

A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms

BY

Jannatul Ferdous Aney
ID: 153-15-6376

AND

MD. Fuad Newaz Khan
ID: 153-15-6521

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Dr. Karim Mohammed Rezaul

Visiting Professor
Faculty of Arts, Science and Technology
Wrexham Glyndŵr University
Mold Road, Wrexham, LL11 2AW
United Kingdom

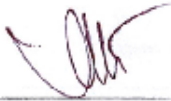


DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
SEPTEMBER 2019

APPROVAL

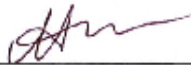
This Research titled “A Hybrid Framework for Security in Cloud Computing”, submitted by Jannatul Ferdous, ID No: 153-15-6376 and Md. Fuad Newaz Khan, ID. No: 153-15-6521 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on September 14, 2019

BOARD OF EXAMINERS



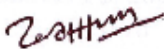
Dr. Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



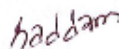
Nazmun Nessa Moon
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Zahid Hasan
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md. Saddam Hossain
Assistant Professor
Department of Computer Science and Engineering
United International University

External Examiner

Declaration

We hereby declare that, this project has been done by us under the supervision of **Dr. Karim Mohammed Rezaul, Visiting Professor, Wrexham Glyndwr University, United Kingdom**. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Dr. Mohammed Rezaul Karim
Visiting Professor
Faculty of Arts, Science and Technology
Wrexham Glyndŵr University
Mold Road, Wrexham, LL11 2AW
United Kingdom

Submitted by:



(Jannatul Ferdous Aney)
ID: 153-15-6376
Department of CSE
Daffodil International University



(Md. Fuad Newaz Khan)
ID: 153-15-6501
Department of CSE

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound indebtedness to **Dr. Karim Mohammed Rezaul, Visiting Professor, Wrexham Glyndwr University, United Kingdom.** Deep Knowledge & keen interest of our supervisor in the field of “*Networking*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Allah and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

Abstract

Cloud computing is the concept used to decode Daily Computing Issues. Cloud computing is essentially a virtual pool of resources and also provides these tools to customers through the internet. Cloud computing is your net-based advancement and utilized in computer technology. The widespread problem connected with cloud computing is information privacy, protection, anonymity and dependability, etc. However, the main involving them is safety and how cloud supplier guarantees it. To secure the cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider. Cloud computing is architecturally focused on client servers. Cloud computing is a hub of various server and many databases to store data. Cloud computing provide many services to user which is reliable, efficient and low cost. The paper reviews concurrent articles on security in cloud computing. As it is Internet-based technology security, data security becomes a big issue to the cloud data. Many issues like data authenticity, integrity, data hiding and availability. By conducting research, we introduce a mechanism to provide secure data. We have combined three algorithms DSA, AES and Steganography to provide security of data in cloud computing.

Table of Contents

CONTENTS	PAGE
Board of Examiners	i
Declaration	ii
ACKNOWLEDGEMENT	iii
Abstract	iv
CHAPTER	
CHAPTER 1 (Introduction)	1-7
1.1 Introduction	1
1.2 Main Features of Cloud	3
1.3 Cloud computing service delivery models	4
1.4 Motivation	5
1.5 Rationale of the Study	6
1.6 Research Questions	6
1.7 Expected Output	6
1.8 Report Layout	7
CHAPTER 2 (Background)	8-13
2.1 Introduction	8
2.2 Cloud data security considerations	8
2.3 Related Works	11
2.4 Research Summary	13
2.5 Scope of the Problem	13
2.6 Challenges	13
CHAPTER 3 (Research Methodology)	14-29
3.1 Introduction	14
3.2 Cryptographic Algorithms	15
3.3 Design of proposed work	18

3.4 Elaboration of Overall System	19
3.5 Research Subject and Instrumentation	28
3.6 Data Collection Procedure	28
3.7 Statistical Analysis	29
CHAPTER 4 (Experimental results and discussion)	30-31
4.1 Introduction	30
4.2 Experimental Results	30
4.3 Descriptive Analysis	30
4.4 How the Data will be secured in our system	31
4.5 Summary	31
CHAPTER 5 (Summary, Conclusion, and Implication for Further Research)	32-33
5.1 Summary of the study	32
5.2 Conclusion	32
5.3 Implication for Further Study	33
CONTRIBUTION FROM THIS R&D PROJECT	34
REFERENCES	35

LIST OF FIGURES

FIGURES	PAGE NO
Figure 1.1: Three Main Features of Cloud	3
Figure 3.1: Hybrid framework for security in cloud computing	18
Figure 3.2: Digital signature generation using DSA	19
Figure 3.3: Encryption Using AES	21
Figure 3.4: Encryption using steganography	22
Figure 3.5: Framework Algorithm for encryption using steganography	23
Figure 3.6: Decryption using steganography	24
Figure 3.7: Framework Algorithm for decryption using steganography	25
Figure 3.8: Decryption Using AES	26
Figure 3.9: Signature Verification using DSA	27

LIST OF TABLES

TABLES	PAGE NO
Table 2.1: Comparison between different cryptographic algorithms	12
Table 4.1: Two best algorithms according to Table 2.1	30

CHAPTER 1 (Introduction)

1.1 Introduction

Cloud computing is an information technology paradigm that provides scalable on-demand computing services such as computing, storage, network, software, and much more on the Internet [41], enabling companies and organizations to focus their efforts on their key business or activity by outsourcing their IT resources [42]. This new technology offers many benefits such as cost efficiency, increased storage capacity, backup and recovery, ongoing accessibility of resources and independence of location [34]. While cloud computing (CC) is not entirely new, traction between organizations and individual users still benefits. For example, the cloud adoption expected by Garner would continue to grow at a compound growth rate of 41.7 percent in 2016[1]. However, the transition into the cloud environment is not straightforward, and there are many operational and security issues. Ensuring the security of information outsourced to the cloud is becoming increasingly important due to the trend towards more cloud storage of information [1,2]. Users of the public cloud may have more control over access to infrastructure than others [33].

Using a hypervisor and Virtual Machine (VM) technique is also a safety issue as this and VM technology is susceptible to assaults at VM stage. These programs have quite a few computer organizations on-site that could have a huge amount of hardware and software systems. Attackers could exploit vulnerabilities in VM infrastructure to exfiltrate information or carry out assaults such as DDoS (Dispersed Denial of Services) [3,4]. This is a consequence of the TCP / IP stack's intrinsic faults. Also, several fresh events have recently appeared that breach screening using polymorphism and metamorphosis. As an example, information about the victim's computers can be easily acquired and utilized within an IaaS cloud environment; thus, enabling attacks on VMs [5,6,7].

Attackers can inject kernel files into the server operating system (OS), and as all client operating systems use this kernel to run their operating system, attackers can control all VMs. Also, by effectively exploiting recognized or zero-day vulnerabilities in the host VM, attackers can then enter the VMs of the host as the hypervisor retains the hardware

and apps in the popular virtual environment [8]. Some hypervisors provide APIs that make the VM plant fully traffic-observable. These APIs, however, provide extra routes to view and utilize network communication for attackers [9]. Also, other attacks target CC [10] such as the intrusion of information, accessibility of information and data integrity. Whenever customers rely on these parties, there is no credible data deposited in the cloud. Thus, customers are now involved in the method of encrypting their delicate information before bringing it to the cloud for storage [35]. To prove this, Gartner [37] predicts that cloud data centers will process 92 percent of the workload by 2020. It is anticipated that cloud workloads will increase by 3.2 times fold over the same moment, predicts Cisco [38]. But this technology's primary drawback arises with the failure of command over the cloud infrastructure. Therefore, individuals, companies, and organizations withstand public cloud implementation due to safety and privacy concerns [39,40]. Recent cloud assaults, like the one in 2014 when the 50 million user accounts of Dropbox were accessed, indicate cloud data security has become a hot topic in the study [43]. Al Awadhi et al. [44] demonstrated the risks the cloud faces. They used honey boxes to check the cloud setting's insecurity and that it is the object of many different countries' attacks.

1.2 Main Features of Cloud

Cloud computing has some important features that overcome the feature of traditional services and proves the importance of the growth of the IT industry. Figure1 illustrates the main 3 features of the cloud.

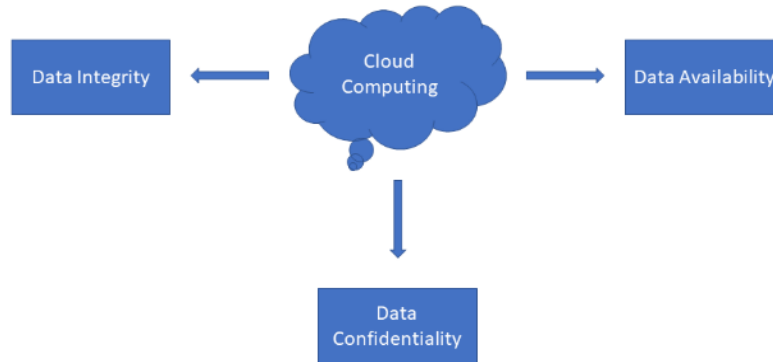


Figure 1.1: Main Three Features of Cloud [26]

A. Data Integrity

Data integrity ensures complete and valid data. Integrity involves controlling or strictly maintaining the devices which are connected to the network and information from Illegal access. It also includes atomicity, durability, isolation, and consistency characteristics [11]. The cloud service supplier should guarantee data integrity and give customer confidence in the privacy or safety of their information.

B. Data Availability

It is the feature that can be accessed and used over a defined time [36]. We can therefore say that all machines need to retain data and applications and supply or manage information when the client needs it. Cloud vendors use the real retrieval system to collect and shop client data, use a proxy server to secure data, and provide network (internet) data as required by the user [11,20]. Two popular techniques of accessibility to data are the Network Storage Area (SAN) and Network Attached Storage (NAS). The

quantity of information can be measured on how frequently the information is accessible and how much information can pass at a moment.

C. Data Confidentiality

Confidentiality of data concerns several legislation restricting entry to information or data and confidentiality of outsiders [20]. Confidentiality of data is the responsibility of the service provider to provide service to the customer and to store data in the cloud. Disclosure of data is the source of the damage, deprivation, and theft of an unlawful person. Providers and clients maintain multiple levels of confidentiality such as SLA, data portability, retention, and traceability. We use many data protection or confidentiality methods at the moment, such as data encryption, code security, and biometric inspection.

