s data could be stored on any one or more of the computers used to create the cloud. The actual storage location may even differ from day to day or even minute to minute, as the cloud dynamically manages available storage space. But even though the location is virtual, the user sees a ―static‖ location for his data and can actually manage his storage space as if it were connected to his own PC.

2.4 Storage in wireless Sensor network.

WSNs are composed of a set of wireless devices called sensor nodes which comprise of processing, communication, storage, and sensing modules(Yick &Mukherjee, 2008).

The sensing module is referred to simply as a sensor. Sensor nodes can also be equipped with an actuator to perform certain tasks such as opening a door or turning a machine on .The information sensed by the sensor nodes can either be processed locally, or sent over to a more powerful sink node for processing. (Wood & Virone, 2006).

A sink node can exist on site, or be reached through some type of network infrastructure such as Wi-Fi, cellular, or satellite network. In Delay Tolerant Networks (DTNs), network connectivity is not available all the time. For example, consider a WSN where a sink node is not available all the time. Instead, a sink node visits the network occasionally to collect data from sensor nodes. (Yick & Mukherjee, 2008)

2.5 Cloud Computing Definitions

There are a number of definitions of the term cloud computing given in the literature. In fact, the term itself refers to a new technology concept that is still changing and developing. Although several definitions are proposed to reflect the essential characteristics of this new computing paradigm, each definition focuses on certain features and characteristics. Pavithra &Ramadevi, (2012)point out that asset of minimum features found in most definitions lists virtualization, pay-per-use utility model and scalability, with virtualization considered as the main technology behind cloud computing. Nevertheless, there are many other features and characteristics, such as provisioning, usability, and data and process out sourcing, that should be considered to produce a more comprehensive definition. Although the 16th version of the definition of cloud computing published by the US National Institute of Standards and Technology (NIST) is widely adopted

and well-defined, the definition of cloud computing proposed is more comprehensive because it covers more aspects, such as usability, and the definition is as follows:

―Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized Service-Level Agreements (SLAs)‖ Formulating the definition can be another approach for achieving a better understanding of the fundamental elements of cloud systems from a technical point of view. For example, the initial formulation definition proposed in conceives the cloud model as equations that reflect the relation between the essential cloud components, such as data centres, hardware machines and locations, which are used to construct the cloud. A definition of cloud computing must recognize the fundamental characteristics that make cloud computing services valuable and distinguishable. The NIST pointed out most of the characteristics that are widely used among the cloud computing community and these characteristics include:

On-demand self-service. Cloud computing resources (e. g. CPU, storage, software) are provided as needed and scheduled without requiring human interactions with a service provider. The key points of this feature are timesaving, cost effectiveness, usability and the range of services provided.

 Broad network access. Cloud services are accessed through a widely accessible network, mainly the internet, which uses standard protocols and mechanisms to support various types of devices and platforms e.g., smart phones, thin clients, and PDAs.

Resource pooling. The physical cloud resources, based on virtualization technology, are shared among cloud users, depending on their consumption demands. The users are not aware of the physical limitations of resources as they are virtually provisioned and de-provisioned automatically according to demand.

 Measured service. As the service is provided under the pay-as-you-use business model, the usage of services and resources can be metered and automatically billed for each particular user session.

2.6 Secure and Robust Data in Cloud Computing

Cloud computing is a promising, evolving Internet computing of this era (Qi &Gani, 2012).It presents the users with a secure storage for storing the documents online wherein the users can take the benefit of privilege to access it remotely avoiding the usage of the data storage services. The companies which use the newly developed cloud computing model purchase the computing resources with the capabilities of scalability of expanding the resources, providing on-demand privilege with a little or no up-front IT infrastructure investment cost. (Kalpana& Singaraju,2012).

Users generally pay for their cloud data storage on a per-consumption, monthly rate. Although the per-gigabyte cost has been radically driven down, cloud storage providers have added operating expenses that can make the technology more expensive than users bargained for. Cloud security continues to be a concern among users. Providers have tried to deal with those fears by building security capabilities, such as encryption and authentication, into their services .The most common use cases are cloud backup, disaster recovery and archiving infrequently accessed data. A greater number of customers also use cloud storage services for DevOps as a capital cost-

cutting measure. They can just spin up the compute and storage resources for the duration of the project and then spin them down when it ends. (Yick & Mukherjee, 2008)

Cloud storage differs from traditional storage in that most but not all cloud storage offerings are built on an object-based storage platform. The reason for this is that object-based storage platforms can scale to massive levels of capacity and still deliver a very high level of performance. (Kulkarni &Waghmare, 2012)

Although cloud storage gateways are designed primarily as a mechanism for making cloudstorage accessible using standard file-based protocols, it's common for vendors to design gateway appliances with features designed to enhance the use of cloud storage. (Prahlad& Muller, 2014)

Some vendors include local storage within cloud gateway appliances. This storage is commonly used for caching purposes. Files that are read the most frequently might be copied to a local read cache so data doesn't have to be remotely retrieved each time it's needed. Read caching provides a better all-around end-user experience. (Kulkarni &Waghmare, 2012)

Similarly, most cloud storage appliances have a write cache. The write cache is important because data can be written to local storage faster than it can be to cloud storage. Having a write cache allows the appliance to quickly store data during write bursts and then copy that data to the cloud storage as available bandwidth allows. (Kulkarni & Waghmare, 2012)

It is highly recommended that businesses have an emergency backup plan ready in the case of an emergency. Cloud storage can be used as a back-up plan by businesses by providing a second copy of important files. These files are stored at a remote location and can be accessed through an internet connection.(Coyne & Hajas, 2016)

Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

However there are concerns with the safety and privacy of important data stored remotely. The possibility of private data commingling with other organizations makes some businesses uneasy (Bahga&Madisetti2013).

Also several cloud storage services have a specific bandwidth allowance. If an organization surpasses the given allowance, the additional charges could be significant. However, some providers allow unlimited bandwidth. This is a factor that companies should consider when looking at a cloud storage provider.(Prahlad& Muller, 2012) .

2.6: Review of existing approaches for cloud data security

Different factors such as integrity of data, data dynamics and data privacy affects. The performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications.

2.6.1 MAC (Message Authentication Code)

It can be used to protect the data integrity. Dataowners will initially locally maintain a small amount of MACs for the data files which are to be outsourced. The data owner can verify the integrity by recalculating the MAC of the received

data file when he/she wants to retrieve data and will compare it to the local pre computed value but if the data file is large, MACs cannot be employed.(Dhinya&Nithya,2013)

2.6.2 Hash Tree

For large data file a hash tree can be employed, where the leaves are hashes ofdata blocks and internal nodes are hashes of their children of the tree. The data owner only needs to store the root hash of the tree to authenticate his received data. But it does not give any assurance about the correctness of other outsourced data.(Bharan Makhija et al,2013)

2.6.3 TPA (Third Party Auditor)

It relieves the burden of data owner of local data storage andmaintenance; it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. An auditing service helps to save data owner‘s computation resources and provides a transparent yet cost-effective method for data owners to gain trust in the cloud. It eliminates the involvement of the client through the auditing of whether his data stored in the cloud. The author Abhishek Mohta, R. Sahu and L. A wasthi have given algorithm which ensures data integrity and dynamic data operations. They have designed algorithm for data manipulation, insertion of record and record deletion. Insertion and manipulation algorithms inserts and manipulate data efficiently but in data deletion we can‘t identify the person who have deleted record, how and when means if any one deletes record then this algorithm can no longer work.(Abhishek et al,2012)

2.6.4 Indexing Scheme

If we trace every record by index we can easily identify which user isaccessing the record and deleting the record as we have traced him by index. (Sun-Ho-Lee,2013)

2.6.5 PDP Method

The authors Ateniese et al. are the first who have considered the publicadaptability in their defined \provable data possession. (PDP) method which ensures possession of data files on untrusted storages. For auditing outsourced data their technique utilizes the RSA-based

homomorphic authenticators and suggests to randomly sample a few blocks of the file. However, in their scheme the public audit ability demands the linear combination of sampled blocks which exposed to the external auditor. The goal of a PDP scheme that achieves probabilistic proof of data possession is to detect server misbehavior when the server has deleted a fraction of the file.(Ateniese et al,2007)

Requirements and Parameters: The important performance parameters of a PDP scheme include:

- **Computation complexity**: The computational cost to pre-process a file (at C), togenerate a proof of possession (at S) and to verify such a proof (at C);
- **Block access complexity**: The number of file blocks accessed to generate a proof ofpossession (at S);
- **Communication complexity**: The amount of data transferred (between C and S).

Homomorphic Verifiable Tags (HVTs): Given a message m (corresponding to a file block), wedenote by Tm its homomorphic verifiable tag. The tags will be stored on the server together with the file F.

Homomorphic Verifiable tags act as verification metadata for the file blocks and, besides being unforgettable, they also have the following properties:

- **Blockless verification**: Using HVTs the server can construct a proof that allows theclient to verify if the server possesses certain file blocks, even when the client does not

  have access to the actual file blocks.
- **Homomorphic tags**: Given two values Tmi and Tmj , anyone can combine them into avalue Tmi+mj corresponding to the sum of the messages mi + mj.

2.6.6 Random Mask Technique

uses the public key based homomorphic authenticator and toachieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind, it uniquely integrates it with random mask technique. For efficiently handling multiple auditing tasks, the technique of bilinear aggregate signature can be explored to extend the main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.(Cong Wang et al,2010)

2.7. Proof of retrievability

A keyed hash function hk(F) is used in Proof of retrievability(POR) scheme. The verifier, pre-computes the cryptographic hash of F using hk(F) before archiving the data file F in the cloud storage, and stores this hash as well as the secret key K. The verifier releases the secret key K to the cloud archive to check the integrity of the file F and asks it to compute and return the value of hk(F). The verifier can check for the integrity of the file F for multiple times by storing multiple hash values for different keys, each one being an independent proof. Although this scheme is very simple and easily implementable the main drawback of this scheme is that it requires higher resource costs for the implementation.(Juels A. et al,2007)

Verifier has to store as many keys as the number of check sit wants to perform as well as the hash value of the data file F with each hash key. Computation of the hash value for even a moderately large data files can be computationally burdensome for some clients (PDAs, mobile phones, etc.).

Each invocation of the protocol at archive requires the archive to process the entire file F. This processing can be computationally burdensome for the archive even for a lightweight operation like Hashing. Furthermore, it requires the prover to read the entire file F - a significant overhead for an archive whose intended load is only an occasional read per file, where every file to be

tested frequently . The author Ari Juels and Burton S. KaliskiJr proposed a scheme ―Proof of retrievability‖ for large files using ―sentinels‖. In this scheme, only a single key can be used irrespective of the size of the file or the number of files unlike in the key-hash approach scheme in which many number of keys are used.

2.8 CRYPTOGRAPHIC TECHNIQUES

2.8.1 THE ADVANCED ENCRYPTION STANDARD (AES)

Defination:

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

How AES encryption works

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted.

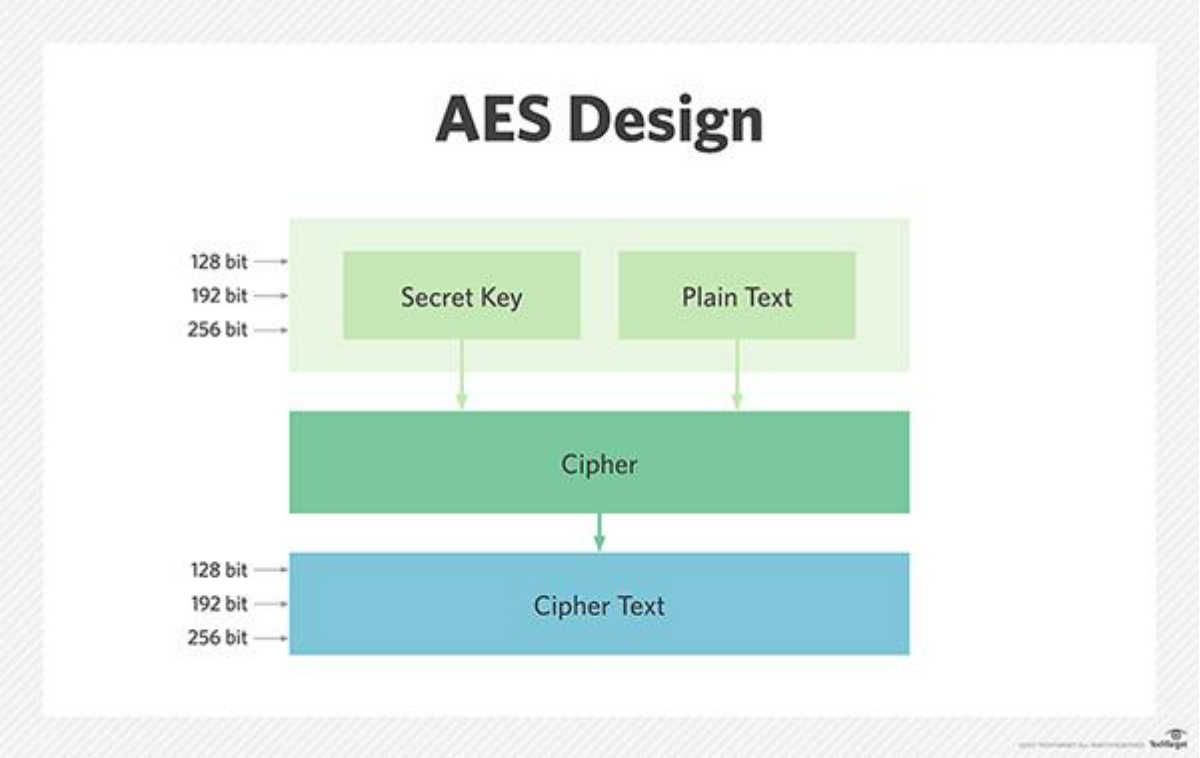


Figure 2 How AES encryption works

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The

number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.

