Review Of Some Cryptographic Algorithms In Cloud Computing

Mawaddah Fouad Alharbi†, , Fahd Aldosari , Nawaf Fouad Alharbi
s43980131@st.uqu.edu.sa ,fmdosari@uqu.edu.sa , en_nawaf@hotmail.com
UQU Computer science and Engineering KSA , Makkah
†UQU Computer Science And Information System , Computer Engineering Department KSA, Makkah
1&2 Dpartment of Computer Science and Computer Engineering, La Trobe University, Australia

Abstract
Cloud computing is one of the most expanding technologies nowadays; it offers many benefits that make it more cost-effective and more reliable in the business. This paper highlights the various benefits of cloud computing and discusses different cryptography algorithms being used to secure communications in cloud computing environments. Moreover, this thesis aims to propose some improvements to enhance the security and safety of cloud computing technologies.
***Key words**: Cloud Computing, Cryptography, Symmetric Algorithms, Asymmetric Algorithms , Hybrid Encryption, Cloud Storage, and Security.*

1. Introduction

With the accelerated progress of the digital world and the increase of data being generated. The "cloud" term has appeared to facilitate the storage and processing of this data. Recently, information technology organizations start taking into consideration the importance of cloud computing as the most common concept in Internet-based services. Cloud computing can be defined as distributed computing connections over the network to provide the different services needed by the end-users. [4].

Data storage security is one of the most important field in cloud computing , in this paper we aims to provide a review and comprehensive study on Encryption/Decryption algorithms used in cloud data storage to enhance the performance and security .

2. Cloud computing concept

Cloud computing provides Internet-based services for sharing resources at a minimum cost. The National Institute of Standards and Technology (NIST) is a U.S. government entity that formally defines standards and metrics, defines cloud computing as " a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [2].
The NIST determines a cloud essential characteristics as following:

- **On-demand self-service:** Users can access the cloud services and resources as needed through an online control panel automatically without any interaction with the service provider.
- **Vast access**: Cloud Computing Provides the available capabilities over the network through different client platforms (e.g. phones, tablets, laptops).
- **Resource pooling:** The services provider's computing resources (applications, storage, processing, and network bandwidth) are pooled to serve different users when needed.
- **Measured service and management:** Cloud systems provide automated control and optimized resource use by monitoring, controlling, reporting, and providing transparency for both the provider and consumer of the utilized service.
- **Rapid and elastic services:** Cloud computing provides flexible and scalable services to be suitable for the users' needs. The cloud provides flexibility for software, resources, users and any other features to be added or deleted without confliction.
- The cloud computing services can be provided to customers in three different service models:
- **Software as a Service (SaaS):** This model provides access to multiple software applications and resources stored on a remote location using the internet web browser or an application interface.
- **Platform as a Service (PaaS):** This service model provides consumer all the capabilities to set up their application from scratch in the cloud and deploy it onto the cloud infrastructure using programming languages, libraries, tools and services that are supported by providers. In this model, the consumer does not have any control or management on the cloud infrastructure, they can only control the deployed applications and settings for the application-hosting environment. **Infrastructure as Service (IaaS):** This type of service allows users to access the infrastructure resources such as hardware resources, data storage, network resources, etc. As a service. For security purposes, the *IaaS* is presented as the bottom layer

Manuscript received September 5, 2021
Manuscript revised September 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.9.5

of the *SaaS* and PaaS as shown in figure1, if the *IaaS* layer is at risk of being attacked, it instantly affects the above layers because of their dependence upon the *IaaS* layer [5].

2.1 Deployment strategies of cloud computing models

The NIST defined four deployment strategies of the cloud model (public, private, hybrid, and community cloud). The infrastructure in public cloud computing is made available to the public and is owned by a cloud provider who is responsible for the data controlling and operations inside the cloud and is responsible for the cloud infrastructure. On the contrary in the private cloud, the private cloud infrastructure is operated only for a specific organization, it may be managed by this specific organization itself or via a third party, the Cloud Provider (CP) is responsible only for the infrastructure.

In hybrid cloud computing, the cloud infrastructure is the composition of two or more types of clouds for instance (public and private clouds). the last type is community cloud, the cloud infrastructure in this type of cloud is shared by different organizations that share some of the same concerns such as mission, security requirements, policy…etc. The infrastructure of this Type can be managed by the organizations or by another third party.[6]

2.2 Benefits of cloud computing

Recently, the cloud is widely used as it allows users convenient access to data and applications via the Internet without having to have the knowledge about the deployment and management of infrastructure or hardware, we summarize some cloud benefits in the following points:

• **Cost efficiency:** the most significant benefit of cloud computing is the cost-saving, the consumer does not need any physical hardware investments to utilize the cloud services, in addition to other different costs (such as maintenance employees) which is afforded by the cloud provider. Cloud computing also uses ‘pay as you use’ business model.

