Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, July 2021: 5140-5154

Research Article

Enhancing Cloud Data Security using Multilevel Encryption Techniques

Najd Almoysheer [a], Mamoona Humayun [b], A. A. bd El-Aziz [b, c], NZ Jhanjhi [d,e]

Abstract

Cloud computing is the provision of IT services over the Internet with the aim of offering faster innovation, flexible resources, and economies of scale. Cloud computing security is in a continuous evolving, it is the one of the main research issues in Cloud. This paper proposes a multilevel encryption technique to secure the transaction of data in public cloud. The proposed technique model is a hybrid method that combines both the symmetric and asymmetric cryptography techniques. Our proposal uses use the Blowfish encryption to encrypt could data and Elliptic Curve Cryptography (ECC) to generate and manage encryption keys. Hence, it ensures a multilevel encryption /decryption process for both the sender and the receiver. Our work ensures Cloud security, transparency and reduces the security threats. Furthermore, we aim to propose multilevel cryptographic schema based on a combination of the Blowfish encryption and Elliptic curve cryptography. Our solution combines both encryption methods: a symmetric method using Blowfish to encrypt data and an asymmetric method using ECC to manage the encryption keys. Our proposition aims to ensure the security of delivered data in public SaaS and prevent non-authorized user to have access to the sensitive information exchanged between the client and the cloud server.

Keywords: Cloud Computing, Security, Multilevel, Encryption, ECC, Blowfich

1. Introduction

Data can be stored, processed, manipulated, and accessed thanks to Cloud computing (CC). Cloud computing ensures access and management of shared resources from a centralized point. This is possible because of its characteristics like resource pooling, broad access network, on-demand self-service, rapid elasticity and many more. Cloud computing refers to secure remote servers for accessing and storing data. The cloud makes it possible to access information anytime and through any medium. There is different model for CC depending on the provided services. Among these models, there is Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Privacy and security are major issues in the context of cloud computing for both service providers and clients. In the context of cloud services, the cloud provider is responsible for

[1] [a] College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[b] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka , KSA
[c] Department of IST, Cairo University, FGSSR, Egypt
[d] School of Computer Science and Engineering (SCE), Taylor's University, Malaysia
[e] Center for Smart Society 5.0 (CSS5), Faculty of Innovation and Technology (FIT), Taylor's University, Malaysia
401205537@ju.edu.sa, aaeldamarany@ ju.edu.sa , mahumayun@ju.edu.my, noorzaman.jhanjhi@taylors.edu.my

securing the underlying infrastructure, while the customer is responsible for securing the applications and data in the cloud. Several challenges confront the security of the cloud such as user access control, data separation, safe interface, and safely stored data which determines if the end-user or the cloud storage provider can manage encryption and decryption. As a solution, users need to be vigilant when they use the cloud to store their information. Besides, before the transmission of data to the cloud storage, it must be encrypted.

Cloud encryption is a commonly used solution for securing cloud data. This enables consumers and users to access shared cloud resources efficiently and securely, provided that all data are encrypted using different encryption methods and algorithms. According to authors in [1], the best way to ensure security in the cloud is the use of encryption algorithms. There are different algorithms for the cloud, among these the traditional and the most used ones are: Advanced Encryption Standard (AES) [2], Data Encryption Standard (DES) [3], RSA [4], and Message Digest 5 (MD5) [5]. In addition, there are more recent encryption algorithms such as Homographic encryption [6] and Blowfish cryptography (BE) [7]. A lot of researches have been conducted to prove the efficiency of each of these algorithms for cloud data security.

In this work, we aim to propose a multilevel cryptographic technique based on a combination of the Blowfish encryption and Elliptic curve cryptography. Our solution combines both encryption methods: a symmetric method using Blowfish to encrypt data and an asymmetric method using ECC to encrypt the keys. Our proposition aims to ensure the security of delivered data in public SaaS and prevent non-authorized users to have access to the sensitive information exchanged between client and cloud server. The objective of this work is to propose a strong cryptographic technique that will protect SaaS public cloud data integrity and confidentiality and prevent unauthorized access and security breaches by ensuring a strong authentication mechanism. The main contribution of this paper is as follows:

- Conducting in-depth analysis of existing cryptographic algorithm to identify the most effective ones.
- Providing a new multilevel encryption system that combine efficient encryption algorithm and methods.
- Proposing a hybrid security system based on the chosen algorithm to enhance data security in SaaS.
- Ensuring the security of data delivery between the client (application) and the cloud (server) in terms of integrity, privacy and confidentiality, hence only authorized user will get the access to the stored data on the cloud.

The rest of the paper is organized as follows; section 2 highlights the State of the art on cloud computing security. In Section 3, we present a background that introduces security issues and proposed solutions in Cloud Computing. The proposed technique is presented in section 4 and finally, section 5 concludes the paper.