2.8.2 BLOWFISH

Blowfish is a symmetric block cipher that can beeffectively used for encryption and safeguarding of data. Ittakes a variable-length key, from 32 bits to 448 bits,making it ideal for securing data. Blowfish was designedin 1993 by Bruce Schneier as a fast, free alternative toexisting encryption algorithms. Blowfish is unpatented andlicense-free, and is available free for all uses.

BlowfishAlgorithm is a Feistel Network, iterating a simpleencryption function 16 times. The block size is 64 bits,and the key can be any length up to 448 bits. Althoughthere is complex initialization phase required before anyencryption can take place, the actual encryption of data isvery efficient on large microprocessors.

Each line - 32 bits.Algorithm keeps two sub-keyarrays: The 18-entry P-array four 256-entry S-boxes. Sboxes accept 8-bit input Produce 32-bit output. One entryof P-array is used every round. After final round, each halfof data block is XORed with one of the two remainingunused P-entries. The blowfish algorithm Manipulatesdata in large blocksHas a 64-bit block size. It has a scalable key,from 32 bits to at least 256 bits. It Uses simple operationsthat are efficient on microprocessors. e.g., exclusive-or,addition, table lookup,

modular- multiplication. It does notuse variable-length shifts or bit-wise permutations, orconditional jumps. Employs precomputable subkeys.

On large-memory systems, these subkeys can beprecomputed for faster operation. Not precomputing thesubkeys will result in slower operation, but it should stillbe possible to encrypt data without any pre computations.Consists of a variable number of iterations. Forapplications with a small key size, the trade-off betweenthe complexity of a brute-force attack and a differentialattack make a large number of iterations superfluous.

Hence, it should be possible to reduce the number ofiterations with no loss of security (beyond that of the reduced key size).

BLOWFISH ENCRYPTION

Basically, Blowfish encryption algorithm is requires 32 bit microprocessor at a rate of one byte forevery 26 clock cycles. Blowfish contains 16 rounds. Eachround consists of XOR operation and a function. Eachround consists of key expansion and data encryption. Keyexpansion generally used for generating intial contents ofone arry and data encryption uses a 16 round feiesteknetwork methods.

Fig 3 below shows how blowfish algorithmworks.

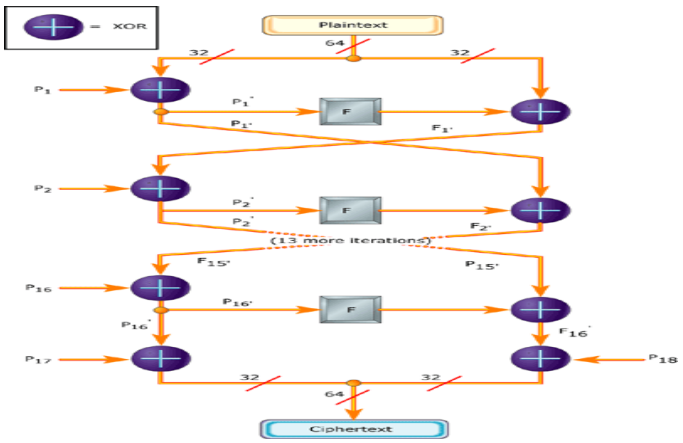


Figure 3 Blowfish encryption

In this description, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value I'll call P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value I'll call F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit ciphertext.

2.8.3. TWO FISH

Twofish is a symmetric block cipher; a single key is used for encryption and decryption. Twofish has a block size of 128 bits, and accepts a key of any length up to 256 bits. (NIST required the algorithm to accept 128-, 192-, and 256-bit keys.) Twofish is fast on both 32-bit and 8-bit CPUs (smart cards, embedded chips, and the like), and in hardware. And it's flexible; it can be used in network applications where keys are changed frequently and in applications where there is little or no RAM and ROM available.

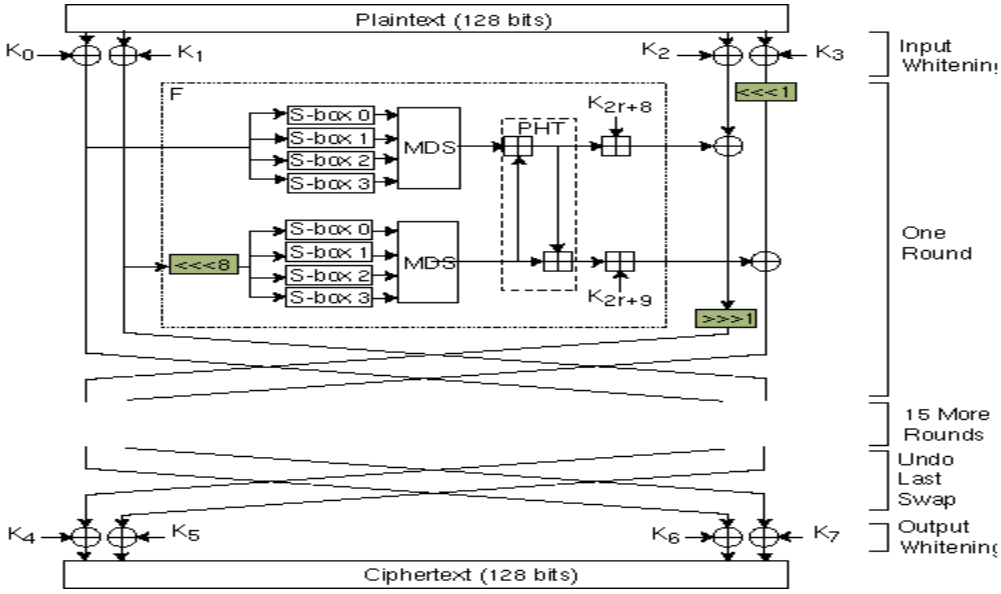


Figure 4 Two fish

As Figure 1 illustrates, Twofish is a Feistel network. This means that in each round, half of the text block is sent through an F function, and then XORed with the other half of the text block. DES is a Feistel network. Blowfish (another Schneier algorithm) is a Feistel network. Five of the AES submissions are Feistel networks. Feistel networks have long been studied in cryptography, and we know how they work.

In each round of Twofish, two 32-bit words (the two vertical lines along the left of Figure 1) serve as input into the F function. Each word is broken up into four bytes. Those four bytes are sent through four different key-dependent S-boxes. The four output bytes (the S-boxes have 8-bit input and output) are combined using a Maximum Distance Separable (MDS) matrix and combined into a 32-bit word. Then the two 32-bit words are combined using a Pseudo-Hadamard Transform (PHT), added to two round subkeys, then XORed with the right half of the text. There are also two 1-bit rotations going on, one before and one after the XOR. Twofish also has something called "prewhitening" and "postwhitening;" additional subkeys are XORed into the text block both before the first round and after the last round.

Each step of the round function is bijective. That is, every output is possible. There has been too many attacks against ciphers that don't have this property not to include it. The round function mixes up operations from different algebraic groups: S-box substitution, an MDS matrix in $GF(2^8)$, addition in $GF(2^{32})$, addition in GF(2) (also called XOR), and 1-bit rotations. This makes the algorithm difficult to attack mathematically.

The key-dependent S-boxes are designed to be resistant against the two big attacks of the early 1990s—differential cryptanalysis and linear cryptanalysis—and resistant against whatever

unknown attacks come next. Too many algorithm designers optimize their designs against specific attacks, without thinking about resistance against the unknown.

Key-dependent S-boxes are not selected randomly, as they are in Blowfish. Instead, they are carefully designed S-box construction rules, and tested them with all possible 128-bit keys (and a subset of possible longer keys) to make sure that all the S-boxes were indeed strong. This approach allows to combine the strength of fixed, strong S-boxes with the strength of secret S-boxes. And Twofish has no weak keys, as Blowfish does in reduced-round variants.

The MDS matrix was carefully chosen to provide good diffusion, to retain its MDS property even after the 1-bit rotation, and to be fast in both hardware and software. This means that we had to search through all possible matrices and find the one that best met our criteria.

The PHT and key addition provide diffusion between the subblocks and the key. And using the LEA instruction on the Pentium (and above), we can do all four additions in just two operations.

The round subkeys are carefully calculated, using a mechanism similar to the S-box construction rules, to prevent related-key attacks and to provide good key mixing. One of the things we learned during this process is that a good key schedule is not grafted onto a cipher, but designed in tandem with the cipher. We spent a lot of time on the Twofish key schedule, and are proud of the results.

The 1-bit rotation is designed to break up the byte structure; without it, everything operates on bytes. This operation exists to frustrate cryptanalysts; it certainly frustrated our attempts at cryptanalyzing Twofish.

The prewhitening and postwhitening seems to add at least a round to the difficulty of any attack. Since eight XORs are cheaper than a round, it makes sense to leave them in.

2.8.4 DES

DES is a ***block cipher***--meaning it operates on plaintext blocks of a given size (64-bits) and returns ciphertext blocks of the same size. Thus DES results in a ***permutation*** among the 2^64 possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

DES (and most of the other major symmetric ciphers) is based on a cipher known as the **Feistel block cipher**. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure (known as a **feistel network**).

As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric,

64 bit **block cipher** as it uses the same key for both encryption and decryption and only operates

on 64 bit blocks of data at a time5 (be they plaintext or ciphertext). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way.

All blocks are numbered from left to right which makes the eight bit of each byte the parity bit.

Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. However, it is generally accepted that the initial and final permutations offer little or no contribution to the security of DES and in fact some software implementations omit them (although strictly speaking these are not DES as they do not adhere to the standard).

Overall structure

Figure 2.2 shows the sequence of events that occur during an encryption operation. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks,*Li* and *Ri* which are then passed into what is known as a **round** (see figure 2.3), of which there are 16 (the subscript *i* in *Li* and *Ri* indicates the current round). Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key6. At the end of the 16th round, the 32 bit *Li* and *Ri* output quantities are swapped to create what is known as the **pre-output**. This [*R*16, *L*16] concatenation is permuted using a function which is the exact inverse of the initial permutation.

The output of this final permutation is the 64 bit ciphertext.

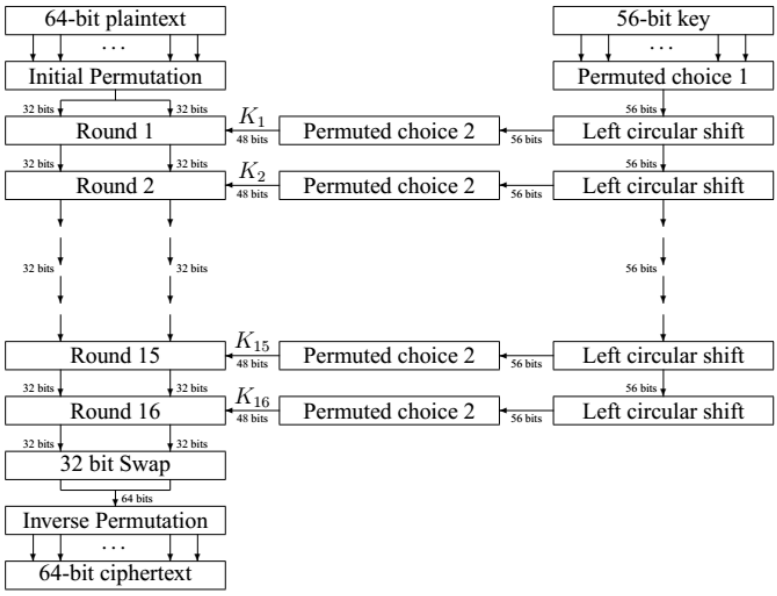


Figure 5 Overall structure

2.8.5. IDEA

Description of IDEA

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process.