• **Scalability**: the consumers can rapidly expand their storage capacity or computing capabilities at any time to suit their needs.

• **Load balancing:** cloud computing provides load balancing to distribute the extravagant load on a specific server to other servers, this feature shows reliability.

• **Flexibility:** cloud computing offers accessibility to the latest applications at any time without the need to spend time and money on installations.

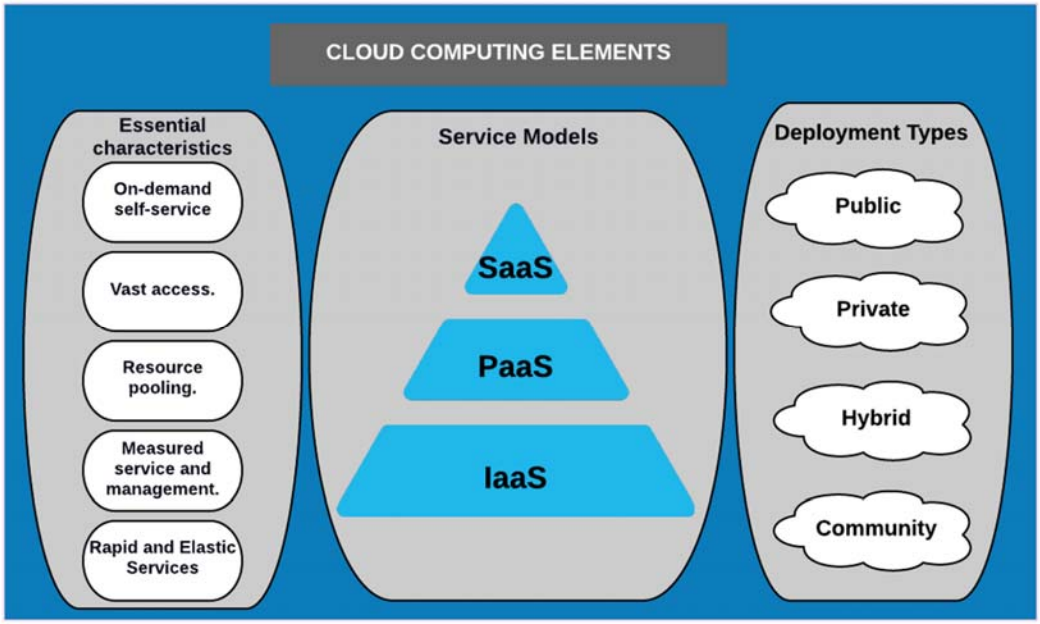

Figure 1 Cloud Computing Elements

• **Improved mobility:** the consumer can access the cloud via their smart phone or tablets easily.

• **Better resources utilization:** the cloud computing is considered as a trend and an inexpensive solution for different organizations to facilitate the access of remote information technology (it) resources by hosting their applications on the cloud. [3] it offers on-demand self-service, the resources can be utilized without any human interaction from the service provider side. Cloud computing facilitates information communication, getting services or applications from distant places using less hardware and/or software infrastructure. It helps reducing the need for complex hardware such as (a huge storage capacity) on the end-users. As a result, it helps to reduce the overall cost of physical equipment, by moving data and computing from the personal computers (pcs) into away large data centers where users can access applications as utilities and information, over the internet. [1].

3. Security challenges in cloud computing

Despite many benefits of cloud computing, but it has an enormous number of security problems and risks such as attacks, malicious insiders, data theft or loss, cloning and added security challenges related to virtualization, etc.

Cloud computing poses an extra level of risk because of the critical services offered by it to a third party, which makes it hard to uphold data privacy and security. There are a lot of threats and challenges which may affect cloud security so cloud providers, brokers, and consumers must take in their account the importance of cloud safety [16][17]. Extensive efforts are made by cloud providers (CP) to keep services and systems secure from threats and attacks and keeps data integrity and confidentiality [1]. As various economics is joined to cloud computing it will be preferable to resolve the challenges and issues as early as possible.