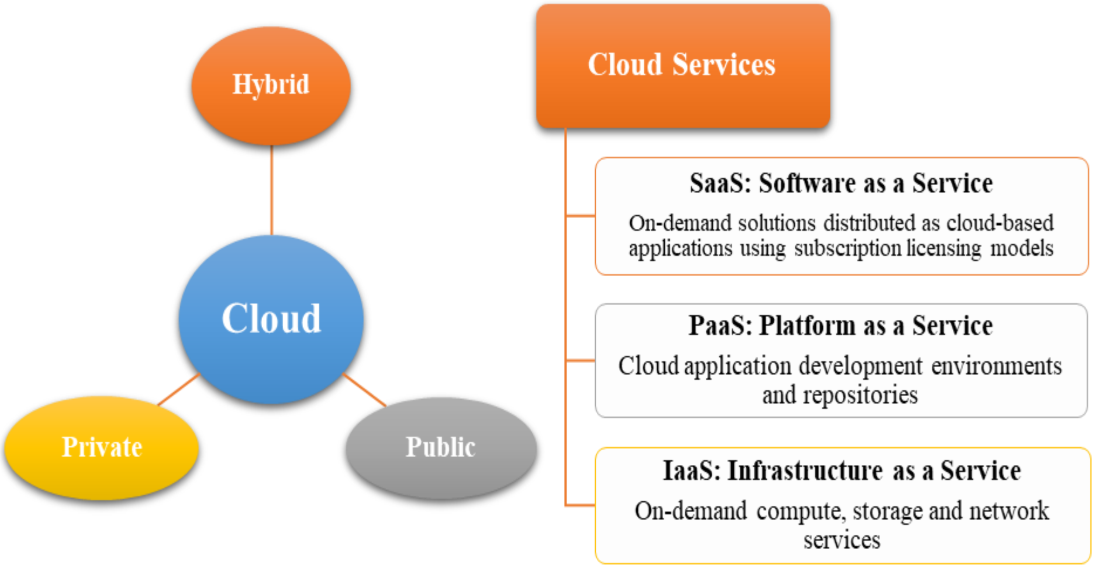
Hybrid
Cloud
Private
Public
Cloud Services
SaaS: Software as a Service
On-demand solutions distributed as cloud-based applications using subscription licensing models
PaaS: Platform as a Service
Cloud application development environments and repositories
IaaS: Infrastructure as a Service
On-demand compute, storage and network services

Figure 1 cloud deployments model and service types

2. State of Art

In this section, we review prior works that handled the problem of security in the Cloud. We study the security mechanism and approach proposed to secure the exchange of data between the client (application) and cloud (server) in SaaS, with emphasis on works based on hybrid approaches. Among the existing algorithms and encryption techniques, there is a growing number of researches that propose the combination of several techniques to benefits from their advantages. Namely, the study conducted in [8] proves the efficiency of applying various techniques of encryption. The authors explicated how hybrid systems and cryptographic algorithms can improve the security in Cloud. Multiple examples of hybrid systems can be found in the literature such as the combination of RSA algorithm with MD5 in [9], AES with MD5 [10], or the use of SSL over RSA [11]. Regarding RSA and AES, they are the most used encryption algorithms. However, according the comparative study conducted in [12], AES is most effective and more secure than RSA. AES encryption and decryption is faster and more secure than RSA, and RSA is vulnerable to brute force attacks.

AES was used in [13] to implement a security mechanism to secure the delivery of cloud data in SaaS, based on variable length keys. The authors proposed a cryptographic technique based on the key length as an input. This input is introduced by the user, who will also select the secret key according to the cryptographic system of AES, and finally select the chosen cloud data message. As a final step, the Cipher text will be generated and transmitted to the destination. On the inverse direction, the receiver will perform the reverse process using the same key. The authors used Python as a programming language to implement and validate their proposition. In addition, they conducted a comparative analysis with two existing approaches, where they assume that the proposed cryptographic technique can secure any transaction of cloud data messages. However, their analysis lacks the verification of the computational complexity of the proposed solution.

Another technique regarding encryption keys is presented in [14]. The authors propose to use AES to protect the exchange of data between the client and cloud. Their contribution differs in the fact that they have used Elliptic Curve Cryptography (ECC) to encrypt the AES encryption keys. Hence, they propose a multilevel encryption scheme that secure cloud data and ensure authentication. Thus, only successful authenticated users are able to access the cloud data. Using AES includes the use of a symmetric key to be used by both the client and the server to encrypt and decrypt data. Authors assume that proposition is safe and secure by guarantying the integrity and the confidentiality of data as well as the authentication ensure by the encryption of keys using ECC. However, in their analysis the authors only measured the execution time regarding the keys size, while file size is also quite important to prove the effectiveness of the schema. Additionally, the computational complexity was not considered.

More recent encryption algorithms have been proposed to secure the delivery of data for public cloud such as the work presented in [15]. The authors propose a hybrid system based on the blowfish encryption and RSA. They used Field-Programmable-Gate-Array (FPGA) to implement their cryptographic technique. Despite that this method is very effective because of low cost and high security, the main drawback is the large size of the key (448 bits) and the vulnerabilities inherited from RSA.

Another mechanism is proposed in [16], where authors combine the blowfish and the homographic cryptography. This approach aimed to enhance cloud security. Authors propose to encrypt the input text firstly using homographic encryption. Despite that homographic encryption security level is quite good, the execution time is very slow, hence, these techniques useful for in real-time applications.