Encryption

The functional representation of the encryption process is shown in Figure below The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail.

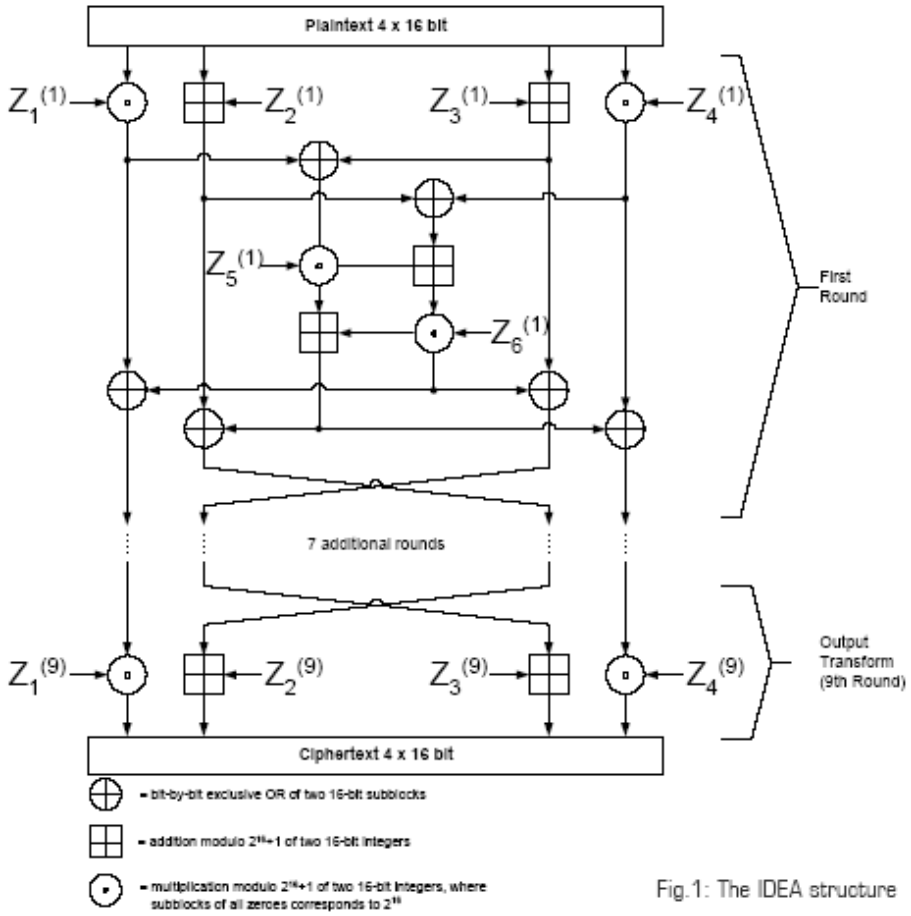


Figure 6: IDEA Encryption

In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^{16}, and with the other two plaintext blocks using multiplication modulo $2^{16} + 1$. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8^{th} encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^{16} and multiplication modulo $2^{16} + 1$ to form the resulting four 16-bit ciphertext blocks.

Decryption

Decryption of the key sub-blocks

Table 2

Round 1	$Z_1^{(9)-1}$ -$Z_2^{(9)}$ -$Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
Round 2	$Z_1^{(8)-1}$ -$Z_3^{(8)}$ -$Z_2^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
Round 3	$Z_1^{(7)-1}$ -$Z_3^{(7)}$ -$Z_2^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
Round 4	$Z_1^{(6)-1}$ -$Z_3^{(6)}$ -$Z_2^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
Round 5	$Z_1^{(5)-1}$ -$Z_3^{(5)}$ -$Z_2^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
Round 6	$Z_1^{(4)-1}$ -$Z_3^{(4)}$ -$Z_2^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
Round 7	$Z_1^{(3)-1}$ -$Z_3^{(3)}$ -$Z_2^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Round 8	$Z_1^{(2)-1}$ -$Z_3^{(2)}$ -$Z_2^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output Transform	$Z_1^{(1)-1}$ -$Z_2^{(1)}$ -$Z_3^{(1)}$ $Z_4^{(1)-1}$

Figure 7: IDEA Decryption

The computational process used for decryption of the ciphertext is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

More precisely, each of the 52 16-bit key sub-blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process as shown in Table 2

2.9 Model framework

The study proposes three security levels in the model which includes basic, confidential and highly confidential.Cloud user

2.9.1. Basic level

The basic level is concerned in encrypting a general type of data like, videos and photos that don not need a high degree of confidentiality. Hence, this level offers a basic level of security and is used by most of the products available online. For that, the study recommends using TLS for encrypting the communication between the application of the client and the server using

HTTPS. TLS guarantees communication privacy between users on the internet. In addition to the TLS. It is important to note that data in the basic level of security will not be encrypted at the client side; it will be encrypted using the encryption key of the backup service after transferring the data on the server side. Many storage service providers use TLS and AES - 256 such as Mozy and Drop box.

2.9.2Confidential level

Confidential level is designed for data with medium confidentiality degree like personal files, photos and videos. In this level, the encryption is done at the client side i.e.it is based on client side encryption. At the confidential level we use AES. The symmetric key block encrypting algorithm with a fixed block size of128-bits and a key length of 128. The mathematical operations in AES are done in 10 rounds for 128-bit keys. Each round consists of multiple processing steps we explained earlier in this section.

2.9.3 Highly confidential level

This level handles the most important data such as financial transactions and military information. Users are very concerned about losing this type of data and still avoid using all the new offered services because of the high confidentiality of the data and the doubts he may have. Therefore, at this level of security the user is provided with a very high degree of confidentiality and integrity by using two recommended algorithms. The first one is the AES-256 encryption algorithm, which is also recommended by the U.S. The second one is the secure hashing algorithm SHA-2.

The algorithm assures integrity of the data. It is performed on the data before sending or uploading it by calculating a hash value. When the user retrieves the

data back, the algorithm calculates the hash value for retrieved data, if the value is the same as the first one then the user can be sure that the data was not tampered

2.9.4 Cloud Architecture

The cloud architecture begins with user interface for the user to interact with the cloud and selecting a task or service (either starting an application or opening a document).After selecting the required service, a request is passed to the system management. In the system management, correct resources are found and then the appropriate provisioning services are called. Later on, these services choose the necessary resources in the cloud, launch the appropriate web application and either creates or opens the requested document. After that, the web application is launched and then the system‘s monitoring and metering functions track the usage of the cloud so that resources are apportioned and attributed to the proper user(s).

2.9.5Cloud Computing Service Deployment Models

Cloud services can be deployed in several models which are classified based on who owns the service and who uses this service. The following is a list of typical deployment models in cloud computing;

2.9.5.1 Private Cloud

The cloud computing services and infrastructure are owned and served by an organisation. A private cloud is used to maximize the utilization of computing resources within the organization. An organization with high security and privacy concerns may find that the private cloud model is the preferred option over other cloud models which involve sharing resources with other

organizations. Furthermore, organizations with mission-critical applications may prefer to rely on their own ability to manage and control their in-house infrastructure.

2.9.5.2 Community Cloud

The cloud resources are owned and used by several organizations that have common requirements and applications .On the one hand, the community cloud adds more cost-effective value than the private cloud as the cost is shared among the organizations involved. On the other hand, the community member organizations need to have some trust relation, especially on the member organization which is responsible for the management of the community cloud. Privacy and security

concerns are limited to the community member organizations.

2.9.5.3 Public Cloud

The term cloud computing is usually used to refer to the public cloud deployment model.
The cloud resources are available to the public mainly through the Internet and provided by

commercial companies. The definition and characteristics discussed in are more related to this delivery model which offers consumers the most cost-effective services but also faces more challenges, particularly in terms of security and privacy. Most of the work of this thesis is about this popular model of deployment.

2.9.5.4 Hybrid Cloud

This model is a combination of two or more other deployment models, i.e., private, community and public clouds. By using more than one model to provide cloud services, the benefits of each

model can be utilized. For example, an organization may use public cloud for part of their application that requires high computation resources but not high security requirement. For applications that require a more secure environment, a private cloud can be used to host the data and applications that require security and privacy. However, moving data between different cloud models or providers faces issues of standardization and cloud interoperability

2.9.5.5 Virtual Private Cloud

The Virtual Private Cloud (VPC) deployment model was first used by Amazon Web Services (AWS) to provide cloud resources via a Virtual Private Network (VPN). The VPN is mainly controlled and configured by the customer [31]. The VPC terminology is not recognized yet in the NIST definition of cloud computing. The AWS offers dedicated physical hardware as an option for VPC customers but it is not an obligation of the VPC service model. The VPC can be considered as an attempt to reach a balance between the benefits of the private cloud and the public cloud that mainly represent the balance between security issues and the benefits of the business model of the cloud [2]. Although the VPC is still a new concept under development, it demonstrates a need to keep the rapid elasticity and cost effectiveness of the public cloud

services while giving the consumer of this service more control of their resource mainly to enhance the privacy and security of their data and applications in the cloud.

2.9.6 Cloud Computing: Issues and Challenges

In cloud computing services, customers are concerned about moving their sensitive data and applications from their own private computing environments to a cloud environment which is shared by different users and which is usually accessible via a public network. Security issues in

cloud computing are generally related to the core technology components on which cloud computing relies. These components are :

2.9.6.1 Web Applications and Services

Are the most used technologies to access cloud computingservices.

2.9.6.2 Virtualization

Is the main technology behind the existence of cloud computing. Both SaaSand PaaS are based on virtualization of the infrastructure provided at IaaS level.

2.9.6.3 Cryptography

Techniques are currently the most common techniques to achieve asatisfactory level of security requirements for cloud computing. Hence, any known vulnerabilities of the above three core technology components can be considered as vulnerabilities of cloud computing systems. For example, HTTP protocol used in web technologies is exposed to session-riding and session hijacking. Therefore, cloud computing systems are vulnerable to this kind of attack and need to overcome this weakness. Virtualization is another vulnerable concern. An attacker can break through the virtual separation and access data and resources either passively by observing data or actively by changing data and configurations In addition, there are various other possible vulnerabilities which can be present in cloud computing systems and they are related to its infrastructure and environment. Since cloud services are usually provided via the Internet, all expected problems related to the Internetare also related to cloud computing. Vulnerabilities in operating systems and other software 30programs installed in a cloud infrastructure can also be seen as being related to cloud computing vulnerabilities. This section reviews several specific security vulnerabilities and issues due to the nature of cloud computing:

2.9.6.4 Unauthorized access to the management interface

In cloud computing, managementinterfaces are typically accessible through public networks for authorized users and possibly unauthorized attackers, while conventional data centres are usually only accessible by authorized administrators directly or via private networks. Moreover, management access is usually conducted via a Web application or service technologies; consequently the cloud management interface is probably subjected to the vulnerabilities of these technologies.

2.9.6.5 Data recovery problem

Due to the nature of virtualization and sharing of cloud servicesat the hardware level, memory and storage areas that have been rented by previous customers can be reallocated to new customers. It is possible that those new customers can recover data from these memory and storage areas which may contains sensitive information belonging to previous customers.

2.9.6.6 Virtual machine (VM) template image vulnerability

A new VM is usually created bycloning a template image of a preconfigured VM as this way saves time and effort. Thus many customers will rent VMs with the same configurations. An attacker can gather information about cloud system template images by becoming a customer of a cloud with administration rights. Once the attacker has access to the template images, he/she can search for vulnerabilities in those images which are also used by other customers.

2.9.6.7 Data leakage possibility

Another vulnerability issue related to the VM template imagesis that cloud providers can use templates created by other customers for new customers. These templates may contain secret backdoors created by an attacker pretending to be a client and allow the attacker to gain access to other customers _virtual machines.

2.9.6.8 Injection vulnerabilities

Since most cloud services use web application services, it ispossible to input malicious codes into a cloud system by making use of the vulnerabilities in such web application services to hack into the web servers housing these services. There are many examples of hacking methods making use of malicious codes, such as SQL codes, OS command or JavaScript codes. Once a web server is compromised, it can be used as a stepping stone by the attacker to hack into the other targets in the system and these targets include databases and operating systems.

2.9.6.9 Security metric and monitoring challenges

Customers are required to be able tomeasure and monitor the security situation of their cloud services and resources. However, providing such capabilities to cloud customers is still a challenge because the available traditional standard tools are not suitable yet for the cloud environment Because the cloud environment has complex and dynamic hierarchical services that may involve different cloud providers, the cloud environment requires novel distributed monitoring capability to fit that nature

2.9.6.10Difficulty in digital key-management and random numbers

In a cloud system, there are different types of keys and random numbers that are necessary for cryptography operations. Managing and storing different keys in a cloud environment are difficult tasks because there is no completely physical isolation between storage resources allocated to different customers. Efficiency in the generation of random numbers mostly depends on the hardware clock used by the random number generator. A lack of such efficiency can be experienced in a cloud environment where, in different sessions, a number of cloud users use the same generation resources at the same time. This may overload the random number generation

resources or might result in weak number generation. Therefore, implementing standard security mechanisms, such as a hardware security module which relies on an efficient random number generation resource, to cloud systems is a security challenge.

