Cloud Application Security using Hybrid Encryption

Alabi Orobosade
Computer Science Department, School of Computing
The Federal University of Technology Akure, Nigeria

Thompson Aderonke Favour-Bethy
Cyber Security Department, School of Computing
The Federal University of Technology Akure, Nigeria

Alese Boniface Kayode
Cyber Security Department, School of Computing
The Federal University of Technology Akure, Nigeria

Arome J. Gabriel
Cyber Security Department, School of Computing
The Federal University of Technology Akure, Nigeria

ABSTRACT

The massive growth of sensitive information on cloud has made it more vulnerable. Thus, undeniably, the vulnerability shoots from the increasing number of users whose intentions are malicious. Since, the cloud is managed by a third party, ensuring cloud security services are of utmost importance, and coupled with the fact that cloud data and services resident in data centers are ubiquitous. The enlarged user surfing on the cloud for numerous purposes, therefore, necessitate a vastly safe and secured data. Consequent upon the highlighted points and providing a secure environment, this paper proposes a hybrid encryption algorithm comprising symmetric and asymmetric cryptography schemes suitable as state-of-the-art safeguarding users' privacy and security in the cloud. We propose a privacy model using Advanced Encryption Standard (AES) as a first level data encryption scheme prior cloud application data storage, while Elliptic Curve Cryptography (ECC) is the subsequent encryption scheme with AES key to achieve our aim of data confidentiality as well as is security in the cloud.

General Terms

Cloud Computing, Cryptography and Security

Keywords

Hybrid Encryption, Advanced Encryption Standard, Elliptic Curve Cryptography

1. INTRODUCTION

Cloud refers to the synergy of available computing power across the Internet. Cloud computing (CC), as clearly stated by the National Institute of Standard and Technology (NIST) is a prototypical environment characterized by a suitable, pervasive, on-demand network access to a shared robust configurable computing resources available for lease at a very reduced management as well little interference from the providers. Some of required resources are networks, servers, storage, applications and services. The flexible in addition to dynamic framework of CC provides a scalable information technology capacity in services as delivered over the Internet users. [1]

There has been a rapid development in technologies which has increased the number of service providers and customers adopting cloud environment. Cloud computing, In Buyya et al. [2] was referred 'the fifth utility', in addition to water, electricity, telephone and, gas as the readily available on-demand computing services over the internet, in today's human society. It has been generally accepted and been used in governance; e-commerce platforms as well military to ensure network connectivity with unbroken availability. This comes along with the Cloud Service Provider (CSP) providing and maintaining the required database and its application remotely; it allows the independent ubiquitous access via a network. Cloud service categories are emerging, the top-three is: software-as-a-service (SaaS), platform-as-a service (PaaS) and infrastructure-as-a-service (IaaS).

Although, CC takes numerous advantages over the traditional data storage; data security has been the consumers' blight to adopting its full services owing to the fact that most cloud service are managed by a third party. This has raised several data storage concern, because users' impression on the exact data location or other data types stored along their data are vague. However, inspite of users' agitation, since CC emergence, established firms such as IBM, Google, Yahoo, eBay, Amazon have invested and continue to invests significantly into CC and its infrastructure; large numbers of users including Governments of various nations, share big data from different locations across the globe with high speed. to enhance their respective services to clients and citizens at large. Therefore, ensuring data security, privacy, integrity and availability to cloud user with currently deployed approaches seem insufficient to attain end users' data security. Encryption scheme will be required to guarantee privacy preservation on users' data in transit or persistent state. In order to ensure the cloud data security, a hybrid encryption algorithm which involves using two crypto-schemes: a symmetric Advanced Encryption Standard (AES) and an asymmetric algorithm Elliptic Curve Cryptography (ECC). Using a symmetric algorithm otherwise known as private key cryptography with a single key for encryption and decryption coupled with an asymmetric algorithm (that is, public-key cryptography (PKC)) to enhance the cloud data security as required for the best practices. The symmetric key encryption is of great advantages in term of speed, and computation time however public key encryption has better key management than private key encryption. Public-key cryptography was invented to proffer solution to the symmetric-key cryptography challenges [3]. The proposed approach provides a hybrid encryption scheme using AES and ECC to enhance the cloud data security by encrypting data using AES then encrypt AES key with ECC when in cloud. This paper discusses different cryptographic encryption methods and also provides a hybrid encryption method for a cloud application.

The rest of the paper is organized as follows. literature review is presented in Section 2, while section 3 discussed the proposed scheme. Section 4 highlights performance evaluation with section 5 giving the concluding remarks.