More recent work has also used the Blowfish cryptography for the Cloud [17]. In this work authors propose a new security model that combines the blowfish algorithm with the clustering technique. Even taught clustering is not an encryption algorithm the K-method is used to cluster the secret information based on the measurement of data distance. Subsequently, this clustered data is encoded with Blowfish then stored in the cloud. Authors have proved that blowfish algorithm enhance cyber security accuracy for secret data compared to existing algorithms. Table 1summarizes the most important proposed approaches which we are relevant to our work.

Table 1. A comparison between related works proposed to secure Cloud computing

Work	Encryption technique	Used Approach	Advantage	Disadvantages
[13]	AES	Approach based on key length out put	Secure cloud data message transaction between the client and the server	No verification of computational complexity
[14]	AES+ECC	A multilevel schema where ECC is used to encrypt AES keys	Ensres authentication, confidentiality and integrity	No evaluation of execution time regarding file size
[15]	Blowfish + RSA	Use Field programmable gate	Ensure low cost and high security level	Large size of key and RSA related issues

		array for the implementation		
[16]	Blowfish + HA	Encrypt the input text firstly with HA then BE	Enhance cloud security (high security level)	Very slow execution time
[17]	Blowfish + clustering	Combine blowfish with clustering techniques (K-method)	Ensures high security level	High cost and complexity

3. Background

Cloud security includes the protection of application and data integrity hosted in the cloud. This term applies to all cloud deployment models: public cloud, private cloud, and hybrid cloud In addition to the deployment models, clouds can be classified according to the types of on-demand services and solutions: IaaS, PaaS, and SaaS (figure 1). In this work, the focus is given for SAAS models. Many different software companies advertise themselves as Software-As-A-Service (SAAS) or SAAS vendors. SAAS is a third-party application available over the internet with no physical connection to any device [18]. SAAS companies create the business software and take care of hosting and maintenance. This is means everything is available over the internet letting business access their application from any device with an internet connection. Nevertheless, there is a notable disadvantage for SaaS, as the organization must rely on outside vendors for the software, providers might experience services disruptions and pose unwanted services changes, or fall victim to a security breach [19, 20]. Thus, unfortunately whatever the delivery services model is, they are susceptible to a variety of security breaches performed by attackers. Therefore, ensuring security is a challenging concern to be taken into consideration in cloud environment.

3.1. Cloud security

Cloud security is a discipline of cybersecurity dedicated to securing IT systems in the Cloud. It aims in particular to preserve the privacy and security of data in infrastructures, applications and online platforms. Securing cloud services starts with knowing exactly what secure and what aspects of the system is need to be managed. While cloud-based models offer more convenience and permanent connectivity, they require new arrangements to ensure their security. The introduction of cloud technology has forced everyone to re-evaluate cybersecurity. Data and applications may flow between local and remote systems, and still be accessible over the Internet. This makes it more difficult to protect them than when it was simply a matter of preventing unwanted users from accessing your network. Cloud security basically consists of 5 categories as shown in figure 2. In this work we are interesting to securing data. Encryption is one of the most powerful tools available. Encryption scrambles data so that it can only be read by someone who has the encryption key. If data is lost or stolen, it will be unreadable and unusable [21].

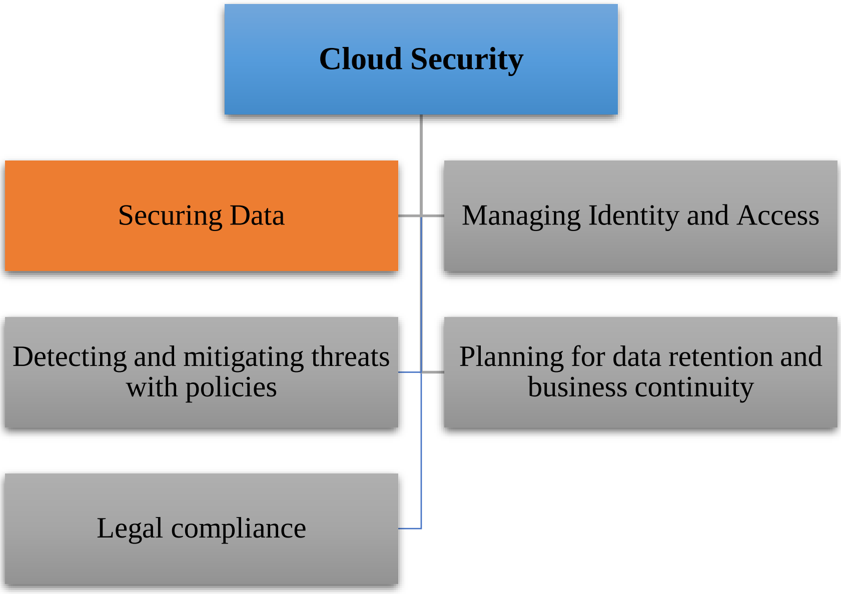
Cloud Security
Securing Data
Managing Identity and Access
Detecting and mitigating threats with policies
Planning for data retention and business continuity
Legal compliance

Figure 2 Cloud security categories

Cloud assets and workloads are exposed to a wide range of cybersecurity threats, including data breaches, ransomware, DDoS attacks, and phishing attacks. Cybercriminals can exploit security vulnerabilities in the cloud, using stolen credentials or compromised applications to launch attacks, disrupt services or steal sensitive data. The reliability of cloud security systems and practices is essential to maintain the availability of critical business applications, protect confidential information, and ensure regulatory compliance.