2.9.6.11 Cloud interoperability issue

This issue is about how different cloud vendors allow dataowners to seamlessly move their data from one vendor to another or from a cloud provider back to their local resources whenever they need. Without interoperability amongst cloud providers, a data owner may lock in a certain vendor and cannot easily move to other vendors or optimize the services among different providers.

2.9.6.12 Observing activity patterns

Activity patterns of one cloud user can be observed eitherby other users on the same cloud or by the cloud provider. This observation can be a step for a security attack or can be used to reveal business activities that cannot be exposed in normal circumstances. For example, sharing information between two companies can be an indication of planning to merge.

2.9.6.13 The need of mutual audit-ability, accountability and trustworthiness

Trust needs tobe built between providers and customers in a cloud environment. Transparency via a high level of audibility and accountability is essential to build a trust relation. The trust relation will be more complicated when cloud providers

delegate some of the cloud services to subcontracts. Cloud computing consumers should know if there are any subcontracts that can also be responsible for their data band applications behind the cloud For example, Linkup had provided online storage service via another subcontracted provider called Nirvanix before it shutdown as a result of losing a remarkable amount of customers‘ data. Probably a sub contractor was responsible for the loss of the customers‘ data

2.9.7 Cloud Storage Security Requirements

In the process of storing data to the cloud, and retrieving it back from the cloud, there are mainly three elements involved, which are the client, the server (CSP) and the communication link between them. In order to make sure that the data is stored securely,

all the three elements must have a solid security. For the client, he/she has to make sure that unauthorized party can access his machine. While for cloud storage provider (CSP), he has to make sure that data have confidentiality, integrity and availability in rest.

but not least, the communication between client and server must be performed through a secure channel, i.e. the data must have confidentiality and integrity during its transfer between server and client. One of the ways to achieve secure communication is having a cryptographic protocol, such as SSL

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction.

This chapter presents a detailed description of the methodology to be employed in the study. The study proposes to address the vulnerabilities of cloud data by deploying a data encryption model. This model has encryption/decryption service that can be employed either locally or remotely according to level of severity of the data. This model shall remove the burden of key management and maintained from data owners.

3.2 Research Design.

According to Donald (2006), a research design is a structure of the research that holds together all the elements of a research project. The study will adopt a quasi-experimental nonrandomized control pretest-posttest quantitative research method is used. It is a quasi-experimental process as the nature of cloud storage means the devices are connected to the Internet to gather data and establish the circumstances for review, which can lead to changes to the devices outside the scope of the experiment. The proposed framework shall ensure that outsourced data can only be accessed (decrypted) by authorized users, and during the whole process cloud server is unable to learn any useful information that can lead to a potential privacy breach. To achieve the privacy of these components, our scheme processes the data in three fundamental steps: data outsourcing, file access and revocation.

3.2.1 Sample population

In quantitative research methodology, a data sample is a setoff data allowed and/ or selected from a statistical population by a defined procedure .Nubisave is freely available space controller 22for RAID or even optimal clouds which make dispersion, this makes data secure beyond encryption and made inaccessible in its entirely to the individual storage providers. Nubisave was used as the source of data since it freely provides space that securely stores data beyond encryption (Ilaghi Hosseini, (2015).

In this research the population consisted of sixty data storage providers that were extracted from sixty storage systems. The population was then clustered into five cloud storages containing ten cryptographic techniques representing five of the several cloud storages. the five cloud storages used are ; Dropbox, SugarSync, Amazon S3, Google storage and T-online media center.

3.2.2 Sample Size

Sample refers to a proportion of the research population that can be used to generalize certain characteristics on the research population after a study.

in order to gather enough data that could be used for conclusive analysis a total of fourty cloud storage companies were selected from the five cloud storage provider and each company was represented by ten cryptographic techniques

3.2.3 Data Collection Methods

The data collection method that was adopted in this research was experimental and used software to automate the collection process.

The various parameters used were to calculate the values of each parameter

3.3 Conceptual Framework.

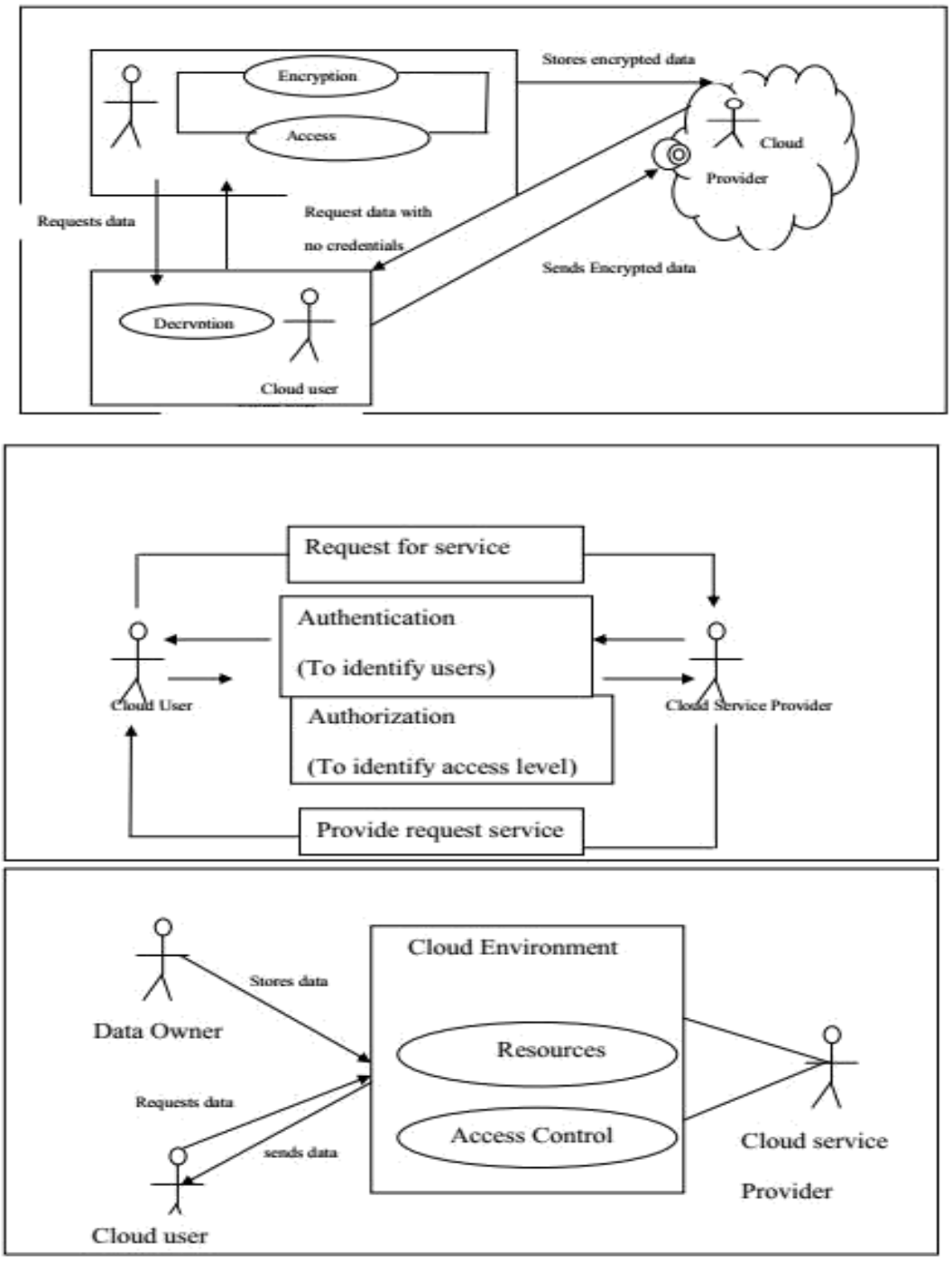


Figure 8: conceptual framework

A conceptual framework is defined as a model, which presents and better explains existing relationship between several variables. Packets of interest (with high probability) The key issue, of course, is whether it is possible to achieve this robust and secure distributed storage with minimal computation and communication. Three pillars of cloud security requirements are confidentiality, integrity and availability (CIA). If any cloud community achieves these requirements then it is a highly secured system. But in reality, achieving the CIA requirements is difficult**.** The figured epicts the conceptual framework of authentication and authorization involved in cloud computing. When a cloud user requests a service from CSP using his identity as an authentication tool, CSP verifies user's credentials as well as his rights on resources. After verification, if the user is an authorized user, CSP provides the respective services.

3.4 Cloud Service Models

This consist of the three conceptual layers of a generalized cloud environment which defines thebasic services provided by cloud providers*Software as a Service (SaaS).* The capability provided to the consumer is to use the provider'sapplications running on a cloud infrastructure. The applications are accessible from variousclient devices through either a thin client interface, such as a web browser (e.g., web-basedemail), or a program interface. The consumer does not manage or control the underlying cloudinfrastructure including network, servers, operating systems, storage, or even individualapplication capabilities, with the possible exception of limited user-specific applicationconfiguration settings.*Platform as a Service (PaaS).*

The capability provided to the consumer is to deploy onto thecloud infrastructure consumer-created or acquired applications created using programminglanguages, libraries, services, and tools supported by the provider. The consumer does notmanage or control the underlying cloud infrastructure including network, servers, operatingsystems, or storage, but has control over the

deployed applications and possibly configurationsettings for the application-hosting environment.*Infrastructure as a Service (IaaS).*

The capability provided to the consumer is to provisionprocessing, storage, networks, and other fundamental computing resources where the consumeris able to deploy and run arbitrary software, which can include operating systems andapplications. The consumer does not manage or control the underlying cloud infrastructure buthas control over operating systems, storage, and deployed applications; and possibly limitedcontrol of select networking components (e.g., host firewalls).

3.5 Cloud Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.*Community cloud.* The cloud infrastructure is provisioned for exclusive use by a specificcommunity of consumers from organizations that have shared concerns (e.g., mission, securityrequirements, policy, and compliance considerations). It may be owned, managed, and operatedby one or more of the organizations in the community, a third party, or some combination ofthem, and it may exist on or off premises.*Public cloud.* The cloud infrastructure is provisioned for open use by the general public. It maybe owned, managed, and operated by a business, academic, or government organization, or somecombination of them. It exists on the premises of the cloud provider.*Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloudinfrastructures (private, community, or public) that remain unique entities, but are boundtogether by standardized or proprietary technology that enables data and

application portability(e.g., cloud bursting for load balancing between clouds).

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private,community, or public) that remain unique entities but are bound together by standardized or

proprietary technology that enables data and application portability (e.g., cloud bursting for loadbalancing between clouds)

3.6 Cloud Security

The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. The cloud can bring security risks and challenges for IT Management, which can be more challenging for the organization to deal with, even considering the cost saving achieved by moving to the cloud. Therefore, it is very important for businesses to understand their requirements before opting for various deployment models available on the cloud.

3.7 Cloud Security Reference Model

In order to have a fair idea of what to expert in terms of security in the cloud, the cloud security alliance security reference model discusses the importance of knowing (CSA 2010);How cloud services are deployed; This include the four cloud deployment modelsdiscussed above (private cloud, public cloud, community cloud and hybrid cloud)

The manner in which cloud services are consumed: The various cloud service (SaaS,PaaS, Iaas)

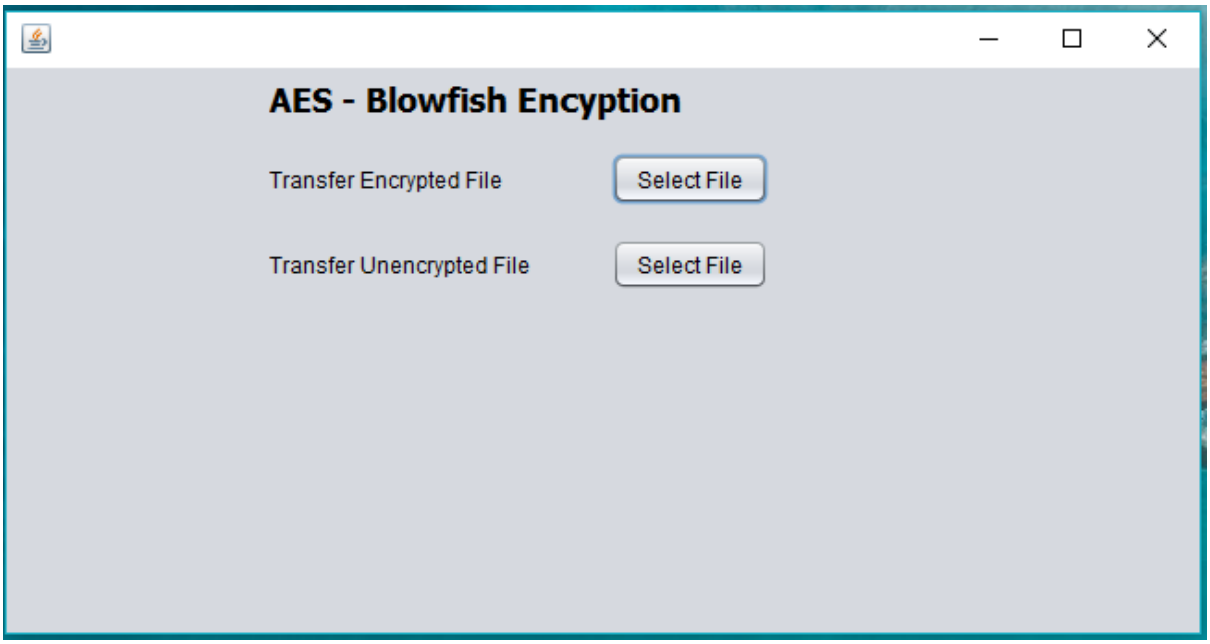
have associated security risk. It is important to understand where securityboundaries lie in terms of cloud computing. This is often described relative to thelocation of an organization's management or security perimeter. (usually defined by thepresence of a firewall).