In August 2019, the cloud security alliance (CSA) which is a nonprofit organization defined standards, certifications to help guarantee a secure cloud environment, CSA identified the top threats in cloud computing as the following in figure 2:

Cloud computing must achieve the following security requirements to protect its customers and help them to achieve their objectives. The security requirements are [6]:

- **Data Confidentiality:** the cloud must assure that private information didn't detected by the unauthorized users, it must keep Confidential.
- **Privacy:** the cloud must ensure that users control or effect on the information related to them , and it collected and stored only by them or by whom allowed by them .
- **Integrity:** cloud computing must ensure the integrity of the data when (transfer, storage, and retrieval) means that it changes only using authorized transactions without any manipulation from unauthorized transaction by the system users.

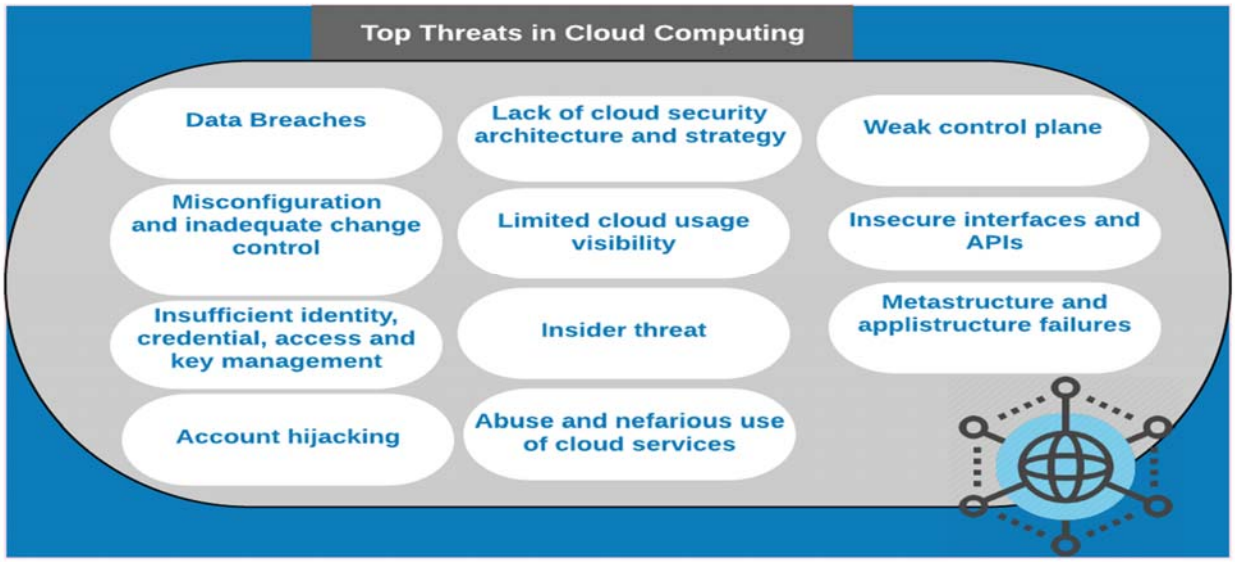

Figure 2: The top Threats in Cloud Computing

• **Availability:** ensure that cloud work immediately and service is not denied to authorized users.

4. Cryptography Algorithms In Cloud Computing

Cloud computing is utilized widely in the various fields of life on a personal use, health, commercial and governmental, all these huge data in cloud storage need to be safe from any unauthorized manipulation, here the important role of cryptography comes to preserve data integrity and confidentiality. Cryptographic algorithms offer the secure communication medium to transfer data reliably, so when malicious users try to hack data, they wouldn't get useful data, because the data is in encrypted form.
Cryptography is derived from the Greek word: “cryptos” which means “secret” and “graphein” which means “writing”[18]. it is the study of art and science of preparing protected and secure data communication, it is essential when there is a need to secure some critical and confidential data. [6][18].
While cloud is a multi-tenant system using cryptography to ensure more privacy and security for users. Therefore, the ability to encrypt cloud storage gives consumers the power to restore personal privacy. Cryptography is the study of art and science of preparing protected and secure data communication , which it makes **encrypted** information [6]. Encryption is said to be a better approach that helps to achieve data confidentiality in cloud systems, is the process of changing plaintext into ciphertext.

4.1 Some Basic Terms In Cryptography

• **Encryption :** is the process of encoding information by converting it from the original representation to the another representation to hide it from unauthorized users , this process done by using different Encryption algorithms.

• **Decryption :**it is the process of converting the Encrypted data to the original data ،It is the reverse process of encryption.

• **Algorithm or cipher**: It is a well-defined mathematical process that is followed in the encryption and decryption process, which will be detailed in the next section.