1.3 Cloud computing service delivery models

Mathisen [60] highlighted the cloud service delivery models are essentially divided into three as follows:

1. Software as a Service (SaaS)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)

1. Software as a Service (SaaS)

Software as a service is delivering software over the Internet through browsers to cloud computing consumers, the most popular uses of SaaS are; email clients, antivirus, and word processors. Users used this model to carry out online business and social computing tasks and pay for the service, not the software used. Besides, SaaS controls the usual compatibility, upgrading, installation issues, etc. desktop issues. However, SaaS architecture is specially tailored to simultaneously cater to various users (multitenancy) [61]. For customers, SaaS may leave out expenditure on servers and software licensing; for SaaS providers, it is not only necessary to keep a program, but it can also significantly decrease the cost. A typical representative is to provide online office software for Google

Apps or Microsoft [64]. SaaS makes access to apps and databases easier for the user. On their local device, the user does not have to install and run the application [65].

2. Platform as a Service (PaaS)

PaaS is identical to SaaS, as a service provides a complete framework for development, from design to implementation and testing. PaaS allows developers to outsource virtual development framework information on immediate on-demand service via the Internet and to use it to create and implement vendor-supported application instruments and programming languages [62]. Besides, PaaS provides an Integrated Development Environment (IDE) that supports a full application development lifecycle (planning, design, building application, deployment, testing, and maintenance). PaaS offers a platform for the cloud user to test any request [66]. PaaS services are hosted in the cloud and accessed merely through their web browser by customers [67].

3. Infrastructure as a Service (IaaS)

IaaS provides computing infrastructure as services to inform Virtual Machine (VM) that has all of the developer's resources. Also, a user can request infrastructure or resources needed over the Internet via web browser and pay for use instead of buying the software, network tools, servers, datacenter and the expertise needed to handle it. Furthermore, since cloud services are extremely flexible, a client can automatically shrink or grow the number of VMs running at a particular time [63]. The IaaS offers a virtualization platform by generating VMs to help users perform their duties within a reasonable period of time [68]. According to a study published by North Bridge Venture Partners, 56 percent [69] of companies use IaaS techniques to harness elastic computing resources in combination with Gigaom Research and a record 72 collaborating organizations on 19 June 2014 [69]. IaaS service, for instance, where customers can dynamically alter storage size as required, making it a very scalable resource that can be adapted on demand [70].

1.4 Motivation

The principle motivation of this research is to make aware the people the features of cloud, security in cloud, security consideration in cloud, methods that can be used in

cloud, what is cryptography, what is steganography and mainly to let people know about different types of cryptographic algorithms and comparison between them. And we have proposed a hybrid method to prevent security issues in cloud computing.

1.5 Rationale of the Study

Cloud computing is one of the most usable things in all around the world, but there are a lot of security risks in cloud computing nowadays. Cryptography is one of the most usable security in cloud nowadays and there are a lot of cryptographic algorithms available for encryption and decryption of data. By adding steganography with cryptography our hybrid model can reduce a lot of security risks in cloud computing.

1.6 Research Questions

There are a lot of security issues in cloud like attacks by Other Customers, Shared Technology Vulnerabilities, Failures in Provider Security, Insecure Application Programming Interfaces etc. Our research is to eliminate as much as security threats in cloud computing.

So the questions which arose in the beginning of our research were-

- What are the main features of cloud?
- What are the actual security risks in cloud?
- What are the conventional ways of securing cloud?
- What is actually missing in the conventional ways?
- How can we build a framework to reduce security risks?

1.7 Expected Output

People all over the world are using cloud nowadays without knowing the risks and prevention of these security issues and a lot of people with minimum knowledge of IT are using it and it depends on the cloud vendor to secure their data. But with all the security issues and conventional ways of security its not possible to get the expected outcome. In our research we have tried to make a hybrid framework to reduce the security risks in cloud computing and by applying this framework we believe the risk of security issues in cloud computing can be reduced.

1.8 Report Layout

In this report, by evaluating different cryptographic algorithms we have proposed a hybrid framework for security risks in cloud computing so that people might get a safe cloud all over the world. This report is divided into five parts.

This is the first part where we're talking about our work motivation and the anticipated result.

In the second chapter we address associated work, range of issues, difficulties, etc.

We address the process and execution of information collection in third chapter

Chapter four is for the results and evaluation of experiments.

Lastly chapter six represents the conclusion and future work.

CHAPTER 2 (Background)

2.1 Introduction

Cloud computing deals with data integrity and confidentiality the most prevalent problems of today [26]. Cloud users place their data in various cloud vendor processing technologies. However, the issue is that the customer does not understand where the data is placed and does not have any power over it.

Several security issues cannot be ignored in cloud computing. In its recent research, ENISA (European Union Cybersecurity Agency) acknowledged thirteen technical risks. According to NIST (National Institute of Standards and Technology), cloud computing presents some unique security challenges arising from the very high point of outsourcing, network dependence, exchanging (multi-tenancy) and cloud scale [45]. Fernandes et al. [46] provides an in-depth summary of the literature of studies to identify accessible cloud security issues and challenges.

1. Data Acquisition

Data acquisition is a method of obtaining distinct device data. The information flow and Peer to Peer activities should be known to cloud customers and utility providers [11], how and where we receive the data.

2. Confidentiality

Data confidentiality is essential for clients to obtain their private information in the cloud. It is one of the cloud's biggest problems. Cloud data is collected remotely and suppliers use cloud facilities to record data such as VM device (picture), record and record records or servers [11,21]. The client utilizes the shared storage to split the data and program. Sometimes confidentiality issues occur due to assault, evil intervention, and device inability. We, therefore, want excellent procedures of safety and techniques for fastening sensitive data, unsecured transmission or processing.

3. Ethics and Authenticity

This is another safety issue in the cloud. Information integrity means providing data from unlawful deletion, manufacture or alteration. Data integrity is simple in separate programs and databases; however, it is difficult in cloud instances as cloud providers operate with numerous databases, software, computers, and networks [20,22]. Authenticity relates to data surveillance and accessibility of information. Only those customers have access to the data approved by the provider. Cloud is an affordable data source, so many customers have faced the issue of consent and information accessibility for a while.

4. Multi-tenancy

Multi-tenancy shows where cloud systems share computer instruments, transport, utilities, and network. It is a cost-saving approach and offers greater use of resources. However, it is detrimental because of its data confidentiality owing to mutual assets. Many evil operations destroy computers and group tools, so the stream of information or data (leakage) is not difficult to regulate. A digital device strike is one of the previous issues using multi-tenancy. The improvement of techniques and the use of networks provide a bunch of facilities for individuals. However, it also enhances many safety problems; cyber-attack is just one of these. Cyber-attacks use evil software to change information, leading to harmful effects that can undermine data and contribute to cyber-crimes, including the robbery of information and identification. Some significant threats include identity theft, malware, phishing, spoofing, trojan and virus attacks, password tracing, DoS (Denial of Services) attacks and Dispersed-denial-of-service (DDoS) attacks [12].

5. Vulnerabilities of shared techniques

It's also a safety criticality line that finds the cloud so fascinating. As Navati et al. [47] indicated, vulnerabilities could be exploited by attackers in the hypervisor and entry to the physical computer where other neighboring virtual machines (VM) are situated.

6. Data breach

User data can be affected by both random data loss and evil intrusive actions. Data loss is beyond the reach of this work, as we regard only information breaches here, i.e. the theft of delicate information (such as personal or credit card details) [50].

7. Account or service traffic hijacking

Users may lose control over their account. This allows the intruder to enter critical areas of a deployed service and may compromise the confidentiality, integrity, and availability of such services [50].

8. Denial of Service (DoS)

One of the most alarming scenarios is when the cloud infrastructure becomes unavailable (just think an outage costs \$66 K per minute for Amazon). DoS in a cloud framework is even more hazardous than in a traditional one since the cloud climate gives extra computing energy to that system when the workload rises concerning a particular product. This means, on the one hand, the cloud system counteracts the attack's effects, but on the other, it supports the attacker in his evil activity by providing him with more resources [48].

9. Malicious insiders

This increases the cloud's roster of major risks. An insider's opportunity to be evil – e.g. An employee who might try to bring benefit of his protected position to unlock sensitive information becomes more concrete and worrying [49].

Cloud computing devices provide their clientele with multiple alternatives. Cloud computing is an interconnected network's huge array. The main task, therefore, is to give the cloud society security. Cloud computation has an amount of security issues. Safety's most significant aim is to make the data accessible, confidential and integral. There are so many cloud system-related dangers, such as data that an unlawful person could retrieve. The third party can change data while changing the data. Cryptography is an efficient way to protect delicate information as it is placed on databases or transferred through

network communication routes. In this document, we will use three Different Security Algorithms to use "A Hybrid Framework" in cloud computing.

We have tried to discuss different cryptographic algorithms in these different security approaches, and we have proposed a hybrid framework among those algorithms so that people can get a safer cloud.

2.2 Related Works

Cryptography is the main technique to secure data on clouds so that no one can steal our data and use it somewhere else or abuse it. There are a lot of cryptographic algorithms available in today's technology to secure data on cloud.

In the following table we have discussed and compared different cryptographic algorithms, based on their key size, speed, advantages, limitations, known attacks. The main parameter for assessing the effectiveness of the encryption algorithm is the rate at which the information is encrypted by a specific algorithm [55].

Table 2.1 will reflect an image of related works which have been done in the field of cloud computing.