Cryptography is a broadly utilized strategy to protect the data of the public cloud. It permits customers to access the mutual cloud administrations effectively and dependably since all of the data is protected. Cryptography makes the plain text unreadable and limits the view of the data being transferred. Best cloud cryptographic techniques are encryption methods that do not compromise the speed of sensitive data transfer and their security. Encryption is a fundamental component in a defence-in-depth strategy, as it can mitigate weaknesses in primary access control mechanisms. If the data is encrypted by a strong key, as long as it is not on the same system as your data, it is impossible for an attacker to decrypt it. Encryption helps prevent confidential data from falling into the wrong hands. In other words, encryption preserves the confidentiality of sensitive data.

There are several different ways to use encryption, and they can be offered by a cloud service provider or by a separate cloud security provider as follow:

- Encryption of communications with the cloud in their entirety.
- Encryption of particularly sensitive data, such as account identifiers.
- Encryption End-to-end of all data that is uploaded to the cloud.

When using encryption, it is essential to manage encryption keys in a safe and secure manner. Consequently, there are three kinds of security processes: key generation, data encryption and data decryption. Hence, for the purpose of securing data, several encryptions algorithms where proposed as we will see in the next sub-section.

3.2.Cloud computing encryption Algorithms

Encryption algorithms have vital role in the field of cloud security. Many algorithms are available for cloud security. Most useful algorithms for cloud security are discussed below.

3.2.1 Data Encryption Standard (DES)

It is a symmetric key block cipher which uses unique secret key for the encryption and the decryption. DES operates on 64 bit data blocks and uses a 56 bits key. The round key size is 48 bits. AES divide the entire plaintext into 64 bit blocks, noting that the technique of padding is used when necessary.

3.2.2 Advanced Encryption Standard (AES)

It is the most adopted a symmetric key block cipher. AES computation is performed on bytes; hence it uses a 128 bits plaintext block as 16 bytes. AES uses boxes of 4 columns and 4 rows to arrange these 16 bytes as a matrix. AES process consists of substitutions and permutations operations. The transformation rounds number used for process of encryption is determined by the size of key used for an AES cipher.

3.2.3 Rivest-Shamir-Adleman (RSA)

RSA is the most commonly used asymmetric key algorithm, the size of both data blocks and keys is various. It uses asymmetric keys for encryption/decryption, private keys are used for encryption and public keys are used for decryption. To generate those keys, RSA uses two prime numbers; hence we can classify the process of RSA into 3 main phases: the generation of keys using prime numbers, encryption, and decryption.

3.2.4 Homomorphic Algorithm (HA)

Homomorphic encryption allows processing to be performed on data without having to decrypt it. It can be used with a cloud service, such as when a peer wants to do heavy processing on his database in a cloud service. First, it encrypts his database with a secret that only he knows about. It then sends its encrypted data to the cloud. The latter performs the processing on the encrypted data, generates the results also encrypted and sends them back to this peer. To find the clear results of the treatments carried out by the cloud, it will simply decrypt what the cloud service sent him. However, one of the big limits of this algorithm is that data integrity is not guaranteed because encrypted data is malleable.

3.2.5 Blowfish Encryption Algorithm (BE)

Blowfish is a symmetric encryption algorithm. The data block size used by this algorithm is 64 bits, thus messages which are not an eight multiple are cushioned. The process of this algorithm can be divided into two main stages: the expansion of key and the encryption of data encryption.

- Expansion of keys: in this stage there is the P-array which consists of eighteen boxes of 32 bits, and there are also the S-boxes, which contain four arrays of 32 bits with 256 entries each. The Key is transformed to several sub-key arrays, after the initialization of string:

- The initial 32 bits of the key are XORed with the first 32-bit box in the P-array
- The second 32 bits of the key is XORed with P2, etc until each of the 448.

- Data encryption: data s used with 64-bit plain text and divided into two 32 bits parts which will be is XORed with P cluster and the result is carried to the F function, as shown in figure 3.

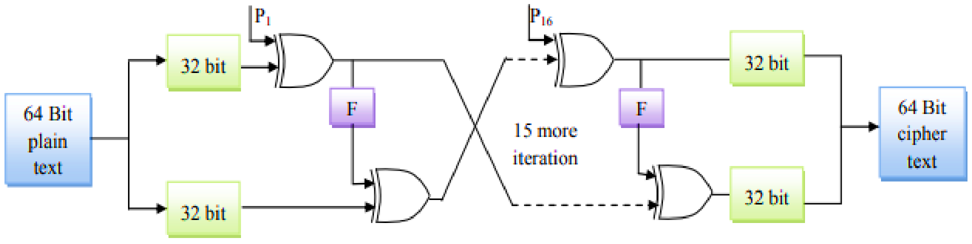

Figure 3 Blowfish Algorithm

The comparison of each of the encryption techniques discussed in this sub-section is presented in table 2.