• **Plain Text:** it is the original message or text that Alice/sender wants to send to bob/receiver . the plain text can be (text , image , audio or video ,etc).

• **Cipher Text:** The encoded text that originates from the encryption process , it will be unreadable text.

• **Avalanche effect:** is used to define some precise property of the encryption algorithm. if a single bit or slightly change of plaintext gets altered then it should alteration multiple bits of a cipher text message or vice versa.

A good cryptography algorithm should always satisfy the following equation: Avalanche > 50% [18].

4.2 Cryptography algorithms types

In cloud services, there are several cryptographic algorithms used by different cloud providers, to ensure that the data are secure from the threats or attacks. They try to make these algorithms difficult as possible to decrypt using a long key which in turn makes the algorithms efficient and secure from cyberattacks [11].

Usually cryptographic systems rely on three dimensions [6] :

The type of encryption operation: all encryption/decryption algorithms are based on two general principles***: substitution and transposition***.

- **Substitution encryption:** this type of encryption mapped each element on plaintext (bit, letter or group of bits/letters) into element in the ciphertext.
- **Transposition encryption:** this type of encryption depends on rearranging the plaintext elements.
-

The number of keys used in encryption operation: dependence of number of keys used in encryption algorithms, the encryption/decryption process consists of two algorithms models:

- **Symmetric-key algorithm model:** when both sender and receiver use the same key.
- **Asymmetric key algorithm model:** when the sender and receiver use different keys, the system will be asymmetric, public-key encryption.

How the plaintext is processed, either block cipher or stream cipher:

- **Block cipher:** this type of encryption producing an output block for each input block, the encryption processes done for each block separately.
- **Stream cipher:** this type of encryption processes the input elements continuously, producing output one element at a time.

o Data can be encrypted using ***hybrid algorithms*** that combining both symmetric key and

asymmetric key techniques, but the major problem of these approaches is how to create, access, store and exchange a secure secret key [10].

4.2.1 Symmetric Key Cryptography algorithms

Symmetric algorithms use a single shared secret key in encryption / decryption processes, Symmetric algorithms use a single shared secret key in encryption / decryption processes, So, the secret key must be kept securely, because if anyone gets the key then he can easily decryption other ciphertext to get the plaintext and change it[18] .
Symmetric algorithms has the capability to process a large amount of data without much power consumption, as well as has a lower overhead on the systems, has a high speed during encryption / decryption processes. Symmetric algorithms encrypt plaintexts as stream ciphers bit by bit, or as block ciphers on a fixed number of 64-bit units [8].

4.2.2 Asymmetric algorithms

Asymmetric algorithms have a pair of related keys, One key called the public key used for encryption, and a different private key used for decryption. The keys distributed between users based on authorization Property , the public key is used by all users to decrypt the information from the encrypted data, but the private key is known only by authorized users to decrypt the cipher text.