Table 2.1: Comparison between different cryptographic algorithms

Type	Algorithm Name	Key size	Speed	Advantages	limitations	Known Attacks	Ref.
Symmetric	DES	64 bits	Very slow	DES has been a well-designed block cipher.	Due to the weak keys, it is subjected to brute force attack	Brute Force Attack	[13][14]
	3 DES	192 bits	Slow	3DES increases the size of the key by using three unique keys to progress the calculation	Due to its threephase encryption characteristics, it always requires more time than DES.	Brute force attack, plaintext selected, plaintext known	[13][14]
	AES	256 bits	Very Fast	It is the most solid security protocol as it is implemented in both hardware and software.	Has a very easy key schedule and easy encryption	Side-Channel Attack	[13][14] [16]
	Blowfish	256 bits	Fast	It provides longterm security of data with no known vulnerability in the backdoor	Due to varying key length, blowfish needed more processing time.	Dictionary Attack	[13][14] [16]

	RC5	0 to 2040 bits	Slow	The RC5 block cipher has a built-in variability parameter that offers flexibility at all safety and effectiveness level	This algorithm's velocity is slow.	differential and linear attacks	[15][16]
Asymmetric	RSA	2048 bits	Very slow	Convenience, tampering detection, non-repudiation provision.	Uses more computer resources, if necessary, a widespread safety compromise	Factoring the Public Key	[13][14][16]
	DSA	1024 bits	Fast	Signature calculation velocity is lower, less storage required	Data is not encrypted in DSA. It takes a lot of computing time.	Chosen Message Attack, Blinding, known partial key attack	[14]
	ABE	320 bits		The hackers find the algorithm very hard because it requires various measures.	The decryption of data is expensive.	Chosen-Ciphertext Attack	[15]
	El Gamal	1024 bits	Fast	ElGamal is useful because each time it provides distinct ciphertext for the same plaintext	Its need for randomness and its slower speed (particularly for signing).	Ciphertext attack	[13][17]
	Diffie-Hellman	—	Slow	Secret sharing is safe, sender and receiver do not know each other beforehand	Can't be used to exchange asymmetric key and sign digital signatures.	man-in-the-middle attack	[14][16]

2.3 Research Summary

There are a lot of people around the world using cloud nowadays and thus cloud has become one of the most usable technologies all around the world. But, there are a lot of risk in cloud computing like data loss, data breaches, denial of service, malicious insiders, abuse of cloud services etc. All of these security breaches are very common nowadays. By analyzing different cryptographic algorithms which are used to prevent these threats we have proposed a hybrid approach in our research to reduce these risks. In our research we have combine Cryptography and Steganography together to build a safer and reliable model based on those cryptographic algorithms.

2.4 Scope of the Problem

Many people are losing their valuable data on internet nowadays. This is a very common but very destructive thing for people. So, we have decided to research cloud computing for more security and to give a perfect model of data security so that people might not have to face doom on the internet. Furthermore, our research will help people to get a

better understanding about security in cloud. So, the scope of the present study is Security issues and solution in cloud computing.

2.5 Challenges

We faced a lot of challenges in our research. But we managed to overcome those difficulties eventually by the grace of almighty.

These following difficulties made our research more difficult –

1. we had to research every algorithm particularly which was very time consuming
2. comparing those algorithms
3. choosing algorithms for our framework
4. defining every aspect of security risk in cloud computing

CHAPTER 3 (Research Methodology)

3.1 Introduction

Many Safety techniques are utilized to secure data and information. We explain some methods here are following -

1. Cryptography

Cryptography is a technique of data transformation that can be used to provide various security-related thoughts such as privacy, data integrity, authentication, permission, and non-repudiation [54]. It is an unreadable file technique for obtaining information and communicating information. To change the readable text (recognized as plain text) to an unreadable hidden format (recognized as ciphertext), we use encryption. We claim it's a secret writing technique. Cloud computing's main issues are data security, backups, network traffic, file system, and server security [52], and cryptography can somehow fix these issues. Only those individuals who encrypt the data and comprehend the decryption key can get readable form information or data (policy document). Cryptography performs a significant role in ensuring transmission or retention of ATMs, e-commerce, digital press loneliness, and Internet information. For four major problems such as non-repudiation, honesty, authentication, and confidentiality, modern cryptography works. In essence, cryptography is the technique of information encryption and decryption [23]. Encryption will help prevent activities such as man-in - the-middle (MITM), spoofed attacks, and meetings of hijacking [53].

1.1. Encryption and Decryption

Encryption is the technique of turning data or information (plaintext) into a distinct type, called ciphertext, but no one can comprehend it except approved individuals. The technique of turning ciphertext home to plaintext is decryption. The main purpose of encryption is to protect the confidentiality of electronic information recorded on software devices or transferred on the network (Internet) via another laptop. We generate a link to the data encryption period in the encryption and decryption method and also use another or the same button to decrypt the data [24].

2. Steganography

Steganography is the craft of typing that is concealed. In the steganography method, we hide a hidden signal in a standard text (Picture, Video, and Audio) along with the notification of infusion in its destination [23,25]. We are primarily investigating three kinds of steganography, private key steganography, public key steganography, and sheer steganography. Its benefit over cryptography is that the permitted confidential signal does not draw the third party's focus. Using this method, transmitting and saving information on the Internet is therefore quite safe.

3.2 Cryptographic Algorithms

The algorithms which we will be using are -

1. DSA (Digital Signature Algorithm)
2. AES (Advanced Encryption Standard)
3. Steganography (Hiding data behind an audio file or image)

A. DSA (Digital Signature Algorithm)

The Digital Signature Algorithm (DSA) was introduced in the United States in 1994. Department of Commerce and National Institute of Standards and Technology [30]. In the contemporary world, digital signatures are highly important for checking the identification of the sender. A digital signature is a digital signature used for data confirmation and authentication. An electronic signature is depicted in the pc scheme as a sequence of binary numbers. The contract involves several parameters and regulations (algorithm) that could be verified as well as the creativity of this data as the identification of the person registering the paper. The signature is developed with a private key's assistance. Only the sender knows a private key. The receiver verifies the request using a public key that matches the private key. With any kind of information, a digital signature can be used, whether encrypted or not. Digital signatures are used to identify unlawful third-party changes in data. The holders of a digitally signed document also ensure that the document is allocated by the individual who promises to sign. This is regarded as non-repudiation since afterward the individual who submitted the document is unable to

repudiate the signature. Digital signature algorithms can be used in messages, exchange of electronic money, allocation of software, data storage that guarantees information's authenticity, legitimacy, and creativity. In the token creation phase, a hash function is used to get a compressed copy of data called a digest signal. To generate the digital signature, the digest signal is then entered into the digital signature algorithm [18].

B. AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is the standard for electronic encryption of data developed by the United States. In 2001 the National Institute of Standards and Technology (NIST) [32]. AES is focused on a planning concept recognized as a replacement-permutation network that combines substitution as well as permutation, and is fast in both technology and hardware [30]. Once DES had been used for more than 20 years as an encryption model and had been prepared to be deciphered in a relatively brief amount of moment, NIST (United State National Institute of Standard and Technology) chose a fresh benchmark, the Advanced Encryption Standard (AES), had to be brought into position. AES is focused on the cipher of Rijndael. The U.S. government has adopted AES and is common today. This ruling was announced on January 1997, together with the creation of a petition for AES applicants. The AES was to be an algorithm of symmetric matrix code promoting 128-, 192-, and 256-bit key sizes. AES is focused on networks of replacement and permutation. It does not use the network of Feistel. It's safer than DES and hard to break. AES is much more complex than DES, but it is fast and efficient. It works with plain text and main edition numbers of the 128-bit remedy section size [27]. AES has been thoroughly screened for many safety applications [56][57]. It can be implemented in various systems, especially in small devices [58]. It has been discovered in [59] that AES is faster and more efficient than other encryption algorithms.

C. STEGANOGRAPHY

Steganography is the science of concealing messages in such a way that no one knows about the presence of the message apart from the intended recipient. Steganography is the method of concealing in another one only one form of interaction (writing, noise or

image). The word steganography originates from the Greek steganos (covered or hidden) and graphics (drawing or text), which implies coated text. Steganography is the tradition of storing secret information in such a manner that under the image or image in which it is concealed the very presence of the information. For instance, the use of cleverly selected phrases, invisible ink formed between marks, sentence or line spacing modulation, and microdots are documented throughout history. The confidential data is normally concealed by using an innocuous cover to create no trouble for anyone. Steganography edge over cryptography is that the main text does not attract notice to itself because the text could be concealed under image file, audio frame, etc. [19].

Various methods for steganography are accessible as follows:

1. Wax bottle data disguise.
2. Data concealed in a loud image.
3. Hidden messages below some other posts sterile part.
4. Data hiding from the noise record.
5. Data hiding under the audio folder.

3.3 Design of proposed work

Figure 2 represents our framework's working process. At first, it will use DSA to create a digital signature, then it will use AES to encrypt the data of the user and to increase the security we have used steganography.

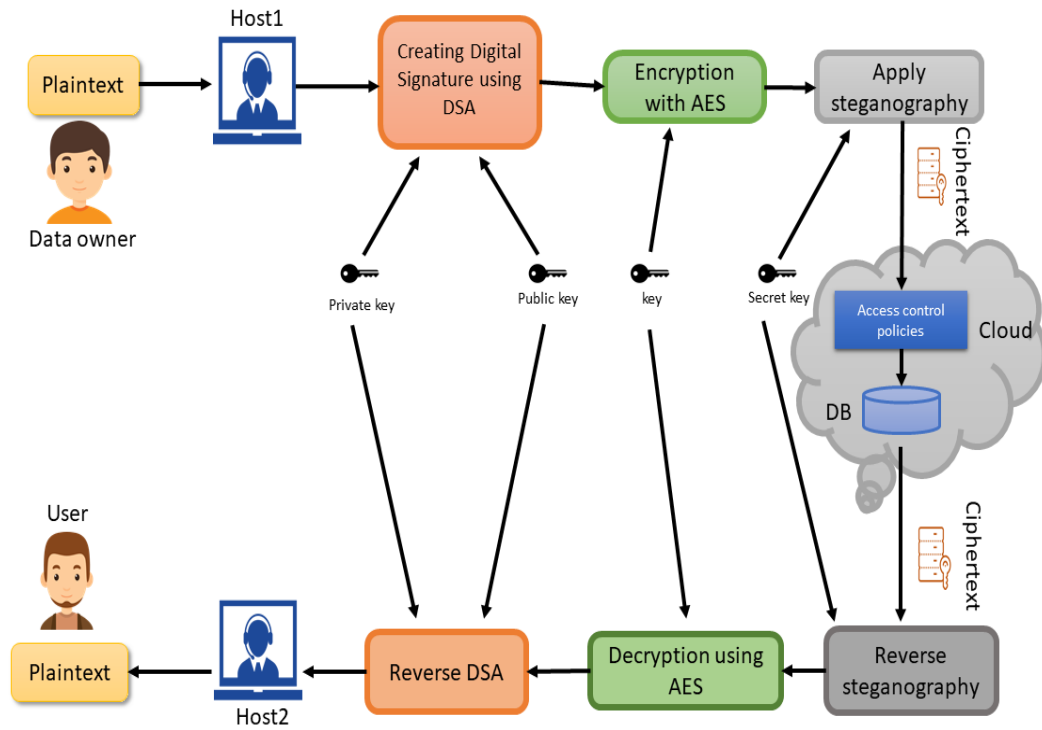


Figure 3.1: Hybrid framework for security in cloud computing

3.4 Elaboration of Overall System

STEP 1 (Applying DSA for generating digital signature)

A digital signature is a mathematical method used to validate a message, software or digital document's authenticity and integrity. A digital signature offers much more inherent security as the digital equivalent of a handwritten signature or stamped seal and is intended to solve the problem of manipulation and impersonation in digital communications. Figure 3.2 shows the generation of a digital signature using a digital signature algorithm.