2. LITERATURE REVIEW

Since the dark age, secret writing has been part of human means of communication. Thus, the systemic information concealment study solely for intended targets continues to impact its operational mode in today's world of information technology (IT). The Internet has paved way for a virtual world in which distance is no longer a barrier to fast communication in a safe and secure mode. The safe and secure communication has Cryptography as its integral for security assurance. Priyadarshini et al.[4] presents Cryptography as the unintelligibility information presentation to unauthorized persons. Studies have shown that information assurance characteristics such as privacy, integrity secret data validation and nonrepudiation are products the existing cryptographic techniques- symmetric and asymmetric [5]. It protects data privacy and prevents alteration occurring during active and passive attacks transmission channels. Cryptography utilization resources cost are time, memory and CPU usability time in other to achieve the ultimate goal of protecting data. Encryption is a major component of cryptography; it is using an algorithm and a key to change the actually meaning of an input into a different meaning which is the encrypted output called the cipher. In the major algorithms mentioned earlier, symmetric technique uses one key, the private key, to encrypt and decrypt. While the asymmetric algorithm has two keys- a private and public; with the public key encrypting, whereas the other key decrypts. Figure 1, presents cryptography classes with examples such as DES, AES, 3DEC, BLOWFISH. The asymmetric key cryptography has mainly RSA, ECC algorithm schemes

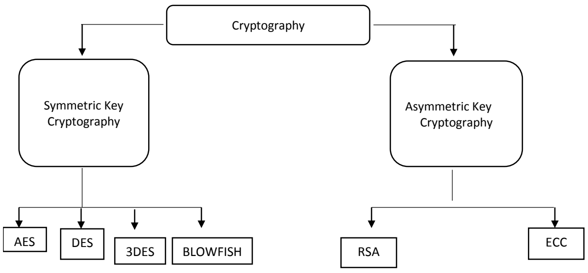


Fig 1: Cryptography Techniques

2.1 Symmetric Algorithm

2.1.1 The Advanced Encryption Standard (AES)

AES is faster and more efficient symmetric algorithm [6, 7]. The Rijndael block cipher is the basic building block as designed by Joan and Vincent Rijmen. Its components of key and block length variants are 128, 192 or 256-bits. Kumar[8] reports AES, a symmetric algorithm with a very high security, proven efficient and safe. AES cipher's properties remain resilient to password investigation; its usage in hardware and software are seamless. In addition, its suitable for hash functions, stream cipher as well as devices with high speed requirement [9]. AES key sizes of 128,192,256 bits and their corresponding rounds number of 10, 12, and 14 respectively. The algorithm uses substitution of byte, Mix Column, shift row and add round key operation to generate private key which covert a plain-text to cipher-text as presented in Figure 2, carried out in each round consisting several processing steps.

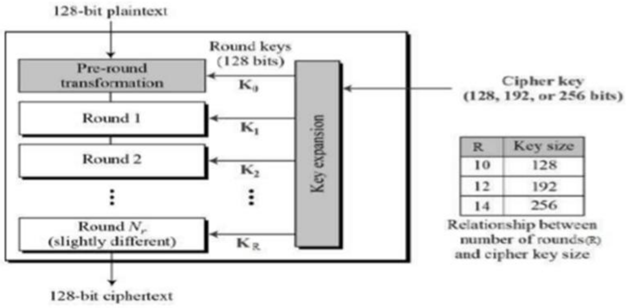


Fig 2: AES Schematic structure

2.1.2 The Data Encryption Standard (DES)

NIST designed block cipher by IBM in 1974. two permutations (P-boxes), tagged initial and final permutations, with sixteen Feistel rounds are the encryption process. DES has 64 bits key length comprising 8 bits parity with effective 56 bits which has been considered too short. Various attacks and techniques vulnerabilities have been observed with DES, thus, making it insecure block cipher [10]. The DES structure is given in Figure 3: the 16 processing stages are identical and its tagged *rounds.*

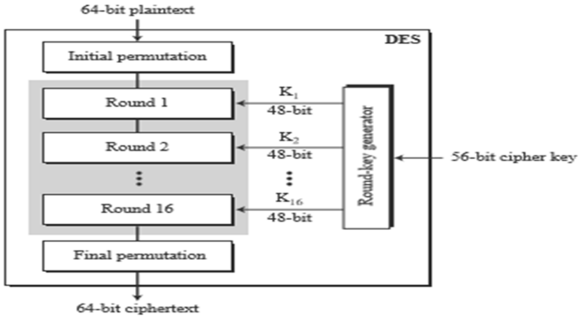


Fig 3: DES Structure

2.1.3 Triple DES

Triple DES, developed in 1998 as a DES enhancement, provides a modest technique of incrementing DES key size to protect against attacks such that no new block cipher is required. It has 64-bit block with 192 bits key size. Triple DES entails more time than DES owing to the triple-tier encryption feature, this in turn consume extra power that yields low throughput. Figure 4 shows 3DES steps and process.