The re-perimeterization and the erosion of trust boundaries: The high level ofinterconnectivity and information interchange due to the exploitation of businessopportunity exposes the business to various security risks. These risk are however notsufficient mitigated by traditional static security controls.

The ability to map cloud models to control frameworks is key to initiating, implementing, maintaining and improving information security within the organization (ISO/IEC 27002). Having security controls in place help mitigate all security risk before they result in security breaches. To do this, it is important to classify cloud service against the cloud architecture modelin order to map security architecture as well as business, regulatory and other compliance requirement against it. Information asset can then be protected thoroughly from the results.

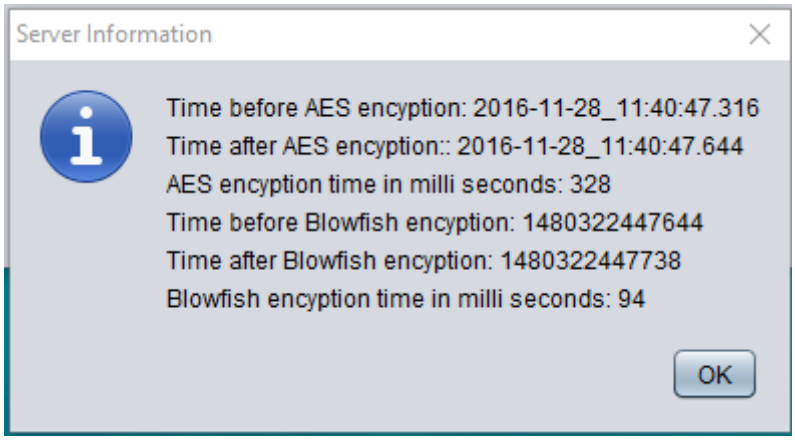
The figure below shows an example of how this can be done to realize which controls exist and which do not — as provided by the consumer, the cloud service provider, or a third party. This can in turn be compared to a compliance framework or set of requirements such as PCI DSS, as shown (CSA 2011).

Server
Main Server Interface

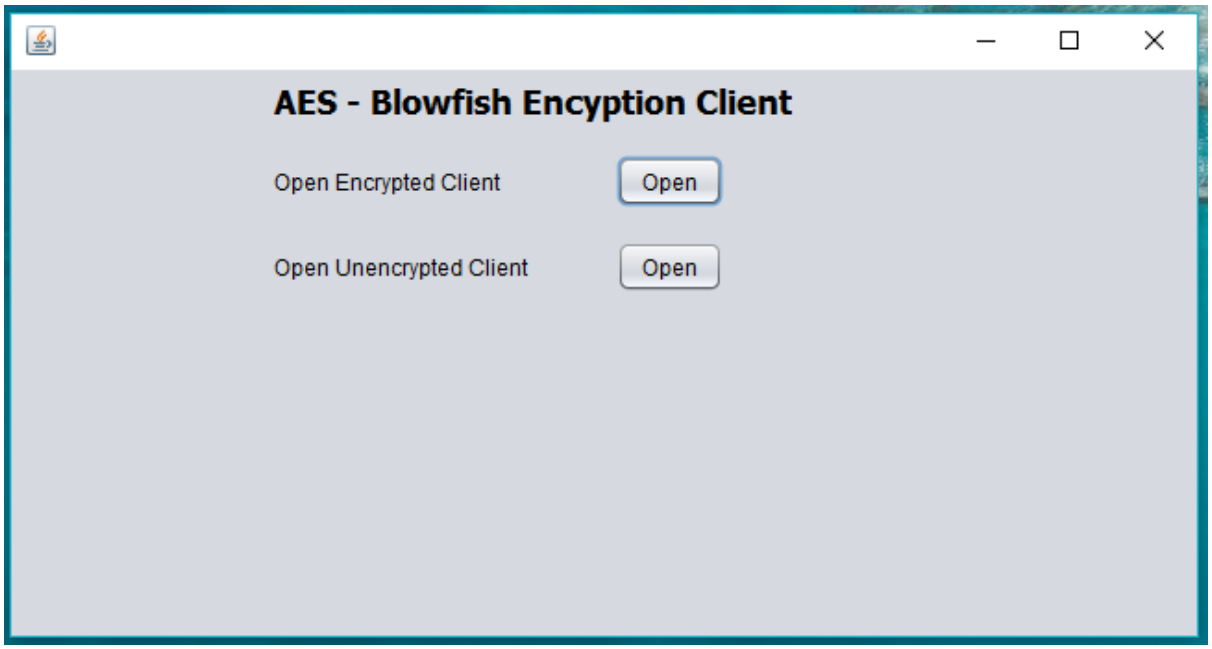


Selecting a file to encrypt using server interface

Server Encryption Output Details



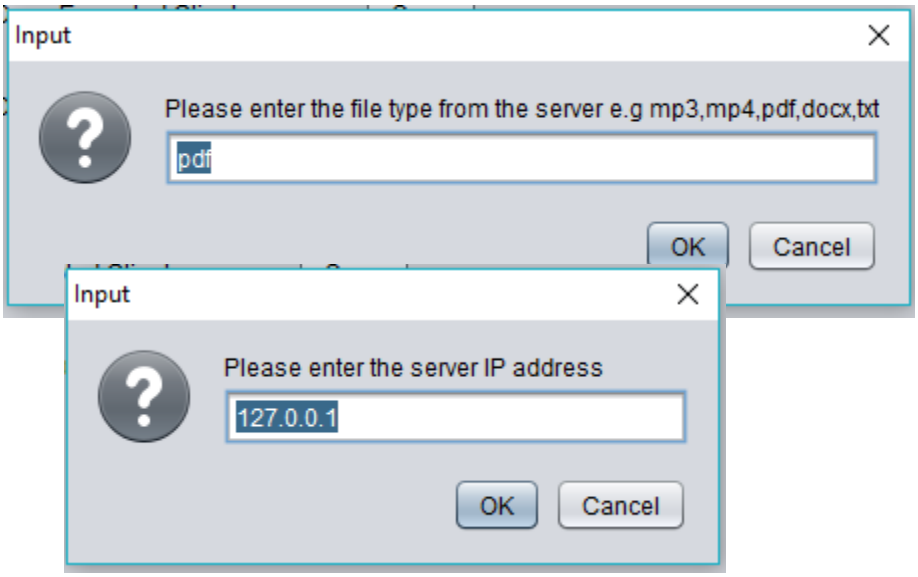
client
Main Client Interface



Client Prompt to enter the IP address of the running server

Client Prompt to enter the type of file to receive from the server

Client Decryption Output Details



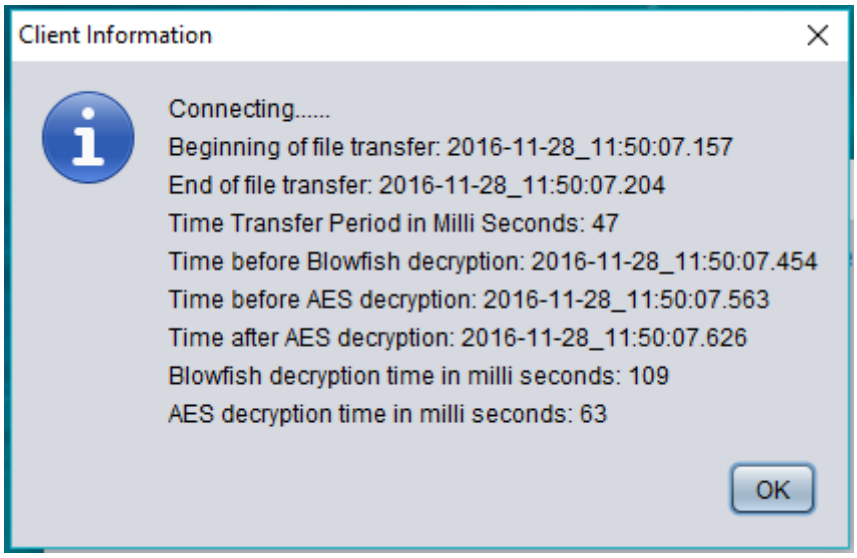


Figure 9: A screen shot showing a Main Client Interface

CHAPTER FOUR

EXPERIMENT, RESULTS AND DISCUSSION

4.1 Introduction

This chapter discusses the conducted experiment that was involved in designing an effective model that ensures security of data in the cloud. This effective way involved combining AES and Blowfish which increases the run time for both encryption and decryption. This means that the total time required for hybrid algorithms will be the addition of both algorithms‘ run time (processing time).Blowfish requires less time as compared to other algorithms. It also adds the additional processing time thus enhancing the security. This section gives the collected filtered data from the experiment which was then analyzed using graphs and discussed in order to understand the observed outcome.

4.2 Experiment Design

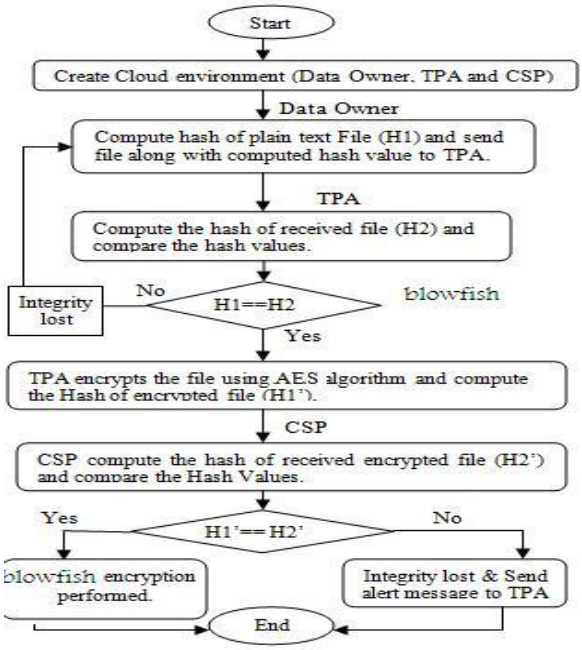


Figure 10: Experimental Design

4.3 Collected Data

This paper mainly concern with the Introduction of the Cloud Computing, Security Challenges related to the cloud and the basic techniques available for the security and integrity of cloud server

This section shows the experiments and data collected on the encryption and decryption of data done by combining both AES and Blowfish algorithms. Combining the two algorithms increases the run time for both encryption/decryption thus increasing the total time required for both processing time.