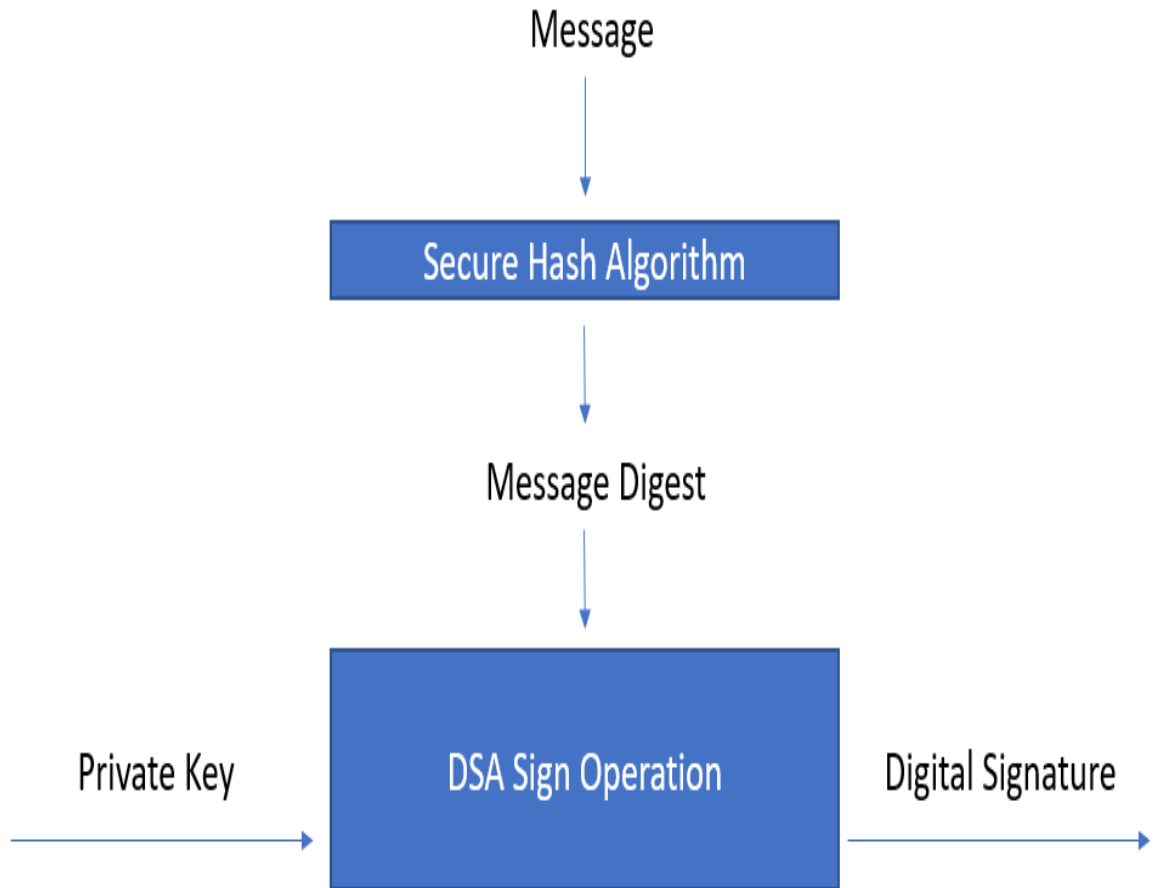


Figure 3.2: Digital signature generation using DSA [30]

Algorithm (DSA for signature creation) [31]

The algorithm used for creating this signature is given below-

INPUT:

Domain parameters (p, q, g) ; signer's private key a ; message-to-be-signed, M , with message digest $h = \text{Hash}(M)$.

OUTPUT: Signature (r, s) .

- Choose a random k in the range $[1, q - 1]$.
- Compute $X = g^k \bmod p$ and $r = X \bmod q$. If $r = 0$ (unlikely) then go to step 1.
- Compute $k^{-1} \bmod q$.
- Compute $h = \text{Hash}(M)$.
- Compute $s = k^{-1}(h + ar) \bmod q$. If $s = 0$ (unlikely) then go to step 1.
- Return (r, s) .

STEP 2 (Applying AES for encryption)

AES is not a Feistel cipher, but an iterative one. It is based on the 'network of substitution – permutation'. It includes a series of linked operations, some of which involve replacing inputs with specific outputs (substitutions) and others involve shuffling bits (permutations) around them. Interestingly, AES performs all its computations on bytes rather than bits. AES therefore treats the 128 parts of the plaintext block as 16 bytes. These 16 bytes are arranged for matrix processing in four columns and four rows. The number of rounds in AES, unlike DES, is variable and depends on the key length. For 128-bit keys, AES utilizes 10 rounds, for 192-bit keys 12 rounds and 256-bit keys 14 rounds. Each round utilizes another 128-bit round key calculated from the initial AES key. Figure 3.3 describes the algorithm for encryption using AES.

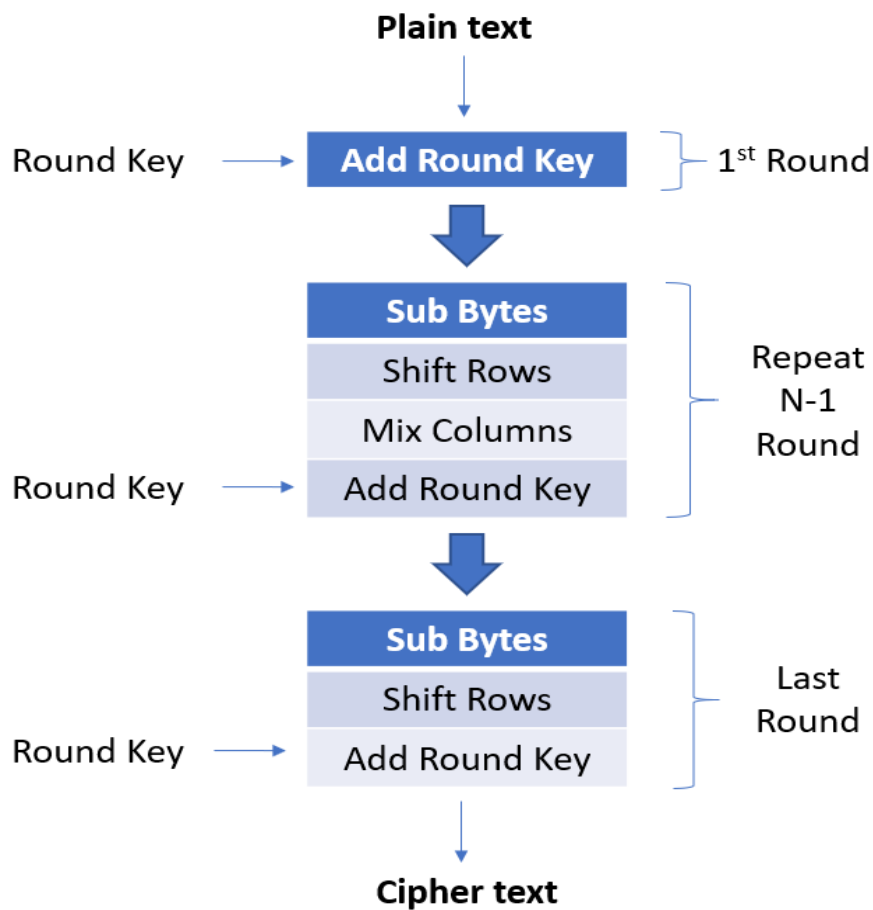


Figure 3.3: Encryption Using AES [32]

STEP 3 (Applying Steganography for encryption)

Figure 3.4 shows a general structure for encryption using steganography. It is presumed that the sender wants to send a signal to a receiver through Steganographic transmission. The sender begins with a cover message, in which the integrated message is concealed, which is an input to the stego system. The message concealed is called the message integrated. A steganographic algorithm combines the cover message with the embedded message, which is something to hide in the cover. The algorithm may or may not use a steganographic key (stego key), which is additional secret data that may be needed in the hidden process [29].