Table 1. Encryption algorithms comparison

Encryption algorithm	Key type	Key size	Block size	Rapidity	security	limits
DES	Symmetric	56	64	Slow	inadequate	Not secure and slow
AES	Symmetric	128/192/256	128/192/256	Fast	Secure	Every block is always encrypted in the same way
RSA	Asymmetric	1024-4096	128	Very slow	Secure	very slow in cases where large data needs to be encrypted
HA	-	-	-	Fast	Secure	Integrity is not ensured
BE	Symmetric	32-448	64	fast	Secure	Weak keys problem

4. The proposed hybrid approach

In this chapter we present our proposed approach which consists of a multilevel encryption scheme for exchanged data between server and client in public SaaS model, it is primordial to preserve confidentiality before sending or outsourcing data in both directions from the cloud server to the client and vice versa[22-25]. Thus, unauthorized access by non-allowed user must be prevented to prohibit security threats coming from intruders. We propose for this aim a hybrid approach where data for uploading cloud server is encrypted by the Blowfish encryption algorithm to enhance the security and preserve data privacy. Moreover, for farther protection, keys used in the encryption process are handled and encrypted by ECC algorithm (figure 4). Our hybrid approach guarantees not only integrity and confidentiality but also provide authentication.

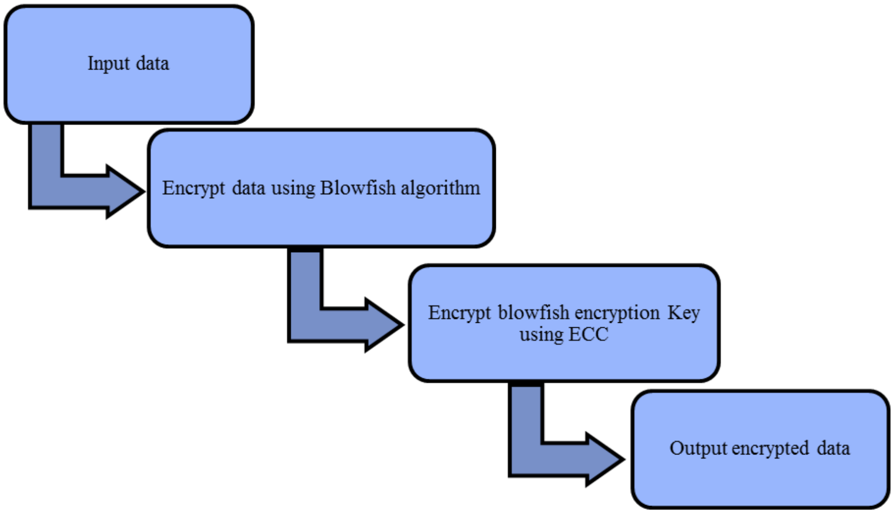
Input data
Encrypt data using Blowfish algorithm
Encrypt blowfish encryption Key using ECC
Output encrypted data

Figure 4 Flow diagram of the proposed system

Our proposed schema uses two types of cryptographic algorithms. We use blowfish encryption as a symmetric algorithm and ECC is used as an asymmetric algorithm. Hence, our hybrid approach combines the benefits of the two models of encryption. The symmetric method is blowfish encryption used to encrypt data before being stored in the cloud. Thus, the reverse process (decryption) is performed when outsourcing the data. The Asymmetric method is ECC, used to manage and encrypt the encryption keys.

4.1. Data uploading and downloading

The proposed method aim to protect data exchanged between server and client n SaaS. Thus, the process of encryption is performed on data to be uploaded by the client before sending it to the server. When downloading data, the reverse process is applied, hence, the client decrypts the downloaded data from the server to be able to use it (figure 5). The functioning of the system is as follows.

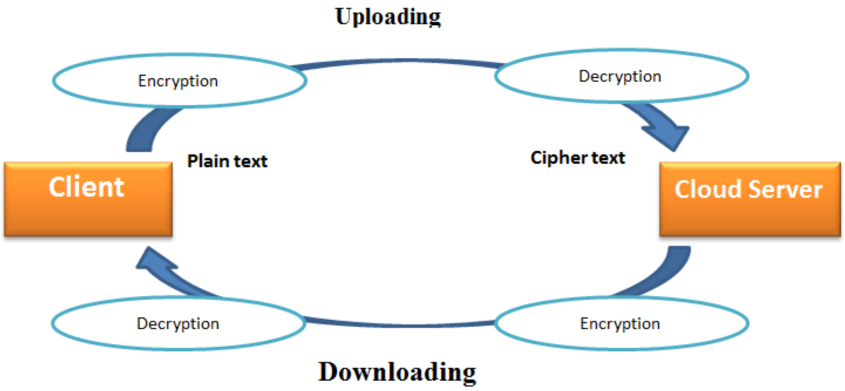

Figure 5 The process of Uploading /Downloading data

1. Uploading data

Before uploading data, it encrypted from plain text into cipher text using the blowfish encryption algorithm. Latter, the encryption key is encrypted with ECC algorithm. Finally, both the encrypted file and generated secret key are sent in cipher text to the cloud server.

2. Downloading data

When downloading data, the reverse process is performed. First the encryption key is decrypted using the ECC algorithm. Then, the generated key is used to decrypt data using blowfish decryption. Ultimately, the plain text is recovered. In this way, unauthorized users cannot use the file when it is secured in an appropriate way thus they cannot access it without decryption.