In this experiments we compare AES, Blowfish and the combination (AES +Blowfish) based on the performance parameters like: **Throughput, Encryption Time, Cipher text Size** and **Delay**

The named parameters can be calculated as follows:

 Throughput: this can be defined as the number of bits transferred per unit time. Its standardunits= **bytes per sec** Throughput= uploaded file size/delay time

 Cipher text size: this refers to the length of encrypted data, its standard units are in **bytes** Cipher text size=length of encrypted data

 Encryption Time: this is the time taken by the server to encrypt any file or data. Its standardunits are in **Nano seconds**.
Encryption Time =Encryption End Time – Encryption Start Time

 Delay time: this is the difference between start time uploading time and end of uploading time. Its standard units are the same as that of Encryption time. Delay Time = End uploading time- Start Uploading Time

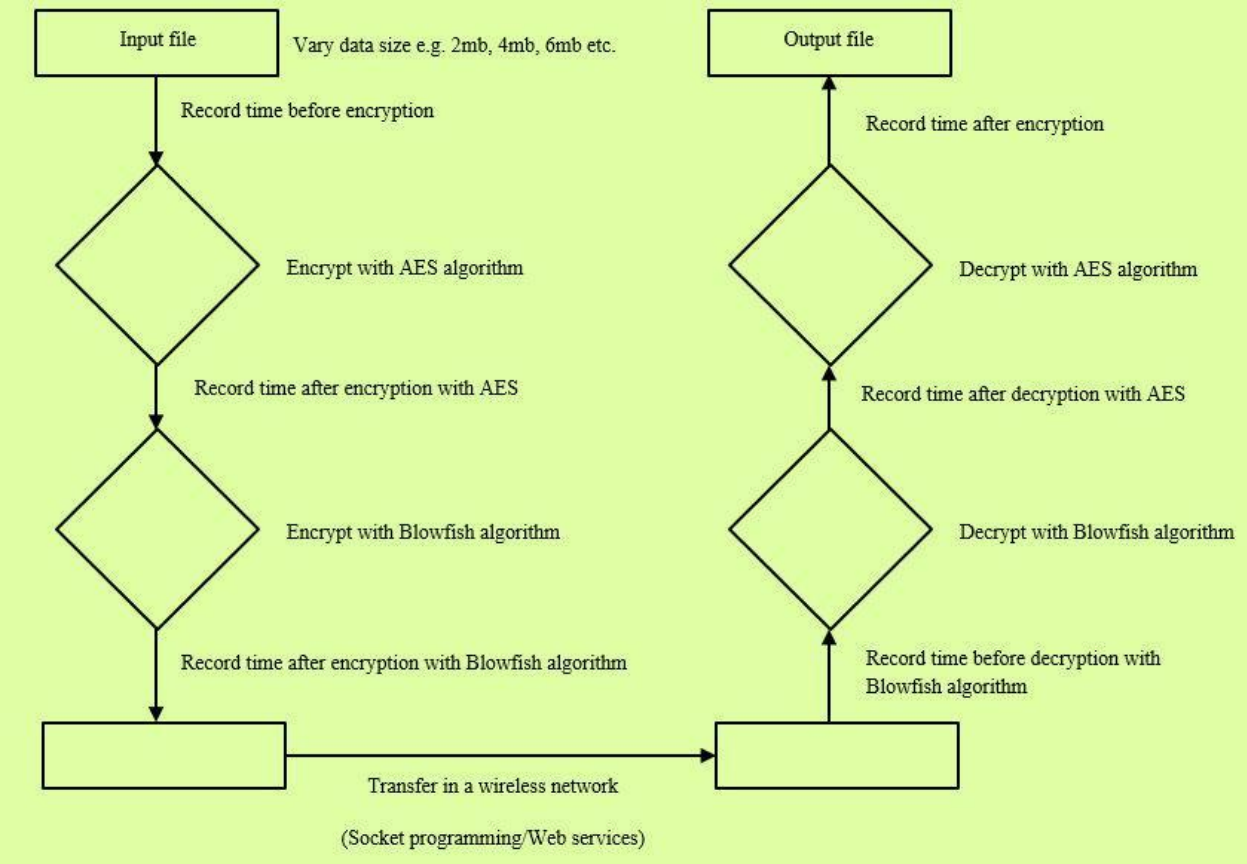


Figure 11 :Hybrid AES and Blowfish data encryption and decryption

4.3 . Experiments and Results

4.3.1 Experiment setup

An application was designed and implemented in java language on the same network to achieve the functionalities of the client and the server. We had it that the cloud and the server were on the same network so that they could be in a position to communicate; we therefore put them on the same IP address for them to communicate without any hindrances. This made the client and the server which were on the same domain to be subjected to the same parameters. Based on the experiment we had computed the parameters value for AES, Blowfish and the combination or

the hybrid system(AES +Blowfish) for the same file size. Below is a table with respective tested parameters and the respective values for the said algorithms:

Table 1: Algorithm Parameter values

Algorithms → / Parameters ↓	*AES*	*Blowfish*	*AES + Blowfish*
Encryption Time	1119	3	1123
Delay Time	586	528	63
Cipher Text	0.020195007	0.020175934	0.019347898
Throughput	0.03583618	0.03977273	0.040768746
File size	21kb	21kb	21kb

Figure 12: A screen shot showing the Main Server Interface

Figure 11 shows the home interface that the user firstly interacts with when they open the tool.

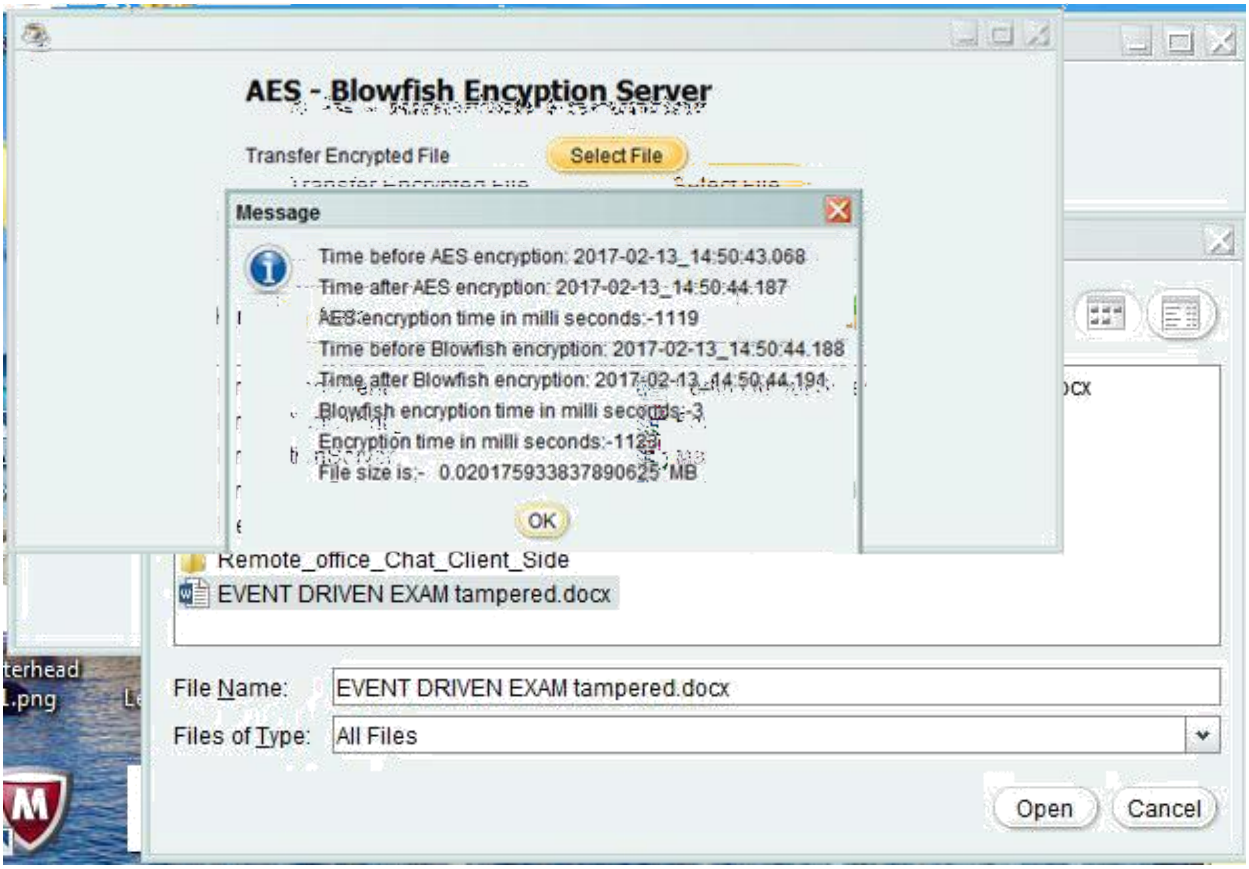


Figure 13: A screen shot showing the process of Selecting a file to encrypt using server

Interface

Figure 14: A screen shot showing the Server Encryption Output Details

Figure 14 shows the interface after the data encryption. The output details indicate the time before encryption and the time after encryption. The server also calculates the time taken during encryption for both AES and blowfish

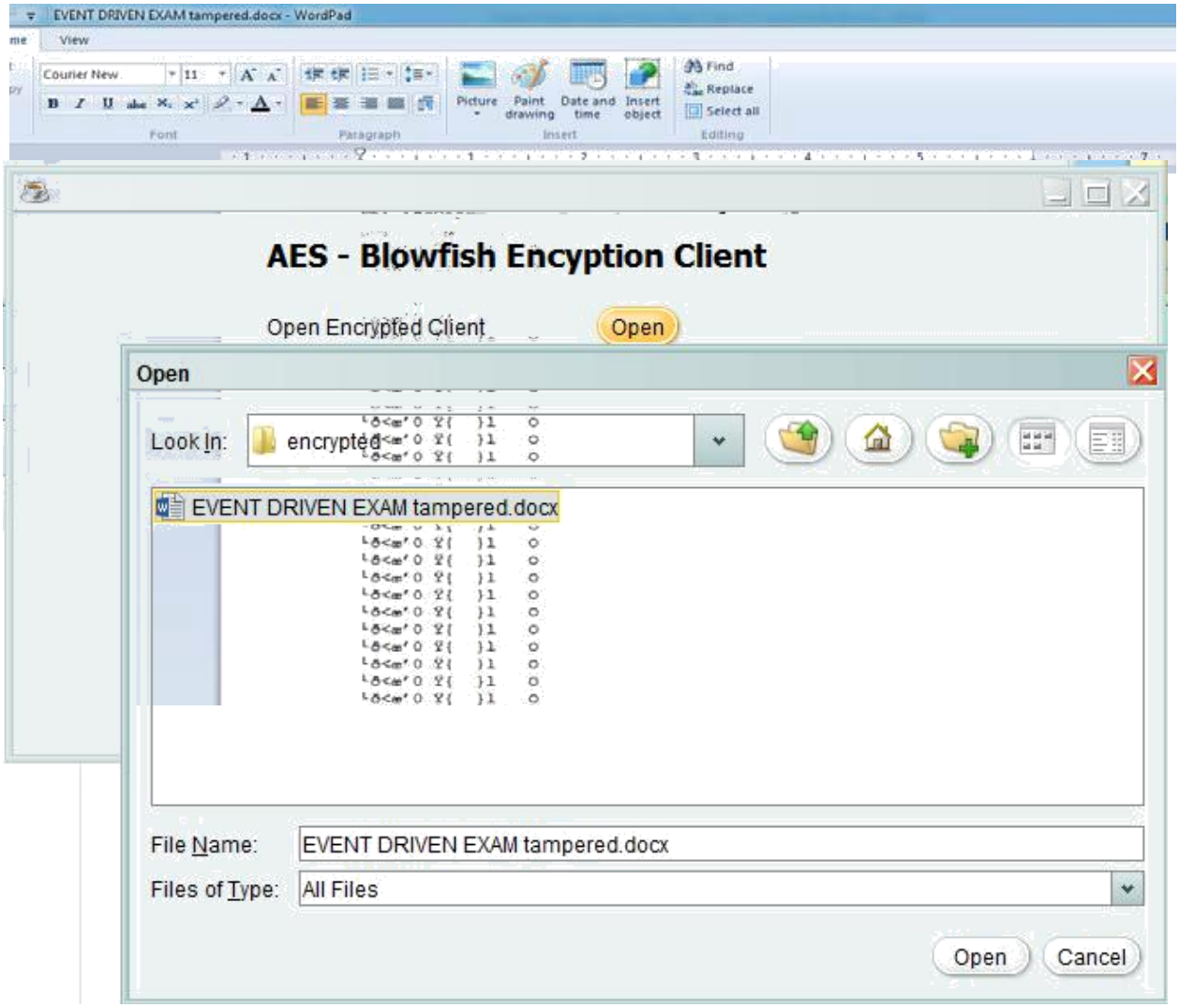


Figure 15 : A screen shot showing A file Saved in predefined folder encrypted, the word

File can not be opened normally and when opened with word pad, the below fig show the encrypted content

Figure 15 shows the interface after the user the file saved in a predefined folder. It shows when the file is opened with WordPad. The content is displayed in its encrypted form.

Figure 15 shows the home interface the client first encounters with while opening the encrypted file stored in the cloud

Figure 16: A screen shot showing Client Prompt to enter the IP address of the running server

Figure 16 shows the interface prompting the client to enter the IP address of the running server.