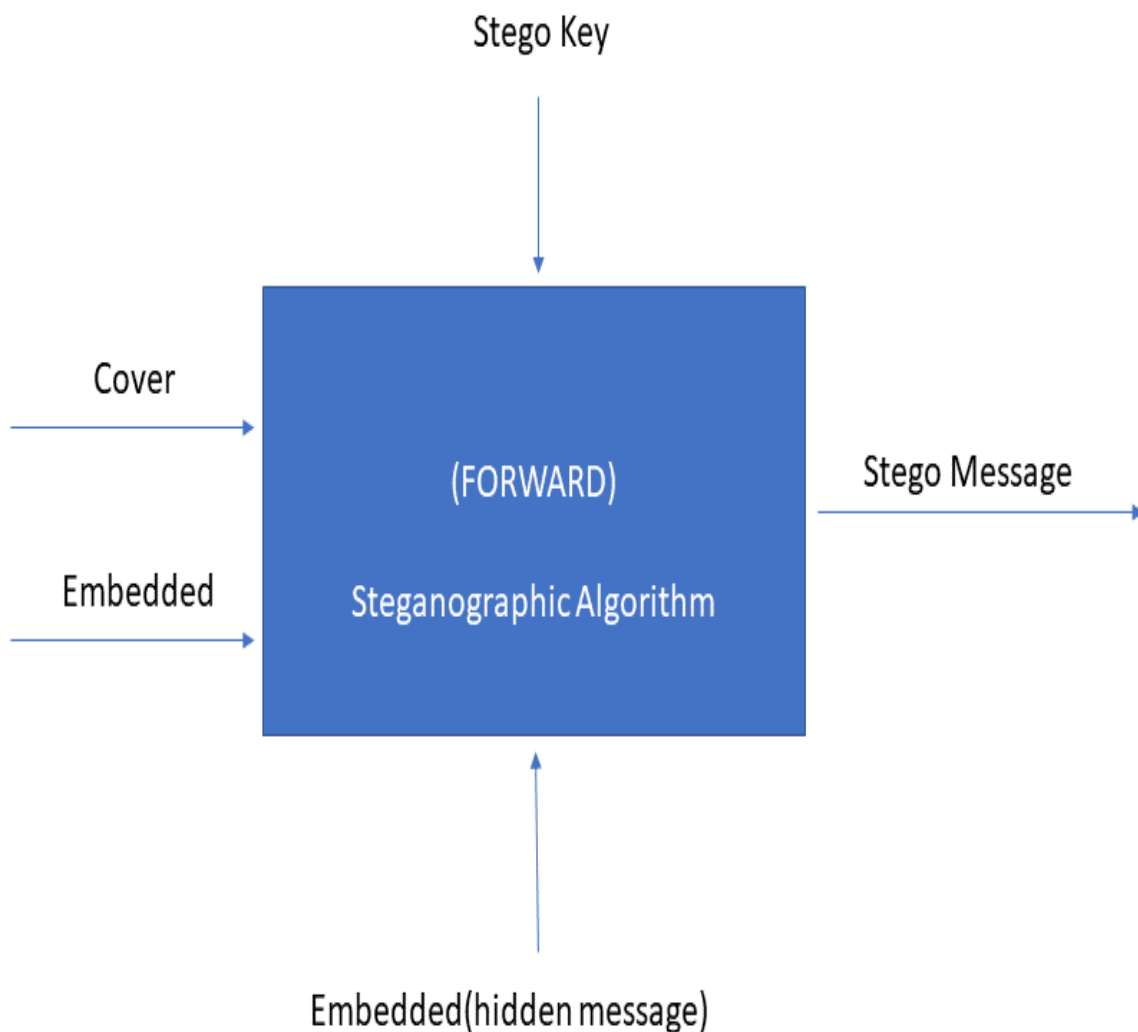


Figure 3.4: Encryption using steganography [28]

Framework (Encryption using Steganography)

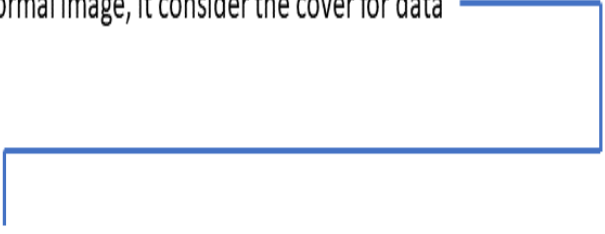
Figure 3.5 shows the framework for hiding operation using steganography-

Input: Hidden file name, cover file name.

Output: Stego-File

- Begin
- Opens the cover file(EXE file).
- Assign a pointer to the end of (section header), which is before the image page of the cover file.

- Select the image page considering normal image, it consider the cover for data

- 
- Begin
 - Write the hidden file name
 - Assign a pointer after hidden file name
 - Encrypt the hidden file content using file name as a key
 - Write the encrypt content to the image page for EXE file after hidden file name
 - End

- End

Figure 3.5: Framework Algorithm for encryption using steganography [28]

STEP 4 (Applying Steganography for decryption)

Usually the same (or linked) key is required to retrieve the integrated message. The Steganographic algorithm's output is the message of stego. The cover message and stego text must be of the same sort of information, but another sort of information may be the integrated message. To extract the embedded signal, the receiver reverses the embedding process [29]. Figure 3.6 shows a general process of reverse steganography-

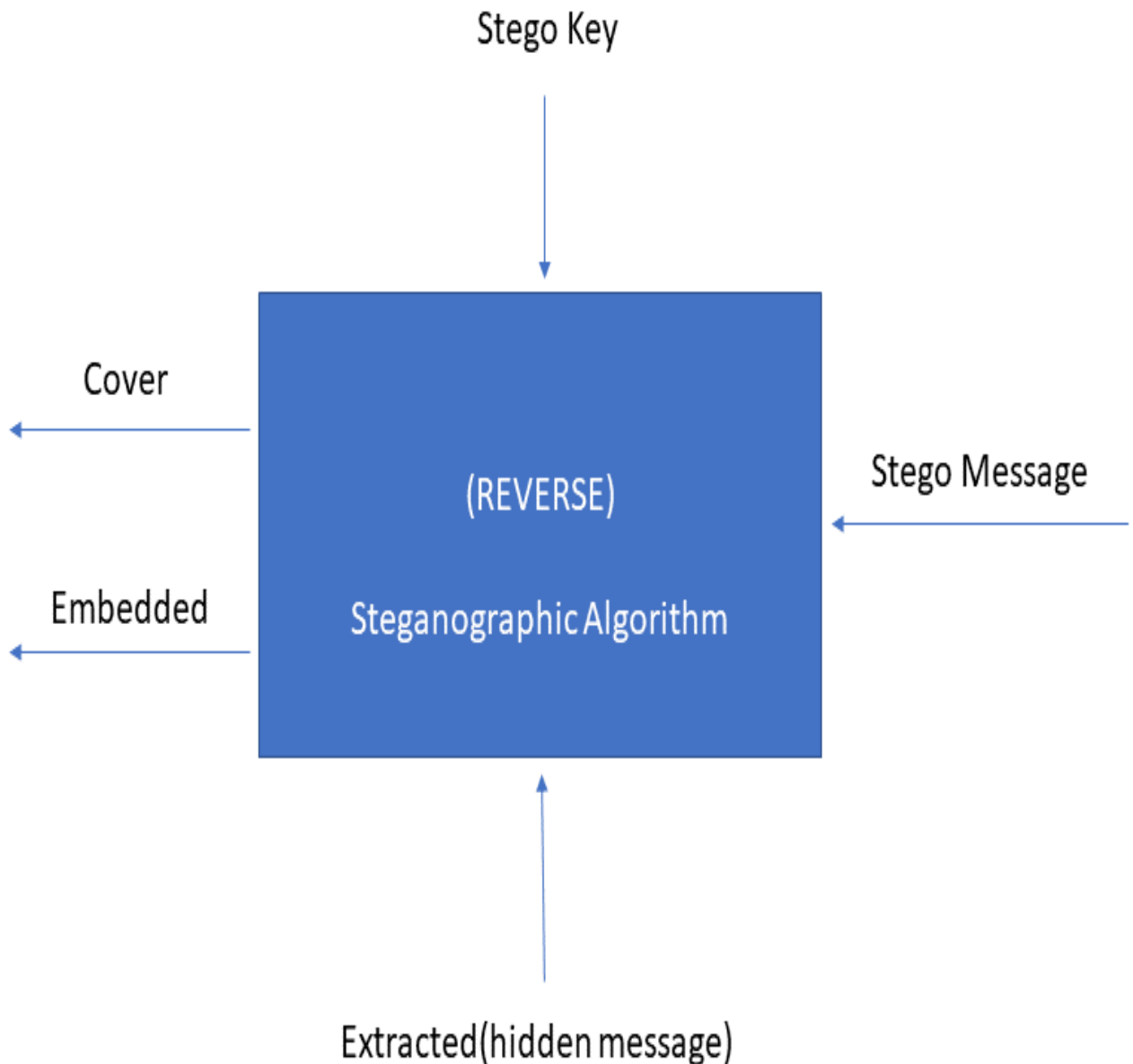


Figure 3.6: Decryption using steganography [28]

Framework (Reverse Steganography)

Figure 3.7 shows the framework for retraction operation using steganography-

Input: Stego-file

Output: Hidden information

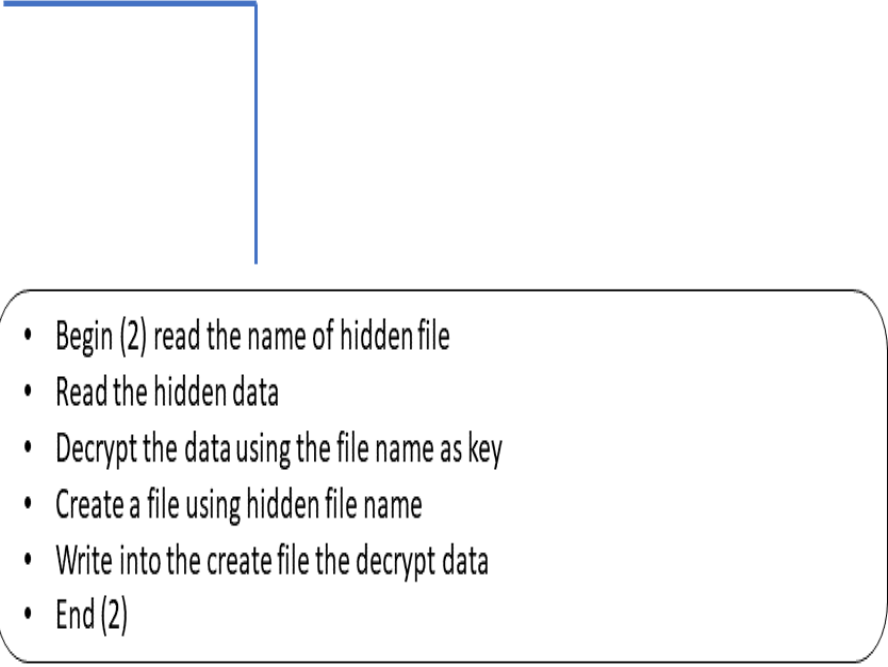
- Begin(1)
 - Select the cover file.
 - Get the end of (Section header) of EXE file
 - Select the image page
- 
- Begin (2) read the name of hidden file
 - Read the hidden data
 - Decrypt the data using the file name as key
 - Create a file using hidden file name
 - Write into the create file the decrypt data
 - End (2)
- End (1)

Figure 3.7: Framework Algorithm for decryption using steganography [28]

STEP 5 (Applying AES for decryption)

The cipher text that we got from step 2 will have to be decrypt in this step by using AES again.