4.2. Data encryption using blowfish algorithm

The basic idea of the algorithm is ensuring the privacy of cloud data. Thus, data is encrypted before being uploading to the server. The proposed algorithm presents a multilevel encryption scheme. Before the upload of data to the cloud server, it must be encrypted by blowfish encryption. As discussed in the chapter 2, BL uses a 64 bit block size and has a variable key length from 32 bits up to 448 bits. For the key expansion or the initialization of keys, the variable key of the user is expended to sub key arrays of 4168 up to 8336 byte. In addition, four S boxes of 32 bits are used along with the P array which contains 18 sub-keys of 32 bits size. Noting that, those arrays generation process is user key dependent. Figure 6 present the key generation process for blowfish algorithm.

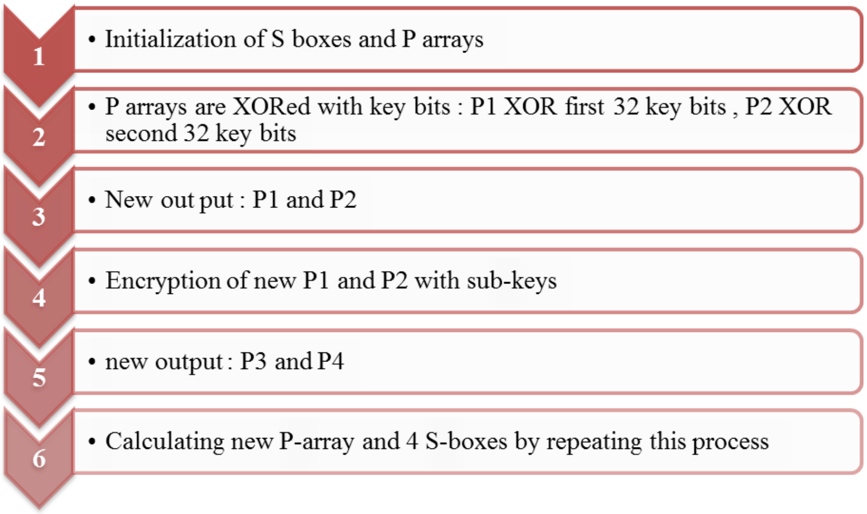
1
• Initialization of S boxes and P arrays
2
• P arrays are XORed with key bits : P1 XOR first 32 key bits , P2 XOR second 32 key bits
3
• New out put : P1 and P2
4
• Encryption of new P1 and P2 with sub-keys
5
• new output : P3 and P4
6
• Calculating new P-array and 4 S-boxes by repeating this process

Figure 6 key generation process for blowfish algorithm

For the encryption process, it is based on a simple repetition of Feistel Network functions 16 iterations. The input is a 64-bit data element X. Each round contains a set of permutation dependent on key along with a set of data substitutions. All operations are additions and XOR on 32-bit variables. Consequently, for each round r (till 16 rounds) the left half of data is XORed with p-array entry, then the XORed data is used as input for the function F of blowfish algorithm. The F function divides input into 4 quarters of 1 byte (A, B, C, and D), which are input to the S-boxes. For the output, they are ordered modulo 232 and XORed to generate an output of 32 bits. After

16th round, Left part (XL) is XORed with K16 and Right part (XR) with K17 without using last swap. Latter, the F-function output is XORed with right half of the data. Ultimately, the left and right half are swapped.

$$F\,(X_L) = ((S1, A + S2, B \bmod 232) \text{ XOR } S3, C) + S4, D \bmod 232$$

For the encryption process, the reverse process of encryption is applied. Thus, the reverse order of P1, to P18 is used.

Algorithm 1: Blowfish encryption process

S(): swapping function, C(): combining function, P: arrays

```
Input X : 64-bit
X is divided into two halves of 32 bits : $X_L$, $X_R$
For i= 1 to 16
    $X_L = X_L$ XOR Pi
    $X_R = F(X_L)$ XOR $X_R$
    $S(X_R, X_L)$
$X_R = X_R$ $XO_R$ P17
$X_L = X_L$ $XO_R$ P18
$C(X_R, X_L)$
End
```

4.3. Key encryption using ECC

ECC is a fast and strong cryptographic procedure for data security and public key cryptosystem. ECC offers a high level of security with short keys length. It can ensure the same level of security as RSA algorithm witch shorter keys and extra advantage such as low computational power. ECC algorithm generates keys using the Elliptic curve properties, as it an asymmetric technique it uses two key s: public key and private key. Hence, both encryption and signature verification are done with public key. However, the private key is used for decryption and signature generation. The General workflow of ECC is shown in Figure 7.