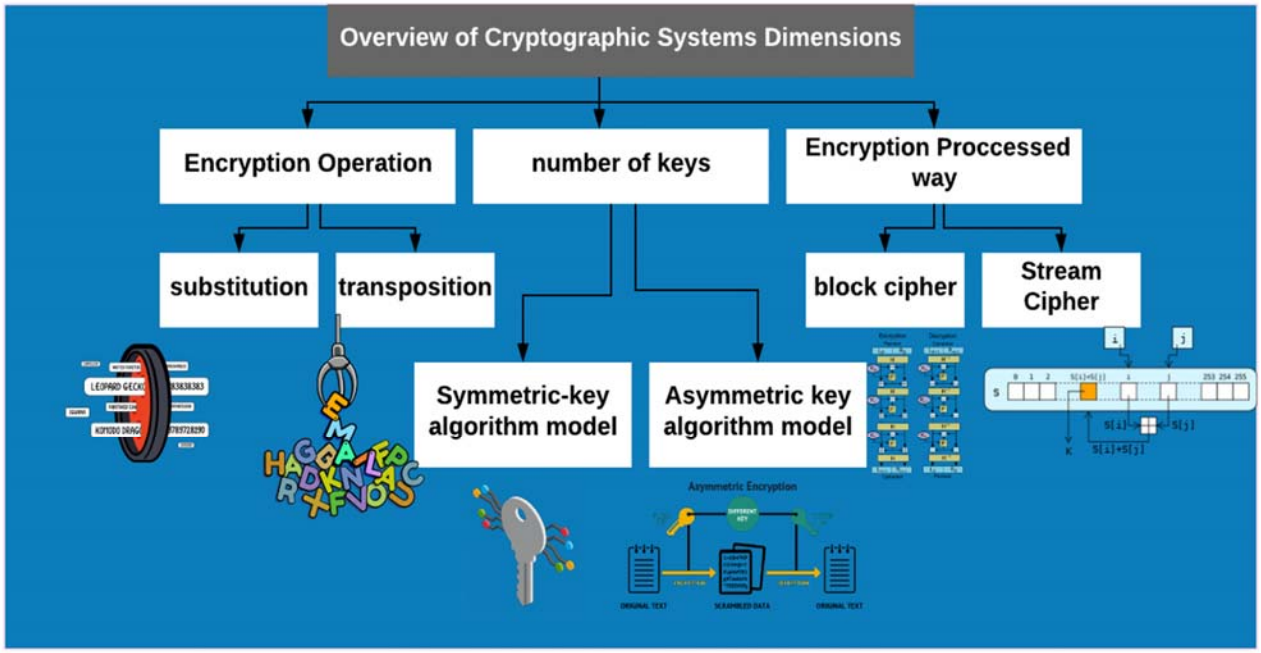

Figure 1: overview of Cryptography system dimension

4.2.3 Hybrid algorithms

With the advancement in computer and information technology, security has become more important than before. Therefore, the hybrid method appeared, as the use of more than one encryption algorithm at the same time contributes to enhancing data security. Hybrid cryptography strategy includes the combination of both symmetric/ asymmetric algorithm .

5. Literature review

In this section of the research, we highlight previous studies in Previous recent years since 2016 to give an overview of the state of art in the field of security in cloud computing.
In [8] the authors provided a summarized review of symmetric and asymmetric algorithms with an focusing on symmetric algorithms for security consideration to asset to choose the best algorithms to be used for cloud-based services.
they compared different algorithms to choose the right scheme to be used in the cloud computing environment and achieve end-user data security While maintaining the cloud performance, they concluded to that , the algorithm that

might be taking a long time to run would prove to be useless in the cloud environment. also they concluded that the using RSA and AES Encryption algorithms helps to enhance and increase the data security for cloud-based applications also they found that , AES is a good candidate for key encryption and md5 being faster when encoding.

In[9] the securing of data sharing, data storage and data transformation for a huge data set are one of the essential issues for cloud computing, this article proposed a framework aimed to secure architecture for cloud computing layered architecture to overcome the security problem over different layers of cloud computing where data is processed and provided a comprehensive study of related algorithms. The algorithms they proposed works on three basic steps (stage1: user identification and verification using the biometric technique, stage2: secure data upload using ERSA and SHA3, stage3: Secure data transmission use 3DES). The proposed architecture is design for all types of deployment models (public cloud, private cloud, and hybrid cloud.(

In[10]the authors worked on a simple data protection framework that performed authentication, verification, and encrypts data transfer and thus maintains data confidentiality. They compared the performance of different security algorithms (AES, RSA, and MD5), for ensuring the security framework. The experimental evaluation is done on the different input sizes between 2KB and 50 KB. The analysis result concluded that the asymmetric encryption algorithms are slower than symmetric encryption algorithms. RSA run time varies with the size of the input and it consumes the longest memory size and found out that AES and MD5 algorithm uses the least time and low memory usage in comparison to RSA.

In [11] they tried combinations of (AES, RSA, DES, IDEA)encryption algorithms for ensuring the security of data stored in the cloud and evaluating their performance in multi-stage encryption.

Their assumption is data is safe at the client's place.

For multi-stage encryption they used RSA to generates (public and private) keys. The RSA uses a key of 1024 bit . They Examining three mixing of algorithms to encrypt the data:

- The first one: a mix of RSA with AES.
- The second is a Mix of RSA with DES.
- The last is a mix of RSA with IDEA.

Then they evaluated their performance and encryption time. In all three mixings, they used RSA for the Personnel domain and the other algorithms for the public domain.

The performance results are very high for the combination of RSA+ IDEA, it gives higher performance than other combinations.

This paper [12] focused on how to analyze and evaluate the most important security encryption algorithms for data protection in cloud computing, they compared two Symmetric key Encryption algorithms (AES and Blowfish), The performance metrics are analyzed in MATLAB upon consideration of two basic parameters which are (a) Time for encryption and decryption, (b) Time taken by CPU processor. Finally, it is concluded that the Blowfish is higher throughput, speed, and less power consumption it is the optimized one among all available algorithms.

Data privacy and security are the two main aspects of the user's concern in cloud information technology.