Figure 3.8 shows the algorithm and process of decrypting the ciphertext using AES.

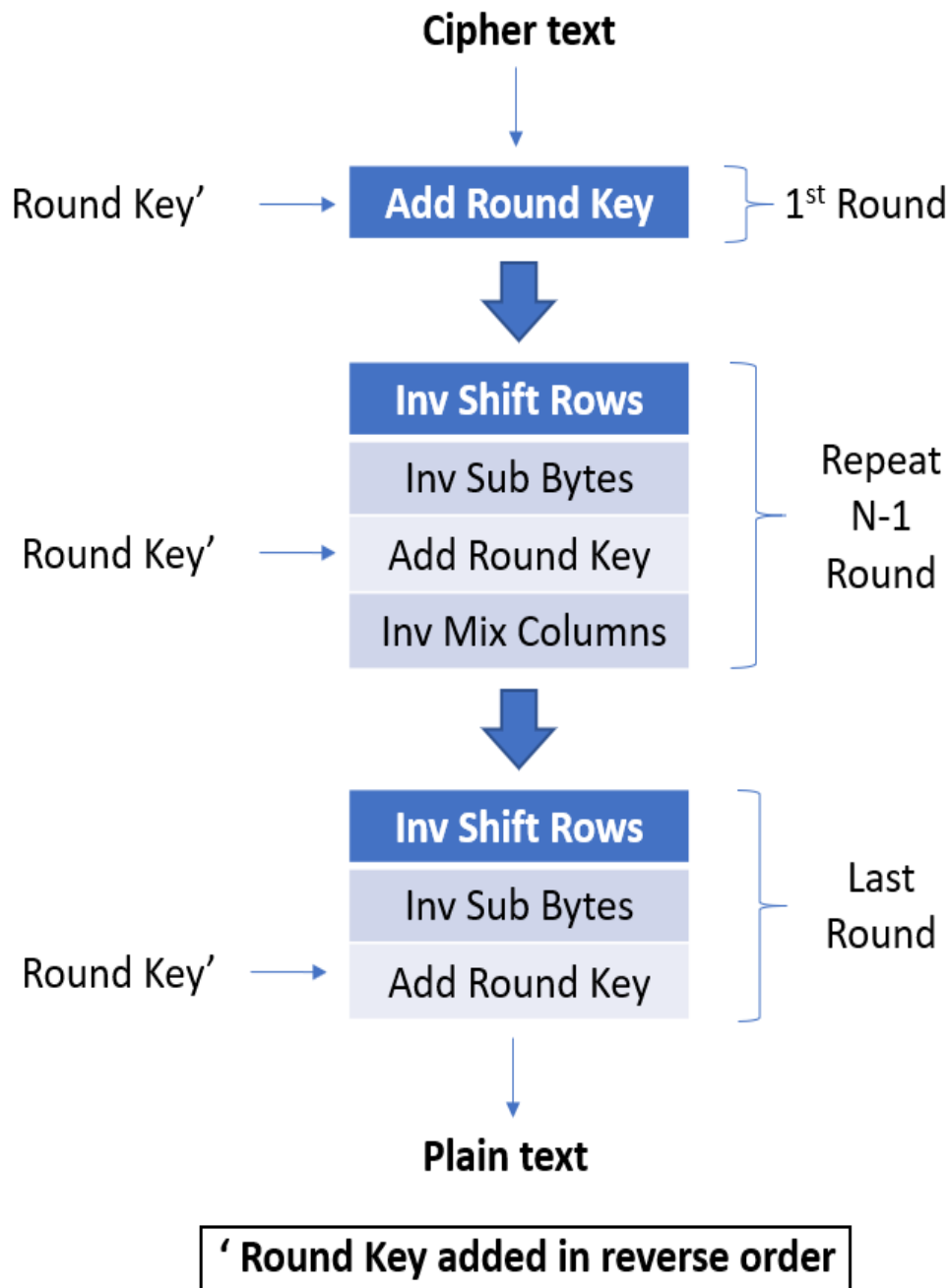


Figure 3.8: Decryption Using AES [32]

STEP 6 (Applying DSA for verifying the digital signature)

The signature we created in step 1 will have to be verified by using DSA in this step. Otherwise the data will be lost. Figure 3.9 shows a general process of signature verification using DSA-

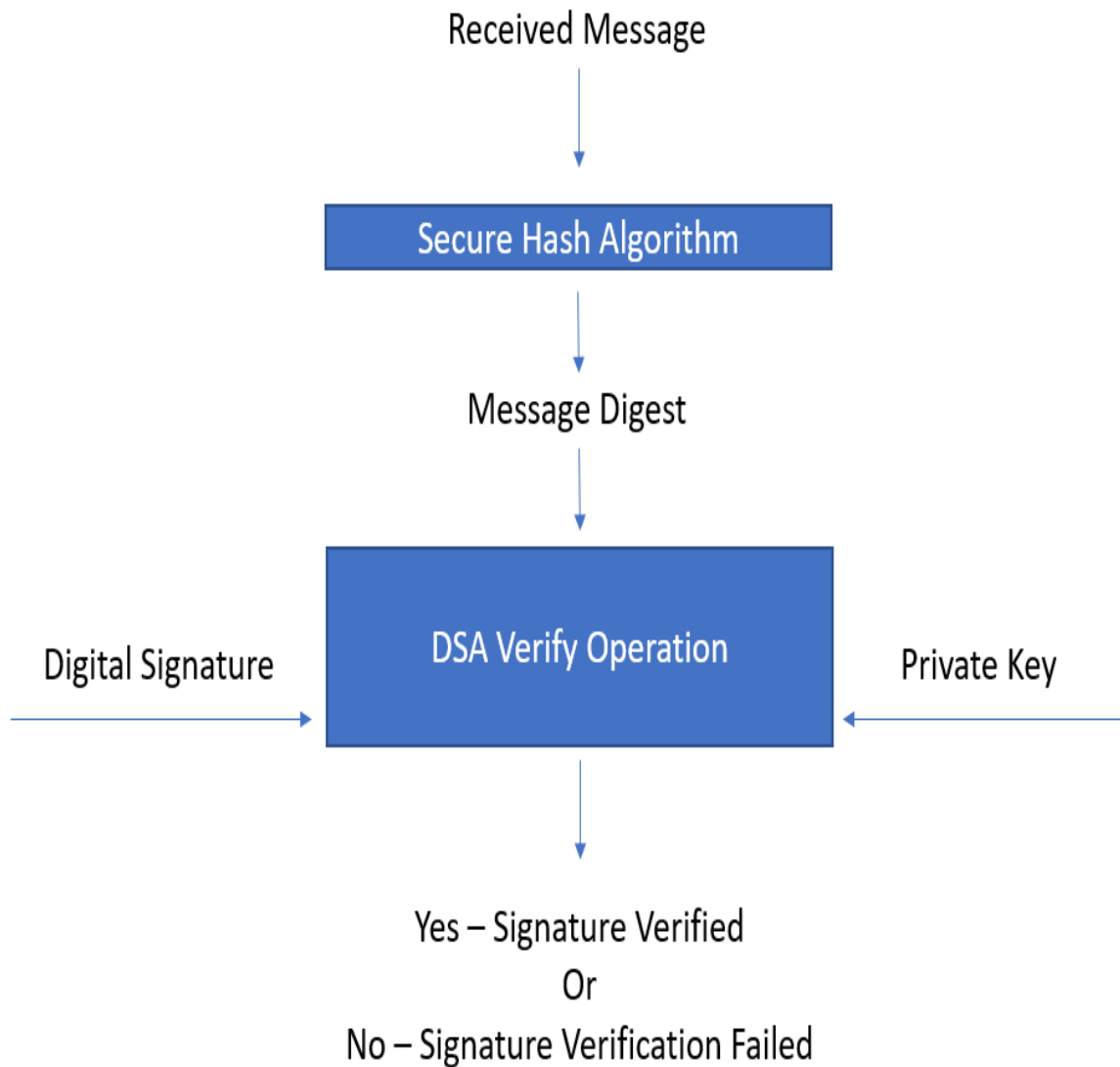


Figure 3.9: Signature Verification using DSA [30]

Algorithm (Reverse DSA) [31]

The algorithm used for verifying this signature is given below-

INPUT:

Domain parameters (p, q, g); signer's public key A; signed-message, M, with message digest $h = \text{Hash}(M)$; signature (r, s).

OUTPUT: "Accept" or "Reject".

- Verify that r and s are in the range $[1, q - 1]$. If not then return "Reject" and stop.
- Compute $w = s^{-1} \bmod q$.
- Compute $h = \text{Hash}(M)$.
- Compute $u_1 = hw \bmod q$ and $u_2 = rw \bmod q$.
- Compute $X = g^{u_1} * A^{u_2}$
- If $v = r$ then return "Accept" otherwise return "Reject".

3.5 Research Subject and Instrumentation

The most important thing in cloud computing is data security. Almost everyone nowadays are using cloud without knowing the risks. Cloud vendors are providing cloud to normal people which they are using but there are a lot of securities issues and it has been common to lose data on the internet nowadays. This is because of internal or external attacks on clouds. So, our research subject is to analyze different cryptographic algorithms and among them we have chosen the best ones to build our hybrid framework. We have analyzed a lot of algorithms in this paper and among those DSA and AES are somewhat better than other algorithms. So, we have chosen these two algorithms along with steganography to build our hybrid framework.

3.6 Data Collection Procedure

For completing our research, we need to collect data. We collected data via online. We downloaded a lot of research papers, journals, report on our chosen topic and gather a lot of data. And then we had to analyze and combine those data to build the comparison table of our paper and among those data we had to choose the best ones to build our framework.

3.7 Statistical Analysis

After collecting our data from different research papers, journals, reports we had to combine them and we built a table to compare those data and according to data we had to choose our algorithms based on different questions-

Q1- What is the key size of the chosen algorithm?

Q2- What is the speed of the chosen algorithm?

Q3- What are the advantages of the chosen algorithm?

Q4- What are the limitations of the chosen algorithm?