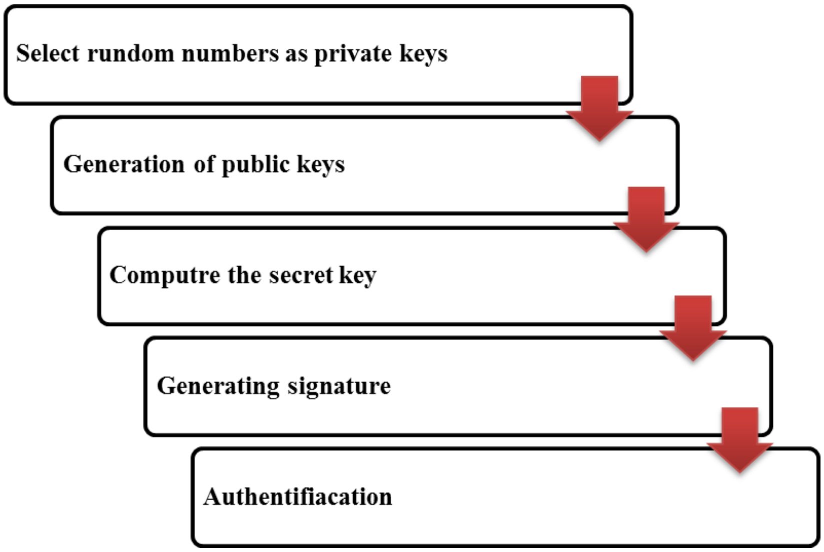
Select rundom numbers as private keys
Generation of public keys
Computre the secret key
Generating signature
Authentifiacation

Figure 7 The General workflow of ECC

The use of ECC reinforces the system security and ensures a strong authentication. Therefore, only authorized users (applications) that have been successfully authenticated will get to access the data stored on the cloud. In this way, the proposed system preserves data integrity and confidentiality.

4.4. The proposed algorithm

In this project we proposed an algorithm as a multilevel encryption system. It is a multilayer cryptography algorithm with Blowfish encryption in the first layer and ECC encryption in the second one. Blowfish encryption is first applied on the input text. Then the obtained encryption result is delivered to the second layer where Blowfish encryption keys are encrypted using ECC. The final output of encryption layer is obtained. The overall flow chart of the proposed algorithm is presented in figure 8.

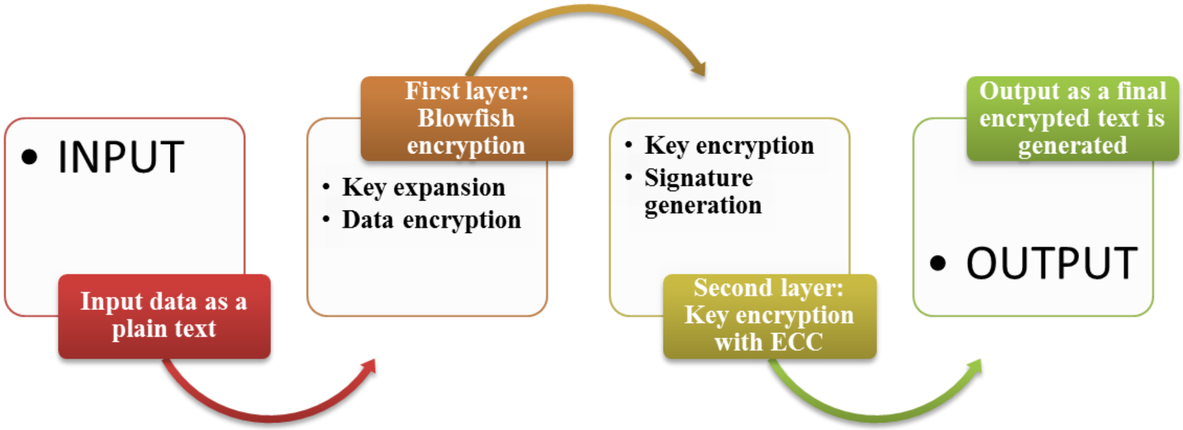
• INPUT
Input data as a plain text
First layer: Blowfish encryption
• Key expansion
• Data encryption
• Key encryption
• Signature generation
Second layer: Key encryption with ECC
Output as a final encrypted text is generated
• OUTPUT

Figure 8 the overall flowchart of the proposed algorithm

For the sake of understanding, we list some variable and some functions as Fb, E (b,k), P(F), Ek and Pk that has been used in the proposed algorithm such as

1. D : Input Data File
2. E: encrypted file
3. N is the number of block in D.
4. E (b,k) is the encryption function which encrypts the text block(b) with the key k using AES algorithm.
5. Function P (F) can allow encrypted file (Fe) to send in cloud server.
6. Ek function encrypts the AES key using ECC Algorithm.
7. Pk is the function which allow encrypted key (K1) generated by Ek in cloud server.

Noting that, we present the encryption algorithm only, as the decryption algorithm is just the reverse process of the encryption.

Proposed multilayer encryption Algorithm

```
Input text
Begin
For b= 1 to N
K= BLexp()
E= BLenc(D, K)
ECC (K)
S (k, E)
End
```

8. Conclusion

Cloud computing security is in a continuous evolving, it is the one of the main research issues in Cloud. our paper proposes a multilevel encryption technique to secure the transaction of data in public cloud. The proposed technique model is a hybrid method that combines both the symmetric and asymmetric cryptography techniques. we propose uses use the Blowfish encryption to encrypt could data and Elliptic Curve Cryptography (ECC) to generate and manage encryption keys. It is a quite important task to protect data stored on cloud. This protection can be offered using different encryption techniques. Several cryptographic algorithms are utilized often to achieve message confidentiality. In this work, we propose a multilevel technique that helps to raise the security level. Blowfish and ECC when used separately aid attaining security but only at some extent. However, the combination of the two ciphers together one after another aim to add layer of security. The proposed multilevel technique offers two level of encryption, which is more difficult to crack and so more secure. Variation may be done in this scheme as a future scope by adding more level of encryption and decryption. another algorithm can be suggested to be combined to be more powerful but it might be difficult to implement.