This paper [13] discussed and compared the performances for some existing security techniques used to provide security in the field of cloud computing based on different parameters aimed to enhance the security of data storage in a cloud environment and proposed a novel security algorithm.

Performance and analysis measurements have been utilized in the Amazon EC2 environment. Optimizations, tuning the benchmarks process were compiled using JAVA command-line arguments. The security algorithms are evaluated in terms of the execution time required to store or retrieve the text data at the cloud, it depends upon Encryption and Decryption time as parameters. The result of the experimental ECDSA is best for other algorithms such as RSA, ECC, and ECDH. They proposed the future scope of the work is to find out an efficient proposed novel algorithm to make them more secure than ECDSA.

User's data security and privacy in cloud computing technology is the utmost dangerous issues because data owner stores their sensitive data onto remote cloud storage. However, successful retrieval of confidential data and computation on confidential data is hard to succeed by a traditional cryptographic algorithm .

In this[14], a Homomorphic cryptographic algorithm is one such technique that has interested homomorphic cryptographic algorithm used to secure user data in cloud s e r v e r. The experts who worked on this article performed computation on ciphertext data that can be operated directly without affecting the confidentiality of the encryption algorithms. They have established a framework for the security of data on cloud storage by using a fully homomorphic cryptographic algorithm. They evaluated the complexity of three homomorphic cryptographic algorithms those are SDC FHE, Paillier, and RSA with encryption time, decryption time, throughput, and memory usage.

The results show that the SDC FHE algorithm better at encryption time and decryption time compared with Pallier and RSA algorithm for given different file size, especially when the file size is increasing the change is growing fast.

The results concluded that the SDC FHE encryption/decryption algorithm has a better performance based on execution speed relative to the other homomorphic cryptographic algorithms. Also, SDC FHE has the highest throughput for a given user is measured by dividing the total ciphertext in binary and total decryption time in each

algorithm. Memory utilization of algorithm based on the variable used in encryption and decryption times with a different file load. By analyzing the memory required for the implementation of SDC FHE, RSA, and Paillier based on given data in bytes. So, SDC FHE is a better option in a case where less memory is required than either Paillier and RSA memory utilization. And as the file size increases the memory size is drastically increased in each cryptographic algorithm .They concluded that FHE is the greatest solution to secure the user data in cloud storage because it enables to perform the additive and multiplicative operations on encrypted data deprived of decrypting user's information on cloud servers .

They recommended for future research work to find a solution to reduce the length of public and private keys because they were Large and the Large key handling is problematic on the cryptographic algorithm .In [15] and [16] some discussion of the issues and challenges that affect cloud security with some suggestions which can be used for better performance of cloud services are given. Data protection and privacy are the most crucial factors among all other factors. So, if appropriate solutions are not being provided, the adoption of the cloud environment becomes more difficult .

This research [17] provided a framework for enhanced security and owner's data privacy in cloud computing. They were modified the 128 AES algorithm aimed to increase the speed of the encryption process, 1000 blocks per second, by the double round key feature were comparing the AES and the proposed Improvement AES using Various parameters such as encryption, decryption, energy consumption, network usage, network delay, trusted devices, and service management devices are compared. The same algorithms are implemented in real-time applications. The results of their framework concluded to minimizes energy consumption by 14.43%, network usage by 11.53%, and delay by 15.67%. Hence, the proposed framework enhances security, minimizes resource utilization, and reduces delay while deploying services of computational clouds.

5.1 Comparison

source	Cryptographic Algorithms	Type of cryptography	Comparison parameters	Environment	results
Security algorithms for cloud computing	RSA	Asymmetric	File size Encryption and Decryption time	Infrastructure for data gathering : Connectivity : 1Mbps WAN circuit link connected to public cloud server provider. Cloud simulation : Hosted web application server in the IaaS systems. Programming language : java.	Data security for cloud based application can be Increased by using RSA And AES Encryption Algorithms. By using keys as 1024 bit RSA and 128 bit AES , the attacker can't determine the private key even if he has the public keys generated. AES is good candidate for key encryption MD5 giving the faster performance through the Encoding
	AES 3DES	Symmetric			
	MD5	cryptographic hash algorithm.			
Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithms	ERSA, SHA, 3DES	Hybrid encryption algorithm (Symmetric , Asymmetric).	SHA and ERSA used for secure data upload process. 3 DES cryptography algorithms for	(not provided)	ERSA provides greater security as compared to RSA. SHA3: most widely used version of SHA series . 3DES offers more security benefits as