Q5- What are the known attacks that can affect the chosen algorithm?

CHAPTER 4 (Experimental results and discussion)

4.1 Introduction

We have discussed the risks in cloud computing and furthermore we have analyzed a lot of cryptographic algorithms, in which we have chosen 2 of them. One is for digital signature and another is for encryption and along with them we have combined steganography to build a safer and more reliable framework for security in cloud computing.

4.2 Experimental Results

Our suggested design consists of the best cryptographic algorithms and steganography. In the following table, we will see the best cryptographic algorithms-

Table 4.1: Two best algorithms according to Table 2.1

Type	Algorithm Name	Key size	Speed	Advantages	limitations	Known Attacks	Ref.
Symmetric	AES	256 bits	Very Fast	It is the most solid security protocol as it is implemented in both hardware and software.	Has a very easy key schedule and easy encryption	Side-Channel Attack	[13] [14] [16]
Asymmetric	DSA	1024 bits	Fast	Signature calculation velocity is lower, less storage required	Data is not encrypted in DSA. It takes a lot of computing time.	Chosen Message Attack, Blinding, known partial key attack	[14]

From Table 2.1, we can compare and see, these two are the best encryption algorithms available.

4.3 Descriptive Analysis

After analyzing all the algorithms we have chosen DSA for digital signature and it's the fastest among all asymmetric algorithms, we have chosen AES for encryption which is the fastest among all symmetric encryption algorithms and combine these two with

steganography for an extra layer of security which will give us a more reliable and safe way to protect our data on cloud.

4.4 How the Data will be secured in our system

In our hybrid framework, in the 1st step, we will create a digital signature using DSA to verify the owner of the data, then in the 2nd step that data will be encrypted by AES algorithm which is the best cryptographic algorithm since time, and then in the 3rd step, that encrypted data will be again encrypted using STEGANOGRAPHY for an extra layer of security.

From the 4th step, our system will start to reverse the whole process to get the original data.

In the 4th step, it will reverse the data through reverse STEGANOGRAPHY to get the encrypted file from step 2 and then it will decrypt that data using AES again in step 5 to get the original data. Afterward, in the 6th step or in the final step, it will verify the data using reverse DSA again to verify the owner of that data.

4.5 Summary

We have discussed about cloud and cloud securities in our research. According to our analysis, we have got two best cryptographic algorithms (DSA and AES) along with steganography to build our framework.

CHAPTER 5 (Summary, Conclusion, and Implication for Further Research)

5.1 Summary of the study

Cloud computing produced both enthusiastic and edgy end users. They are enthusiastic about the cloud's multiple possibilities and are also nervous about the safety issues it provides. As users migrate their data on cloud, they would be alarmed with the security flaws inherent to the cloud environment. As a result, safety threats with cloud computing have appeared as one of the most plausible subjects. This study has analyzed almost every cryptographic algorithm that are used for encryption of data in cloud and we have also discussed about steganography. And among all of them we have chosen two of the encryption algorithms along with steganography to propose a hybrid model for security of data in cloud computing.

5.2 Conclusion

For many Internet facilities, cloud computing provides a flexible and cost-effective alternative [51]. The contemporary sector of IT is focused entirely on online service or Internet facilities. In cloud computing techniques, this article discussed security problems and how they can be averted. Here we use together techniques of cryptography and steganography to protect information. Algorithms for DSA and AES are somewhat more secure than other algorithms. In order to give more data protection, we integrate AES and DSA with steganography. We get an encoded image in the steganography operation, which the human eye looks exactly the same as the initial image. If we study the binary picture codes, we could see the differences. Otherwise, the original picture cannot be spotted. The hybrid framework we suggested in this document for cloud computing security can assist create a strong data security structure in the cloud computing region or internet.

5.3 Implication for Further Study

Data security is the most important issue of cloud computing in the IT industry. Future work includes implementing Digital Signature Algorithm (DSA), Advanced Encryption Standard (AES) and STEGANOGRAPHY to provide maximum security in cloud computing. By implementing these three algorithms, it is possible to provide authenticity, security and data integrity to data. We hope this work help secure data from outsiders or hackers, who try to access and destroy the important data. We have located that the Time complexity is high because it is a one by one process, but in the future, this time complexity could be reduced. We will carry on this research in order to improve the functionalities of these algorithms in terms of robustness, reducing time complexity, hiding capacity and use other security algorithms or methods to protect information (data) on the cloud.

CONTRIBUTION FROM THIS R&D PROJECT

1. A framework named Hybrid Framework for Security in Cloud Computing has been proposed.
2. International paper-1: Scopus & DBLP indexed

Jannatul Ferdous, Md. Fuad Newaz Khan and Karim Mohammed Rezaul, " A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms ", Submitted to *International Journal of Network Security*, September 2019

REFERENCES

- [1] Adrian Duncan ,Sadie Creese , Michael Goldsmith , Jamie S. Quinton, “Cloud Computing: Insider Attacks on Virtual Machines during Migration. In Trust, Security and Privacy in Computing and Communications (TrustCom)”, *12th IEEE International Conference on. 2013. IEEE.* 2013
- [2] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.” *Proceedings of the 16th ACM conference on Computer and communications security*, 2009
- [3] Osanaiye O., K.K.R. Choo, and M. Dlodlo, “Distributed Denial of Service (DDoS) Resilience in Cloud: Review and conceptual Cloud DDoS Mitigation Framework”, *Journal of Network and Computer Applications*, 2016.
- [4] Yossi Gilad, Michael Goberman, Amir Herzberg, Michael Sudkovitch, “CDN-on-Demand: An Affordable DDoS Defense via Untrusted Clouds", 2016.
- [5] Tupakula, U., V. Varadharajan, and N. Akku. “Intrusion detection techniques for infrastructure as a service cloud. In Dependable, Autonomic and Secure Computing (DASC)”, *IEEE Ninth International Conference on. 2011*
- [6] Suleman Khan, Ejaz Ahmad, Muhammad Shiraz, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, “Forensic challenges in mobile cloud computing”, *Computer, Communications, and Control Technology (I4CT) International Conference on. 2014. IEEE,* 2014
- [7] Abdullah Gani, Golam Moktader Nayeem, Muhammad Shiraz, Mehdi Sookhak, “A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing”, *Journal of Network and Computer Applications*, pp. 84-102, 2014
- [8] Amani S. Ibrahim , James Hamlyn-Harris, John Grundy, Mohamed Almorsy, “Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model”, *Network and System Security (NSS) 5th International Conference on. 2011. IEEE,* 2011
- [9] Scarfone, K.,” Guide to security for full virtualization technologies” *DIANE Publishing*, 2011
- [10] AlZain, M.A., B. Soh, and E. Pardede. “MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. in Dependable, Autonomic and Secure Computing (DASC)”, *IEEE Ninth International Conference on. 2011. IEEE,* 2011
- [11] G. Dr. Mohammad V. Malakooti and Nilofar Mansourzadeh, "A Two Level-Security Model for Cloud Computing based on the Biometric Features and Multi-Level Encryption", *The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications*, Dubai, UAE, 2015.
- [12] K.S. Suresh, K.V. Prasad, "Security Issues and Security Algorithms in Cloud Computing", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, Issue 10, 2012.
- [13] Zoran Hercigonja, Druga gimnazija Varaždin, Croatia,” Comparative Analysis of Cryptographic Algorithms”, *International Journal of DIGITAL TECHNOLOGY & ECONOMY*, Vol. 1, No.2, pp.130-131, 2016.
- [14] R.Gowthami Saranya, A.Kousalya, "A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing”, *International Journal of Computer Science and Information Technologies*, Vol. 8 (2), page.309, 2017.

- [15] Saravana Kumar N, Rajya Lakshmi G.V, Balamurugan B,” Enhanced Attribute Based Encryption for Cloud Computing”, *International Conference on Information and Communication Technologies, (ICICT 2014)*.
- [16] Randeep Kaur, Supriya Kinger,” Analysis of Security Algorithms in Cloud Computing”, *International Journal of Application or Innovation in Engineering & Management*, Vol. 3, Issue 3, pp.173, 175, March 2014.
- [17] Rashmi Singh, Shiv Kumar, "Elgamal's Algorithm in Cryptography", *International Journal of Scientific & Engineering Research* Vol. 3, No.12, 2012
- [18] Garima Saini, Naveen Sharma, “Triple Security of Data in Cloud Computing”, *International Journal of Computer Science and Information Technologies*, Vol. 5, No.5, pp.5825-5827, 2014
- [19] Mr. Sailesh S. Iyer, Dr. Kamaljit Lakhtaria, “New robust and secure alphabet pairing text Steganography Algorithm”, *International Journal of Current Trends in Engineering & Research*, Vol. 2, Issue 7, page.15, July 2016
- [20] Mather T, Kumaraswamy S, Latif S, “Cloud Security and Privacy” *Sebastopol, CA: O'Reilly Media, Inc.* 2009
- [21] M.Marwaha, R.Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", *IJCSI International Journal of Computer Science Issues*, Vol. 10, Issue 1, No 1, pp. 367-370, January 2013.
- [22] Vinay Kumar Pant, Mr. Anshuman Saurabh, "Cloud Security Issues, Challenges And Their Optimal Solutions" *International Journal of Engineering Research & Management Technology*, ISSN: 2348-4039, Vol. 2, Issue-3, May- 2015.
- [23] William Stallng, "Cryptography and Network Security-Principles and Practices", *Third Edition, publication-Pearson*.
- [24] Ms. Shubhra Saggat, Dr. R.K. Datta, "An improved RSA Encryption Algorithm for Cloud Computing Environments: Two key Generation Encryption (2KGEA)", *International Journal of Software and Web Sciences* 5(2), ISSN: 2279-0063, pp. 127-131, June-August, 2013.
- [25] Rajeev Kumar, "DATA HIDING IMAGES USING SPREAD SPECTRUM IN CLOUD COMPUTING", *International Journal of Technical Research and Applications*, e-ISSN: 2320-8163, www.ijtra.com Vol. I, Issue 3, pp. 76-79, July-August 2013.
- [26] Vinay kumar pant, Jyoti Prakash, Amit Asthana, “Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques”, *International Conference on Green Computing and Internet of Things*, 2015
- [27] Miss. Shakeeba S. Khan, Miss. Sakshi S. Deshmukh, “Security in Cloud Computing Using Cryptographic Algorithms”, *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.9, September- 2014, pp. 517-525
- [28] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, “Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques”, *International Journal of Computer Science and Information Security*, Vol. 3, No. 1, 2009.
- [29] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, “ Novel Approach of Hidden Data in the (Unused Area 2 within EXE File) Using Computation Between Cryptography and Steganography ”,

International Journal of Computer Science and Network Security (IJCSNS) , Vol.9, No.5 , ISSN : 1738-7906, pp. 294-300.