References (APA)

[1]Nasarul Islam KV, Mohamed Riyas KV (2017) Analysis of various encryption algorithms in cloud computing. Int J Comput Sci Mob Comput 6(7):90–97

[2]Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael. Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication, 112.

[3]Wiener, M. J. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information theory, 36(3), 553-558.

[4]Alayda, Sara, Najad A. Almowaysher, Mamoona Humayun, and N. Z. Jhanjhi. "A Novel Hybrid Approach for Access Control in Cloud Computing."

[5]Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption. In Homomorphic Encryption and Applications (pp. 27-46). Springer, Cham.

[6]Christina, L., & Joe Irudayaraj, V. S. (2014). Optimized Blowfish encryption technique. International Journal of Innovative Research in Computer and Communication Engineering, 2(7), 5009-5015.

[7]Bangar A, Shinde S (2014) Study and comparison of cryptographic methods for cloud security. Int J Comput Sci Eng Inf Technol Res 4(2):205–213

[8]Lenka SR, Nayak B (2014) Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int J Comput Sci Trends Technol 2(3):60–64 using

[9]Sidhu A, Mahajan R (2014) Enhancing security in cloud computing structure by hybrid encryption. Int J Recent Sci Res 5(1):128–132

[10]Mishra, Sambit Kumar, Sonali Mishra, Ahmed Alsayat, N. Z. Jhanjhi, Mamoona Humayun, Kshira Sagar Sahoo, and Ashish Kr Luhach. "Energy-aware task allocation for multi-cloud networks." IEEE Access 8 (2020): 178825-178834.

[11]Kannan, M., Priya, C., & VaishnaviSree, S. (2019). A comparative analysis of DES, AES and RSA crypt algorithms for network security in cloud computing. J Emerg Technol Innov Res (JETIR), 6(3), 574-582.

[12]Ghosh, P., Hasan, M. Z., Atik, S. T., & Jabiullah, M. I. (2019, December). A Variable Length Key Based Cryptographic Approach on Cloud Data. In 2019 International Conference on Information Technology (ICIT) (pp. 285-290). IEEE.

[13]Jana, B., Poray, J., Mandal, T., & Kule, M. (2017, November). A multilevel encryption technique in cloud security. In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 220-224). IEEE.

[14]Ali, Sadia, Yaser Hafeez, N. Z. Jhanjhi, Mamoona Humayun, Muhammad Imran, Anand Nayyar, Saurabh Singh, and In-Ho Ra. "Towards pattern-based change verification framework for cloud-enabled healthcare component-based." IEEE Access 8 (2020): 148007-148020.

[15]Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-10.

[16]Hussaini, S. (2020). Cyber Security in Cloud Using Blowfish Encryption. International Journal of Information Technology (IJIT), 6(5).

[17]Humayun, Mamoona. "Role of emerging IoT big data and cloud computing for real time application." Int. J. Adv. Comput. Sci. Appl. 11, no. 4 (2020): 1-13.

[18]Chung, Shen Ming et al. 2020. “UFETCH: A Unified Searchable Encryption Scheme and Its Saas-Native to Make DBMS Privacy-Preserving.” IEEE Access 8: 93894–906.

[19]DÍaz De León Guillén, Miguel Ángel, Víctor Morales-Rocha, and Luis Felipe Fernández Martínez. 2020. “A Systematic Review of Security Threats and Countermeasures in SaaS.” Journal of Computer Security 28(6): 635–53.

[20]Elsayed, Marwa, and Mohammad Zulkernine. 2019. “Offering Security Diagnosis as a Service for Cloud SaaS Applications.” Journal of Information Security and Applications 44: 32–48. https://doi.org/10.1016/j.jisa.2018.11.006.

[21]Kuciapski, Michał, Paweł Lustofin, and Piotr Soja. 2021. “Examining the Role of Trust and Risk in the Software-as-a-Service Adoption Decision.” Proceedings of the 54th Hawaii International Conference on System Sciences 0: 4693–4702.

[22]Paschal Uchenna, Chinedu. 2018. “Security of Cloud Virtualized Resource on a SaaS Encryption Solution.” Science Journal of Energy Engineering 6(1): 8.

[23]Prakash, J Purna, G Komala, and A Poorna Chandra Reddy. 2014. “Public Key Encryption Algorithms Enabling Efficiency Using SaaS in Cloud Computing.”

[24]Alayda, Sara, Najad A. Almowaysher, Mamoona Humayun, and N. Z. Jhanjhi. "A Novel Hybrid Approach for Access Control in Cloud Computing."

[25]D. A. Shafiq, N. Jhanjhi and A. Abdullah, "Proposing A Load Balancing Algorithm For The Optimization Of Cloud Computing Applications," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.