			secure data transmission		compared to simple DES. Provide security for all type of deployment models (public cloud, private cloud, and hybrid cloud).
A Comprehensive Evaluation of Cryptographic Algorithms in Cloud Computing	AES RSA MD5	Symmetric Algorithms Asymmetric Algorithms Hashing algorithms	Encryption time Decryption time Memory usage Speed Up Ratio	MATLAB2014 version IDE tool and JDK 1.7.	the asymmetric encryption algorithms are slower than symmetric encryption algorithms. the highest speed is achieved in the AES. AES and MD5 algorithm uses the least time and low memory usage in comparison of RSA.
Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for Securing Data in Cloud	RSA+AES RSA+DES RSA + IDEA.	Hybrid Encryption system	Performance	(not provided)	High Medium Very high
Implementation of Encryption Algorithm for Data Security in Cloud Computing	AES BLOWFISH	Symmetric Key - Encryption	Time for encryption and decryption. Time taken by CPU	Java runtime environment of Google App Engine, i.e. JDK 1.6. Eclipse IDE, Google App Engine SDK 1.6.0 or higher	The results the Blowfish is the optimized one among all available algorithms.
TIME COMPLEXITY ANALYSIS OF RSA AND ECC BASED SECURITY ALGORITHMS IN CLOUD DATA	ECC, RSA, ECDH ECDSA	Asymmetric Key algorithms key agreement protocol Digital Signature Algorithm (DSA)	execution time (Encryption and Decryption time)	Amazon EC2 environment. And using JAVA command-line arguments.	the result of the experimental the ECDSA is best for the other algorithms such as RSA,ECC and ECDH
Performance Analysis of Homomorphic Cryptosystem on Data Security in Cloud Computing	SDC FHE Paillier RSA	Asymmetric key Algorithms	encryption time. decryption time. Throughput memory usage	Not provided	the results concluded that : The SDC FHE encryption/decryption algorithm has a better performance based on execution speed relative to the other homomorphic

					cryptographic algorithms. FHE is the greatest solution to secure the user data in cloud storage
Secure Framework Enhancing AES Algorithm in Cloud Computing	(Enhancing) AES	symmetric-key algorithm	energy consumption. network usage delay	The SFCC is developed using CloudSim and iFogSim simulators on the Eclipse integrated development environment. Libraries used are JavaScript object notation (Json) data saver, common math, and JfreeChart.	the proposed framework enhances security, minimizes resource utilization, and reduces delay while deploying services of computational clouds.

6. Discussion and conclusion

All the reviewed research dependent on two or three measuring metrics of cryptographic algorithms, the most important one of them is Encryption/ decryption time, these metrics not enough to judge if the algorithm is the best one or not.in [8] and [10] they compared the same three algorithms (RSA, AES, and MD5) and using different metrics They agreed that RSA slower than AES and MD5 but [10] using memory usage as an additional measuring to prove that AES better than RSA.in [12] they compared AES and Blowfish using three measuring metrics (Encryption time, decryption time, and CPU time) their results show that the Blowfish is better than AES but they used limited measuring metrics they not measuring memory usage, energy consumption, and throughput all these metrics effect on algorithms qualities.

In [17] they proposed Secure Framework Enhancing AES to Use it in cloud computing and they compared between the old version of AES and Enhancing one, the new version optimizes the delay and minimizes resource utilization but these new results are not compared with Blowfish Algorithms, so from [12] and [17] we can't judge if blowfish better than AES.

in [9] they proposed Secure Data Transference Architecture for Cloud Computing using Hybrid encryption algorithms to use in cloud computing they were not measuring the performance of these algorithms they only measuring the security, and They did not mention the environment used in the experiment.

in [11] they measured the Performance of various Hybrid Encryption systems (RSA+AES, RSA+DES, and RSA + IDEA), and the candidate an (RSA + IDEA) as higher performance but they also did not mention the environment used in the experiment.

in [13] they compared between RSA AND ECC in cloud data and using execution time (Encryption and Decryption time) as measurements and they concluded to ECDSA is the best for the other algorithms so based on [11]and [13] we can use ECDSA + IDEA instead of RSA then can measure the performance again.

In [14] they measured the Performance Analysis of Homomorphic Cryptosystem using different measurement parameters (encryption time. , decryption time. , Throughput and memory usage) and they found that The SDC FHE encryption/decryption algorithm has better performance, based on their results, [11] and [13] we can compare SDC +IDEA instead of RSA then can measure the performance again and compare it with each other. the [14] are didn't mention the environment used in the experiment.