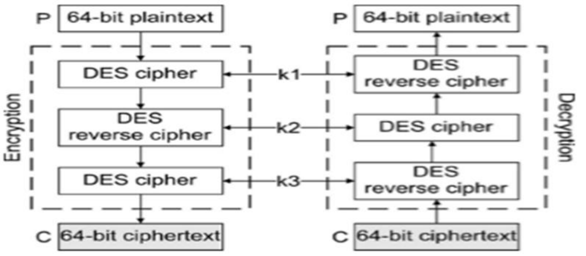
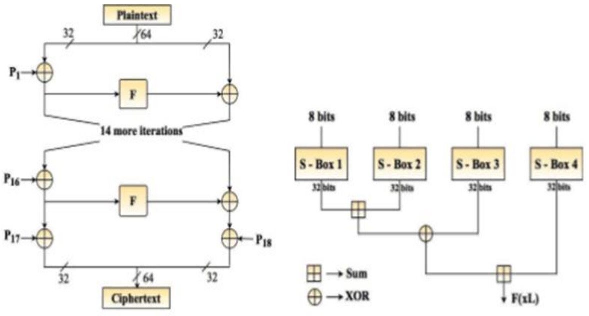


Fig 4: 3DES Structure

2.1.4 Blowfish

A key block cipher with 16 round Feistel steam. It adopts large key tagged dependent S-boxes and repeats a easy encryption with 64 bits block size and varying key –length of 32 bits to 448bits. The two main functions of Blowfish are key expansion and data encryption. Figure 5 presents a Blowfish representation [11].



(a) (b)

Fig 5: (a) Blowfish algorithm (b) Function module

2.2 Asymmetric Algorithm

Asymmetric crypto scheme otherwise known as PKC. The public key encrypts the plain-text and the private key decrypts it. Asymmetric algorithms are: Rivest Shamir Adlemen (RSA), Elliptic Curve Cryptography.

2.2.1 Elliptic Curve Cryptography (ECC)

ECC is a PKC technique grounded on elliptic curve theory to create faster, smaller and more efficient cryptographic keys [12]. It is known for enhancing security as well as achieving more efficient implementations for the security level as compared to other asymmetric cryptography system such as RSA. ECC yields an enhanced security by a 164-bit key while RSA requires a 1,024-bit key to achieve same level of security. ECC offers solution to a robust Cloud environment through enhanced performance in terms of computing power and battery resource usage. Figure 6 shows the elliptic curve representation with two distinct points, P and Q, whose addition is given as the negation of the point resulting from the intersection of the curve, E, and the straight line defined by the points P and Q, giving the point, -R.

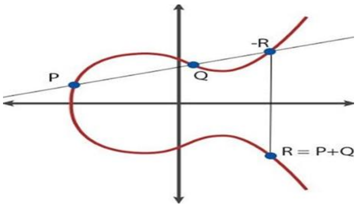


Fig 6: Elliptic Curve Representation

2.2.2 Rivest-Shamir-Adleman (RSA)

The RSA scheme published by Ron Rivest, Adi Shamir and Len Adleman in 1978, is a block cipher., with plain-text and cipher-text lying between integers 0 and n-1, n being 1024 bits. Factoring the product of two large prime numbers is the basis for its asymmetry feature. Thus, encrypted messages with the public key are decrypted rationally in a limited time via its matching private key. Generation of public and private keys are computed with modulus of a composite n and exponent operations, finding a value m such that $C = m^\wedge e(mod\ n)$ where (n, e) is a public key and C is the cipher text. These operations yields the RSA cryptosystem security.

2.3 Cryptography Algorithms Comparison

These algorithms use different key length, block size, cipher type, which produces different security level, speed and power consumption. Table 1 shows different algorithms comparison.