Figure 17: Client Prompt to choose the file to be decrypted from the server and the default file extension is automatically assigned

Figure 17: Client Decryption Output Details

Figure 17 shows the interface after the data encryption. The output details indicates the beginning of the file transfer and the end of the file. The server also calculates the time taken during file transfer for both AES and blowfish

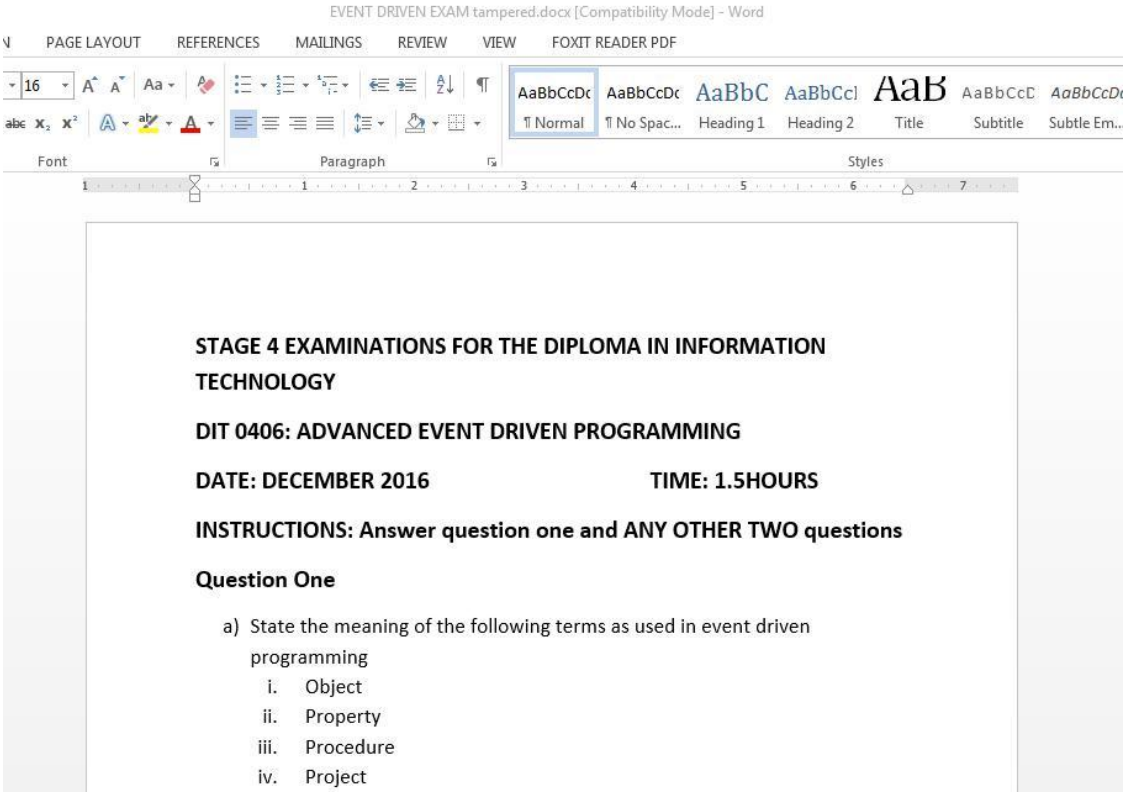


Figure 18 : File is decrypted back and is now in a readable format as shown below, can beopened with Ms. Word

Figure 18shows the recordedencryption and decryption times using different files sizes and different algorithms

TABLE 2:AES and Blowfish Encryption Data Analysis.

FILE SIZE	**ENCRYPTION TIME (IN MILLISECONDS)**		**DECRYPTION TIME (IN MILLISECONDS)**	
	AES	BLOWFISH	AES	BLOWFISH
1MB	547	47	47	62
2.3MB	578	63	62	93
4MB	595	106	78	125
8MB	594	156	110	218
10.5MB	594	219	62	266

Figure 18: Delay time for uploading a file on AES ,Blowfish and AES+Blowfish

Figure 19 indicates the time taken to upload a file using AES, Blowfish and AES+ Blowfish. AES takes the longest delay time while uploading a file while the hybrid AES + blowfish takes the least delay time

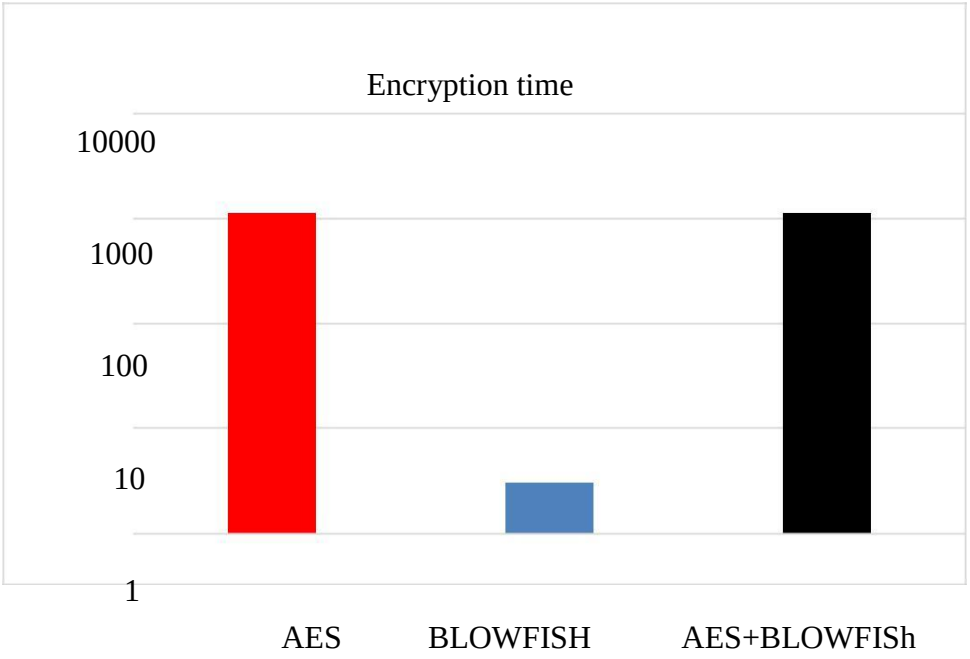
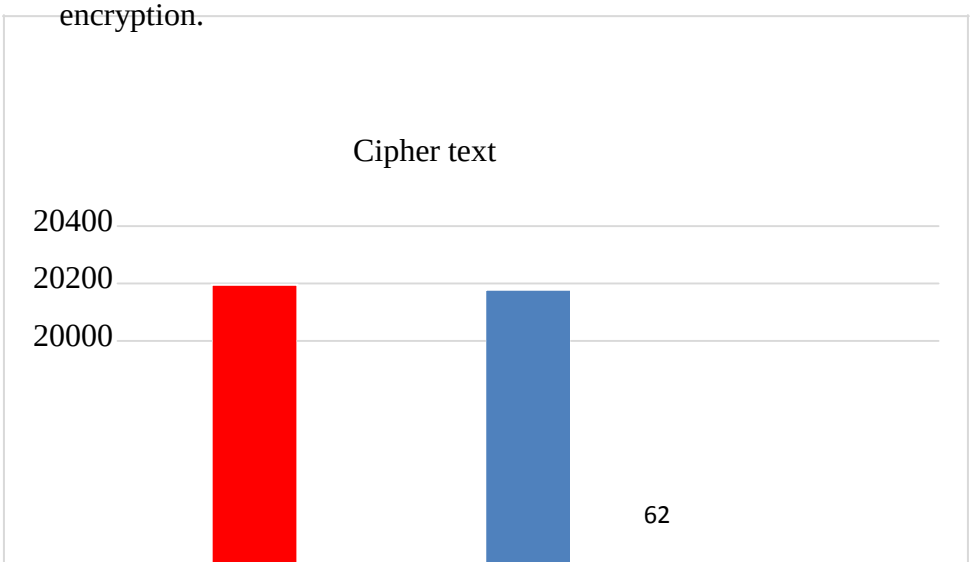


Figure 19 Encryption time taken by AES ,Blowfish and AES+Blowfish in Nano Seconds

Figure 19 indicates the time taken by AES ,Blowfish and AES+Blowfish respectively to encrypt a file. Blowfish takes the least time in encryption while AES takes the longest time in encryption.



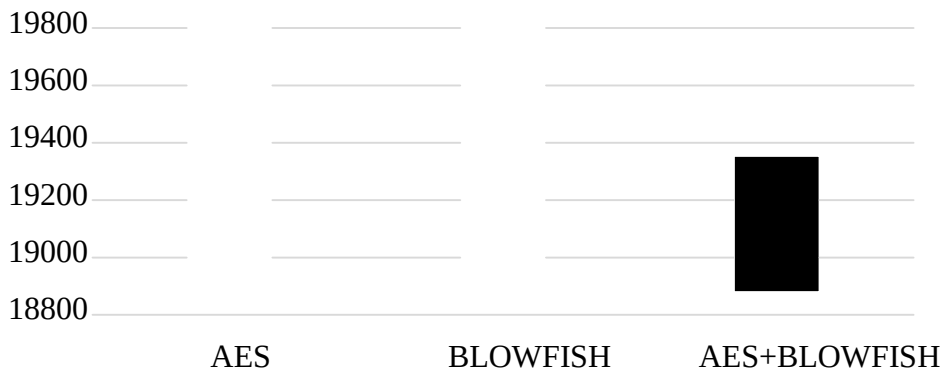


Figure 20: Cipher text size of encrypted file in bytes using AES ,Blowfish and AES + Blowfish

Figure 20 show the length of encrypted data in bytes using AES ,Blowfish and AES + Blowfish . AES has the longest cipher text size while AES + Blowfish has the shortest cipher text size

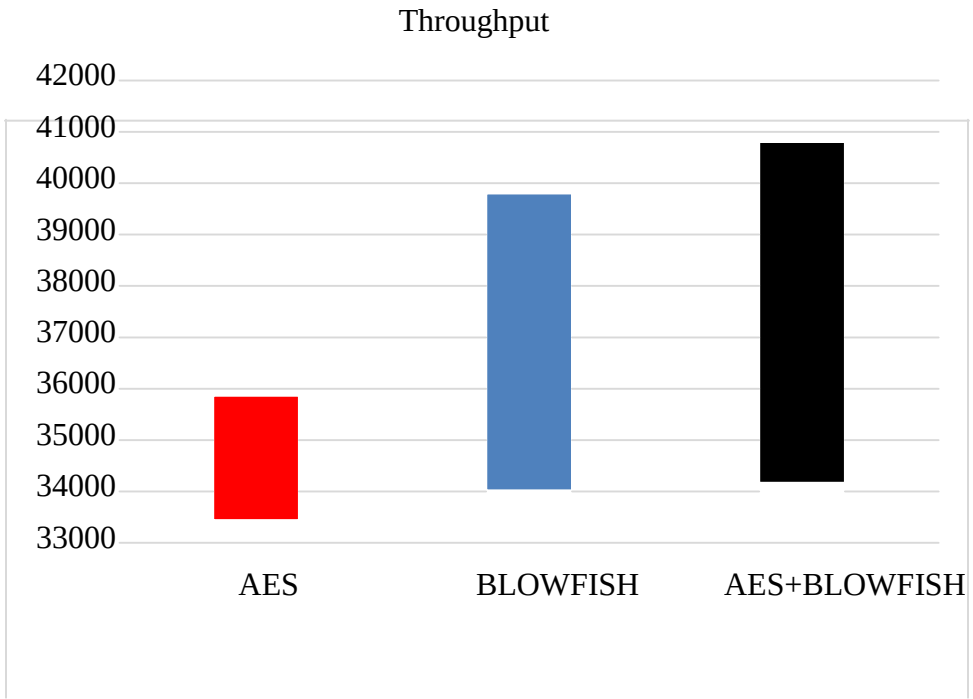


Figure 21 Through put in bytes per second using AES ,Blowfish and AES + Blowfish

Figure 20 shows the number of bits transferred per seconds using AES, Blowfish and AES+Blowfish. AES + Blowfish transfer the highest number of bytes per second while AES transfers the least bytes per second.