Based on these studies we proposed to test the algorithms using more performance indicators such as encryption time, decryption time, throughput of encryption, throughput of decryption, diffusion analysis, CPU process time, and CPU clock cycles, power consumption and memory utilization to improve the performance of these algorithms.

7. Future Work

Based on all previewed papers results , we proposed to compared between two secured system consist of two hybrid Encryption /decryption algorithm , the first system depend on (ECDSA + IDEA) algorithms and second one depends on (SDC + IDEA) based on

performance (encryption time, decryption time) . We will use Cloudsim as Experiments Environment , It helps to test , develop , tune-up and evaluate potential solutions , we can run it using eclipse IDE , and java programming language.

8. References

[1] H. Khan and M. Ahamad, "Security Challenges and Threats in Cloud Computing Systems", *International Journal of Advanced Research in Computer Science*, vol. 8, no. 2, pp. 36-39, 2017.

[2] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing" in Special Publication 800-145 (Sept, 2011) .

[3] S. Jagirdar, K. Reddy and D. Qyser, "CLOUD COMPUTING BASICS", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 5, pp. 343-347, 2012.

[4] M. Alassafi, A. Alharthi, R. Walters and G. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies", *Telematics and Informatics*, vol. 34, no. 7, pp. 996-1010, 2017.

[5] N. Thakkar, M. Karamta, S. Joshi and M. Potdar, "Enhancement of Cloud Security Using Snort", *International Journal of Distributed and Cloud Computing*, vol. 7, no. 1, pp. 25-29, 2019.

[6] W. Stallings, *Cryptography and Network Security*, 7th ed. Harlow, United Kingdom: Pearson Education Limited, 2017, pp. 519-544.

[7] "CSA Releases New Research - Top Threats to | Cloud Security Alliance", *Cloud Security Alliance*, 2019.

[8]. Bhardwaj, A., Subrahmanyam, G., Avasthi, V. and Sastry, H., 2016. Security Algorithms for Cloud Computing. *Procedia Computer Science*, 85, pp.535-542.

[9] Khari, M, Kumar, M & Vaishali 2016, 'Secure data transference architecture for cloud computing using cryptography algorithms', *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 2141–2146, viewed 1 December 2020, <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=edseee&AN=edseee.7724644&site=eds-live>.

[10] Kulshrestha, V., Verma, S. and Challa, C. R. K. (2016) 'A comprehensive evaluation of cryptographic algorithms in cloud computing', *2016 International Conference on Inventive Computation Technologies (ICICT), Inventive Computation Technologies (ICICT), International Conference on*, 1, pp. 1–5. doi: 10.1109/INVENTIVE.2016.7823268.

[11] Chennam, K. K., Muddana, L. and Aluvalu, R. K. (2017) 'Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud', *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on*, pp. 2030–2033. doi: 10.1109/RTEICT.2017.8256955.

[12] Shaik, K., kumar, N. S. and Narayana Rao, T. V. (2017) 'Implementation of Encryption Algorithm for Data Security in Cloud Computing', *International Journal of Advanced Research in Computer Science*, 8(3), pp. 579–583. Available at: http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=aci&AN=122961285&site=eds-live (Accessed: 1 December 2020).

[13] Pharkkavi, D. and Maruthanayagam, D. (2018) 'Time Complexity Analysis of Rsa and Ecc Based Security Algorithms in Cloud Data', *International Journal of Advanced Research in Computer Science*, 9(3), pp. 206–213. doi: 10.26483/ijarcs.v9i3.6104.

[14] Beyene, M. and Shekar, K. R. (2019) 'Performance Analysis of Homomorphic Cryptosystem on Data Security in Cloud Computing', *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Computing, Communication and Networking Technologies (ICCCNT), 2019 10th International Conference on*, pp. 1–7. doi: 10.1109/ICCCNT45670.2019.8944837.

[15] I. Ahmed, "A brief review: security issues in cloud computing and their solutions", *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, p. 2812, 2019.

[16] S. Mukherjee, "Cloud-based Security Solutions", *The IUP Journal of Computer Sciences*, vol., no. 4, p. 72, 2019.

[17] Awan, I. A. *et al.* (2020) 'Secure Framework Enhancing AES Algorithm in Cloud Computing', *Security & Communication Networks*, pp. 1–16. doi: 10.1155/2020/8863345.

[18] Verma, R. and Sharma, A. K. (2020) 'Simulation-Based Comparative Analysis of Symmetric Algorithms', International Journal of Advanced Research in Computer Science, 11(5), pp. 64–69. doi: 10.26483/ijarcs.v11i5.6655.