[30] Shraddha Kulkarni, “Study of Modern Cryptographic Algorithms”, *International Journal of Advanced Research in Computer Science*, Vol. 8, No. 3, March – April 2017

[31] “Public key cryptography using discrete logarithms”. Part 4: Digital Signature Algorithm (DSA) <http://www.di-mgt.com.au/public-key-crypto-discrete-logs-4-dsa.html> (Accessed on 22 aug. 2019)

[32] Boukhatem Mohammed Belkaid, Lahdir Mourad, Cherifi Mehdi, “Meteosat Images Encryption based on AES and RSA Algorithms”, *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 6, 2015.

[33] Dimpi Rani, Rajiv Kumar Ranjan, “A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 6, 2014.

[34] M.Arun Fera, C. Manikandaprabhu, Ilakiya Natarajan, K.Brinda, R.Darathiprincy, “Enhancing security in Cloud using Trusted Monitoring Framework”, *Elsevier Procedia Computer Science* 48, pp. 198 – 203, 2015.

[35] Dr. D.I. George Amalarethinam, H. M. Leena, “Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud”, *World Congress on Computing and Communication Technologies (WCCCT)*, page. 174, 2017

[36] Thomas Erl, Zaigham Mahmood and Ricardo Puttini, “ Cloud Computing Concepts, Technology & Architecture”, *Prentice Hall, Service Technology Press*, 2013.

[37] <https://www.gartner.com/en/newsroom/press-releases/2017-02-22-gartner-says-worldwide-public-cloud-services-market-to-grow-18-percent-in-2017> (accessed on 3 september 2019)

[38] <https://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/global-cloud-index-gci/white-paper-c11-738085.html> (accessed on 3 september 2019)

[39] Casola V, Benedictis AD, Rak M., “On the adoption of security slas in the cloud. In: Accountability and security in the cloud”, *Springer Berlin Heidelberg*, pp. 45–62, 2015.

[40] Luna J, Suri N, Iorga M, Karmel A., “Leveraging the potential of cloud security service-level agreements through standards”, *IEEE Cloud Computing Mag.*, Vol. 2, No. 3, pp. 32–40, 2015.

[41] Deepak R Bharadwaj, Anamika Bhattacharya, Manivannan Chakkaravarthy, “Cloud Threat Defense – a Threat Protection and Security Compliance Solution”, *IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, page.95, 2018.

[42] Carlos André Batista de Carvalho, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho, Nazim Agoulmine, “ State of the art and challenges of security SLA for cloud computing”, *Computers and Electrical Engineering*, page. 1, 2017

[43] <https://blogs.dropbox.com/dropbox/2011/06/yesterdays-authentication-bug/> (Accessed on 3 sept. 2019).

[44] Awadhi EA, Salah K, Martin T, “Assessing the security of the cloud environment”, *GCC conference and exhibition (GCC)*, 7th. Doha: IEEE, page. 251, 2013.

[45] Grance T., Jansen W., “Guidelines on security and privacy in public cloud computing”. *NIST*, 2011.

- [46] Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR., "Security issues in cloud environments: a survey". *Int J Inf Secur*, Vol.13, No.2, pp. 113–70, April 2014
- [47] Nanavati M, Colp P, Aiello B, Warfield A. 2014. "Cloud security: a gathering storm". *Commun ACM*, Vol.57, No.5, pp. 70–9., 2014
- [48] Deshmukh RV, Devadkar KK, "Understanding DDos attack & its effect in cloud environment", *Procedia Computer Science*, Vol. 49, pp.202–10, 2015
- [49] Kandias M., Virvilis N., Gritzalis D., "The insider threat in cloud computing". *Crit Inf Infrastruct Secur*, vol. 6983, pp. 93–103, 2013
- [50] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, " Cloud security: Emerging threats and current solutions", *Computers and Electrical Engineering*, page. 2, 2016
- [51] Nepal, Surya, et al. "DlaaS: Data integrity as a service in the cloud." *Cloud Computing (CLOUD), 2011 IEEE International Conference on*. IEEE, 2011.
- [52] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security" *VSRD International Journal of CS & IT*, Vol. 2 Issue 4, pp. 316-32, 2012.
- [53] Ronald L. Krutz and Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", *Wiley Publishing, Inc. Indianapolis*, Indiana 2010.
- [54] William S., "Cryptography and network security: principles and practice", *Prentice-Hall, Inc.*, pp. 23-50, 1998.
- [55] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", *International Journal of Computer Science and Network Security*, Vol.8 No.12, December 2008.
- [56] Gurpreet Singh, SupriyaKinger, "Integrating AES, DES, and 3-DES Encryption Algorithm for Enhanced Data Security" *International Journal of Scientific & Engineering Research*, volume 4, Issue 7, July-2013.
- [57] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", *2010 First International Conference On parallel, Distributed and Grid Computing*, 2010
- [58] K. Naik, D. S.L. Wei, "Software Implementation Strategies for Power-Conscious Systems," *Mobile Networks and Applications* – Vol.6, pp. 291-305, 2001.
- [59] S. Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," *University of Pittsburgh*, April 9, 2003. Retrieved October 1, 2008.
- [60] Eystein Mathisen, "Security challenges and solutions in cloud computing" *Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on*, IEEE, pp. 208-212. 2011.
- [61] Kuyoro S. O., Frank, I. and Oludele, "Cloud Computing Security Issues and Challenges", *International Journal*. pp. 247-253, 2011
- [62] Rani, A.M.G. and Marimuthu, "A Study on Cloud Security Issues and Challenges" *International Journal*, pp. 344-347, 2012

- [63] Ertaul, L., Singhal, S. and Saldamli, G. "Security Challenges in Cloud Computing", *California State University, East Bay Academic paper* [http://www.mcs.csueastbay.edu/~lertaul/Cloud% 20Security% 20CamREADY.pdf](http://www.mcs.csueastbay.edu/~lertaul/Cloud%20Security%20CamREADY.pdf) [online]. (Accessed on 7 Sept. 2019)
- [64] Xu Xiao-tao, Chen Zhe, Jiang Fei, Wang Hui-tao. "Research on Service-Oriented Cloud Computing Information Security Mechanism," *2016 2nd IEEE International Conference on Computer and Communications*, 2016.
- [65] Mahroosh Irfan, Muhammad Usman, Yan Zhuang, Simon Fong, "A Critical Review of Security Threats in Cloud Computing", *2015 3rd International Symposium on Computational and Business Intelligence*. pp. 106, 2015
- [66] Mary-Jane Sule, Maozhen Li, Gareth Taylor, "Trust Modeling in Cloud Computing", *2016 IEEE Symposium on Service-Oriented System Engineering*, page. 78, 2016.
- [67] C. Venish Raja*, K. Chitra, M. Jonafark, "A Survey on Mobile Cloud Computing", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. page. 2096, 2018.
- [68] Mainak Adhikari and Tarachand Amgoth, "Heuristic-based load-balancing algorithm for IaaS cloud", DOI: <https://doi.org/10.1016/j.future.2017.10.035> (Accessed on 9 sept.2019.)
- [69] Qazi Zia Ullah, Shahzad Hassan, and Gul Muhammad Khan, "Qazi Zia Ullah,1,2 Shahzad Hassan,1 and Gul Muhammad Khan3", *Hindawi Computational Intelligence and Neuroscience* Vol. 2017, Article ID 4873459, page. 1, 2017.
- [70] Abdulaziz Alshammari, Sulaiman Alhaidari, Ali Alharbi, Mohamed Zohdy, "Security Threats and Challenges in Cloud Computing" *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing*, page. 47, 2017.

Turnitin Originality Report Processed on: 12-Sep-2019 17:32 +06 ID: 1171361007 Word Count: 6598 Submitted: 1 A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms By Fuad Newaz Khan	
Similarity Index 20%	Similarity by Source Internet Sources: 9% Publications: 11% Student Papers: 15%

2% match (Internet from 05-Apr-2019) http://www.ijarcs.info/index.php/Ijarcs/article/download/2959/2942
2% match (publications) Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, "Cloud security: Emerging threats and current solutions", Computers & Electrical Engineering, 2017
2% match (publications) Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghhighi, Muzammil Hussain et al. "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service", Journal of Network and Computer Applications, 2016
2% match (student papers from 31-Mar-2018) Submitted to Daffodil International University on 2018-03-31
1% match (student papers from 20-Sep-2012) Submitted to University of Wolverhampton on 2012-09-20
1% match (Internet from 22-Jan-2018) http://shodhganga.inflibnet.ac.in/bitstream/10603/56270/12/12_chapter%202.pdf
1% match (Internet from 03-Jun-2019) https://medium.com/@robillo/cryptography-network-security-e061172979a6
1% match (Internet from 17-Feb-2019) http://www.iioab.org/7(5)_SCMDSA/IIOABJ_7(5)139-149.pdf
1% match (Internet from 01-Aug-2017) http://ijiset.com/vol2/v2s8/IJISSET_V2_I8_64.pdf
1% match (publications) Deepak R Bharadwaj, Anamika Bhattacharya, Manivannan Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution", 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2018
< 1% match (Internet from 06-Feb-2019) http://ijesrt.com/issues%20pdf%20file/Archive-2016/November-2016/73.pdf
< 1% match (publications) Carlos André Batista de Carvalho, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho et al. "State of the art and challenges of security SLA for cloud computing", Computers & Electrical Engineering, 2017
< 1% match (student papers from 20-Sep-2015) Submitted to Southern New Hampshire University - Distance Education on 2015-09-20
< 1% match (publications) F. Campanile, L. Coppolino, S. D'Antonio, L. Ley, G. Mazzeo, L. Romano, L. Scaglione, F. Tessoro, "Cloudifying Critical Applications: A Use Case from the Power Grid Domain", 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), 2017