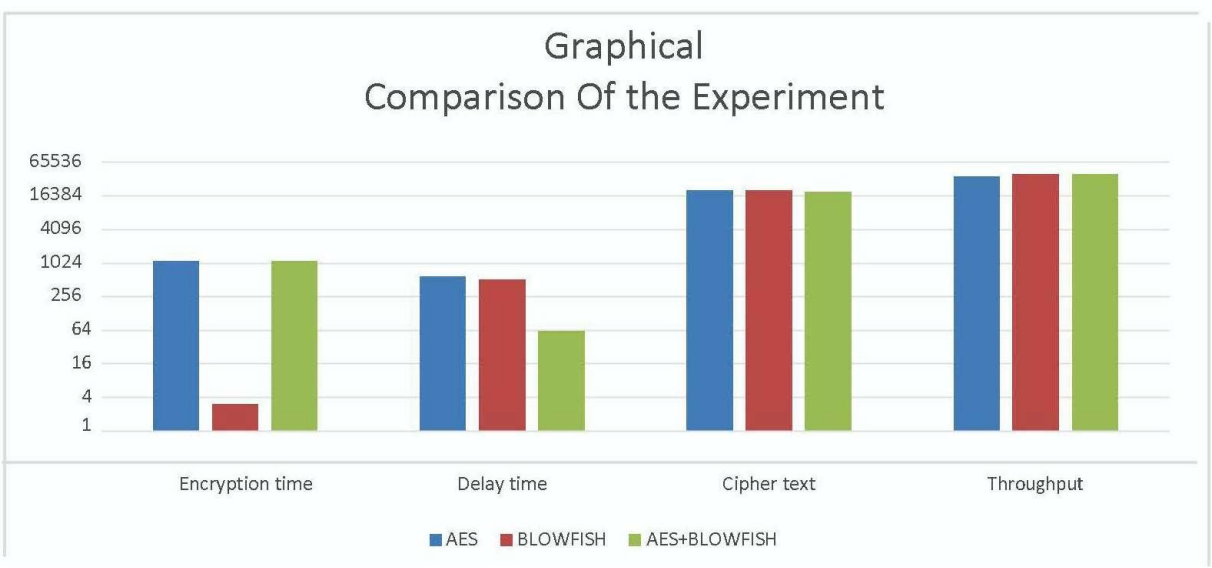


Figure 22: graphical comparison of the experiment

Results show that AES is the best algorithm of symmetric encryption technology. AES algorithm is more secure than the Blowfish algorithm but on the other hand Blowfish is more secure than other algorithms. Blowfish runs faster than other symmetric algorithms AES is the symmetrical based encryption standard by NIST]. The hybrid algorithm is more secure since it has the characteristics of both algorithms and makes it more vulnerable to threats.

CHAPTER FIVE: CONCLUSIONS AND FUTURE WORK

5.1 Conclusion

When the clients store data in the cloud, there‘s always an issue whether or not cloud service provider stores the data securely. Security as earlier discussed is the main challenge faced while storing data in the cloud, the proposed system provides security for the data stored in the cloud computing model through the help of AES and Blowfish algorithms.

Results show that AES is the best symmetric encryption algorithm, it‘s more secure than Blowfish though compared to other algorithms Blowfish is by far the best. Blowfish gives the highest throughput as compared to AES. The hybrid of AES and Blowfish gives the properties of both algorithms thus making the formed hybrid algorithm much stronger to threats. This makes the formed hybrid system secure by increasingly adding the complexity functionalities.

5.2 Recommendations for Future Work

The future scope of this work can be extended by:

- Performing the same experiments using audio and video as well.
- Compression algorithm can be performed for faster encryption.
- Performing the same experiments using some locking techniques for security mechanism

REFERENCES

Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013).Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation ComputerSystems*, *29*(7), 1645-1660.

Friess, P. (2013). *Internet of things: converging technologies for smart environments andintegrated ecosystems*. River Publishers.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., &Suciu, V. (2013, May). Smart cities built on resilient cloud computing and secure internet of things. In *2013 19thInternational Conference on Control Systems and Computer Science* (pp. 513-518).IEEE.

Buyya, R., Ranjan, R., &Calheiros, R. N. (2010, May).Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In *International Conference on Algorithms and Architectures for Parallel Processing* (pp.13-31).Springer Berlin Heidelberg.

Birk, D., & Wegener, C. (2011, May).Technical issues of forensic investigations in cloud computing environments. In *Systematic Approaches to Digital Forensic Engineering(SADFE), 2011 IEEE Sixth International Workshop on* (pp. 1-10). IEEE.

Wu, J., Ping, L., Ge, X., Wang, Y., & Fu, J. (2010, June). Cloud storage as the infrastructure of cloud computing. In *Intelligent Computing and Cognitive Informatics(ICICCI), 2010 International Conference on* (pp. 380-383). IEEE.

Damgard, I., Jakobsen, T. P., Nielsen, J. B., & Pagter, J. I. (2013, December). Secure key management in the cloud. In *IMA International Conference on Cryptography and Coding* (pp. 270-289).Springer Berlin Heidelberg.

Ezell, S. J., Atkinson, R., &Wein, M. A. (2013).Localization barriers to trade: threat to the global innovation economy.*Available at SSRN 2370612*.

Wan, J., Zou, C., Ullah, S., Lai, C. F., Zhou, M., & Wang, X. (2013). Cloud-enabled wireless body area networks for pervasive healthcare. *IEEE Network*, *27*(5), 56-61.

Conzon, D., Brizzi, P., Kasinathan, P., Pastrone, C., Pramudianto, F., &Cultrona, P. (2015, February).Industrial application development exploiting IoT vision and model driven programming. In *Intelligence in Next Generation Networks (ICIN), 2015 18thInternational Conference on* (pp. 168-175). IEEE.

Lee, K., Murray, D., Hughes, D., &J oosen, W. (2010, November).Extending sensor networks into the cloud using amazon web services. In*Networked Embedded Systems forEnterprise Applications (NESEA), 2010 IEEE International Conference on* (pp. 1-7).IEEE.

Yang, K. (2014). Wireless sensor networks. *Principles, Design and Applications*.

Dunham, G. M. (2013). *U.S. Patent Application No. 12/975,678*.

Rosenthal, A., Mork, P., Li, M. H., Stanford, J., Koester, D., & Reynolds, P. (2010).Cloud computing: a new business paradigm for biomedical information sharing.*Journal of biomedical informatics*, *43*(2), 342-353.

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computernetworks*, *52*(12), 2292-2330.

Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., ...& Stankovic, J. (2006). Alarm-net: Wireless sensor networks for assisted-living and residential monitoring. *University of Virginia Computer Science Department Technical Report*, *2*.

Qi, H., &Gani, A. (2012, May). Research on mobile cloud computing: Review, trend and perspectives. In *Digital Information and Communication Technology and it'sApplications (DICTAP), 2012 Second International Conference on* (pp. 195-202). ieee.

Kalpana, P., & Singaraju, S. (2012). Data security in cloud computing using RSA algorithm.*IJRCCT*, *1*(4), 143-146.

Kulkarni, G., Waghmare, R., Palwe, R., Waykule, V., Bankar, H., & Koli, K. (2012, October).Cloud storage architecture. In *Telecommunication Systems, Services, andApplications (TSSA), 2012 7th International Conference on* (pp. 76-81).IEEE.

Prahlad, A., Muller, M. S., Kottomtharayil, R., Kavuri, S., Gokhale, P., & Vijayan, M. (2012).*U.S. Patent No. 8,285,681*. Washington, DC: U.S. Patent and Trademark Office.

Coyne, L., Hajas, T., Hallback, M., Lindström, M., &Vollmar, C. (2016).*IBM Private,Public, and Hybrid Cloud Storage Solutions*. IBM Redbooks.

Bahga, A., &Madisetti, V. (2013).*Cloud Computing: A Hands-on Approach*. Create Space Independent Publishing Platform

Younis, O., Krunz, M., & Ramasubramanian, S. (2006).Node clustering in wireless sensor networks: recent developments and deployment challenges. *IEEE network*, *20*(3), 20-25.

Abbasi, A. A., & Younis, M. (2007).A survey on clustering algorithms for wireless sensor networks. *Computer communications*, *30*(14), 2826-2841.

Forhan, C. E., Galbraith, R. E., & Gerhard, A. C. (2009).*U.S. Patent No. 7,487,394*. Washington, DC: U.S. Patent and Trademark Office.

McGill, K., & Taylor, S. (2011, November). Computational resiliency for distributed applications.In*2011-MILCOM 2011 Military Communications Conference* (pp. 1472-1479).IEEE.

McKean, B., & Kleppen, D. (2008).*U.S. Patent Application No. 12/215,290*.

Leventhal, A. (2010). Triple-parity RAID and beyond. *Communications of the ACM*, *53*(1), 58-63.

Joseph, D. J., Ritter, M. B., & Tierno, J. A. (2015). *U.S. Patent No. 8,949,685*. Washington, DC: U.S. Patent and Trademark Office.

Taylor, J., Goel, A., & Leong, J. (2012).*U.S. Patent No. 8,209,587*. Washington, DC: U.S. Patent and Trademark Office.

Therrien, D. G., Pownell, J. E., VanderSpek, A., Kenna, H. R., Sawyer, C. L., Dougherty, E., ... &Greizerstein, P. B. (2007). *U.S. Patent No. 7,246,140*. Washington, DC: U.S. Patent and Trademark Office.

Kehayias, J., & Krueger, T. (2011).*Troubleshooting SQL Server*.Red gate books.
Velte, A. T., Velte, T. J., Elsenpeter, R. C., &Elsenpeter, R. C. (2010).*Cloud computing:a practical approach* (p. 44). New York: McGraw-Hill.

Koller, R., & Rangaswami, R. (2010). I/O deduplication: Utilizing content similarity to improve I/O performance. *ACM Transactions on Storage (TOS)*, *6*(3), 13.

Call, M., Morrison, J. A., Phan, L. D., & Syu, M. M. L. (2014). *U.S. Patent No.8,700,951*. Washington, DC: U.S. Patent and Trademark Office.

Ilaghi Hosseini, M. (2015). Secured Personal Data Storage Platform for Private Clouds.

de Diego, R., Martínez, J. F., Rodríguez-Molina, J., & Cuerva, A. (2014). A semantic middleware architecture focused on data and heterogeneity management within the smart grid. *Energies*, *7*(9), 5953-5994

Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. *IEEE transactions on computers*, *62*(2), 362-375.

Ms.Payal, P,Killor and Prof.Vijay, B.Gadicha (2014) ―*Data integrity proof inDocument Mnagement system under cloud with multiple storage*‖, international journal ofEngeneering & Computer Science Vol.3.

Sonwalkar, N. (2013, September). The first adaptive MOOC: a case study on pedagogy framework and scalable cloud architecture—Part I. In *MOOCs Forum* (Vol. 1, No. P, pp. 22-29). 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA: Mary Ann Liebert, Inc..

Cao, Y., Chen, C., Guo, F., Jiang, D., Lin, Y., Ooi, B. C., ...&Xu, Q. (2011, April). Es 2: A cloud data storage system for supporting both oltp and olap. In *Data Engineering(ICDE), 2011 IEEE 27th International Conference on* (pp. 291-302). IEEE.

Yang, K., & Jia, X. (2013). An efficient and secure dynamic auditing protocol for data storage in cloud computing. *IEEE transactions on parallel and distributed systems*, *24*(9), 1717-172

Kumar, M. A., &Karthikeyan, S. (2012). Investigating the efficiency of Blowfish and Rejindael (AES) algorithms. *International Journal of Computer Network andInformation Security*, *4*(2), 22.

Ramesh, A., &Suruliandi, A. (2013, March). Performance analysis of encryption algorithms for Information Security. In *Circuits, Power and Computing Technologies(ICCPCT), 2013 International Conference on* (pp. 840-844). IEEE.

Pavithra, S., &Ramadevi, M. E. (2012). Study and performance analysis of cryptography algorithms. *International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)*, *1*(5), pp-82.

Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques.

International Journal of Emerging Trends and Technology in Computer Science, *3*(4), 6.

ShivShakti., etc (January-February -2013)‖ *encryption using different techniques*: A Rieview‖ international journal in multidisciplinary and academic research (SSIJMAR) vol.2 No. 1 (ISSN 2278-6973)

Pavithra, S., &Ramadevi, E. (2012). Throughput Analysis of Symmetric Algorithms. *International Journal of Advanced Networking and Applications*, *4*(2), 1574.

Patil, P., Narayankar, P., Narayan, D. G., &Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *ProcediaComputer Science*, *78*, 617-624.

APPENDICES

Appendix A : Abstract of publication on IJSR

International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391 Volume 6 Issue 3, March 2017 www.ijsr.net

Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)

Fortine Mata1, Michael Kimwele2, George Okeyo3 1, 2, 3Computing Department, Jomo Kenyatta University of Agriculture and Technology

Abstract:*Data stored in the cloud is increasingly gaining popularity for all users includingpersonal, institutions and business purposes. The data is usually highly protected, encrypted and replicated depending on the security and scalability needs. Despite the advances in technology, the practical usefulness and longevity of cloud storage is limited in today's systems. This paper provides a solution to the problem of securely storing the client's data by maintaining the confidentiality and integrity of the data within the cloud. This paper addresses the problem of ensuring data confidentiality against cloud and against accesses beyond authorized rights. To resolve these issues, we designed a data encryption model that is in charge of storing data in an encrypted format in the cloud. To improve the efficiency of the designed architecture, the service in form of the model designed allows the users to choose the level of security of the data and according to this level different encryption algorithms are used.*

Keywords: Data Storage, Security, Confidentiality, Integrity, Cloud Computing