Table 1. Cryptography Algorithm Comparison

Factors	**DES**	**3DES**	**AES**	**Blowfish**	**RSA**	**ECC**
Developed	IBM in 1975	IBM in 1978	Vicent rijman, Joan Daemon 2001	Bruce Schneier 1993	Ron Rivest 1978	Neal Koblitz, Victor Miller 1985
Key length	56bits	168bits (k1, k2, k3) 112bits (k1 and k2)	128, 192, 256 bits	32 to 448bits	1024bits	160bits
Block size	64bits	64bits	128bits	64 bits	Min 512 bits	64bits
Security	Not secure enough	Not secure enough	Adequately secured	Least secure	Least secure	Adequately secured
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher	Asymmetric discrete logarithm
Speed	Moderate	Slower	Faster	Faster	Slower	Faster
Rounds	16	48	10-128 bits key 12- 192 bits key 14- 256 bits key	16	1	16
Power Consumption	Low	Low	Low	Low	High	Low

3. PROPOSED SCHEME

Cloud data Security can be ensured by implementing cryptography algorithm to protect data from eavesdroppers. The use of a hybrid encryption using both symmetric and asymmetric algorithm is the best practice to enhance high level security of cloud data. From Table 1 AES cryptography algorithm is fast, more popular and widely adopted symmetric encryption algorithm with increasing computing power. While ECC asymmetric algorithm with low power consumption and increased computing with a minimum 160 bits key length compared to 1024bit RSA with the same security level was chosen for subsequent level encryption.

3.1 First Level Encryption

Substitution and permutation network are the AES operation units. The encryption components have series of linked operations. Substitution is the idea of mixing operation (linear and nonlinear) in order to establish a relationship among the plain-text, ciphertext and key, while Permutation specifies every bit of the cipher-text rely on every bit of the plain-text with the key. The substitution and permutation network safeguards attacker's plain-text prediction operations linking a specific ciphertext, even after observing a number of (similar) plaintexts and their corresponding cipher-texts [13]. These procedures incorporate byte conversion, array arrangement, mathematical preliminaries, Sub-Bytes transformation, Shift-Row transformation, Mix-Columns transformation, Add-Round-Key transformation. The procedure utilizes the generated output from previous as input to the next stage. The 128bits sequence of blocks has encryption rounds blocks made up of 4 x 4 bytes-array suitable for matrix operation, the block is divided into. AES is considered both cryptographically secure and relatively fast. It can be used in a variety of mode for basic block cipher extension into a stream cipher, which can be used to encrypt arbitrary length of data. AES algorithm supports data and key length combination such as 128, 192 or 256 bits with rounds of 10, 12, and 14 keys respectively.

The private key is shared between both the sender (Alice) and receiver (Bob) for accessing the encrypted data. Generation of the required key is computed with the function -key derivation (KDF). KDF creates required cryptographic keys using an input string of password, secret questions or non-uniform random number

The created keys ensure maintenance of electronic data security and protection while in transit or storage status. A significant feature of KDF key generation is pseudorandom that prevents possible suggestion that the eavesdropper can use for electronic data access; that is, given an input string such as password a dispute so it will confine a pointer to the true string source either key by KDF or same length random string.

AES private key is computed with a given plain text m, KDF generates a private key for encryption K_e to convert m to Cipher text c and private key for decrypting K_d is used to convert c back to m where K_e =K_d

3.1.2 AES Data encryption

i. $Key\ Expansion \leftarrow Round\ key : (Cipher\ key \circ Rijndael's\ key\ schedule)$

ii. $Add\ round\ key \leftarrow Round\ initial\ 1 : Each\ Byte \oplus derived\ round\ key.$

iii. $Rounds\ Processing$

  a. $Sub\ Bytes \leftarrow nonlinear\ substitution: (Every\ Byte \rightarrow Lookup\ Table)$

  b. $Shift\ rows \leftarrow Transposition : \frac{\gg}{cyclic}(row)\ in\ n\ required\ times$

  c. $Mix\ columns \leftarrow (\dim[A(.)] : C(four\_Bytes, j)$

iv. $Final\ Round \leftarrow Sub\ Bytes,\ Shift\ Rows,\ Add\ Round\ Key$

3.2 Subsequent Level Encryption

The second level of encryption for the cloud application, that takes over encryption from the AES is the ECC algorithm. The ECC is introduced to ensure cloud data security from hackers and eavesdropper. ECC is a PKC, based on discrete logarithms, in which the encryption key is public while the decryption key is private. ECC has horizontal symmetry, which are points on the x axis, any non-vertical line intersects the curve in at most three points. An elliptic curve over a field k is a nonsingular cubic curve in two variables, f(x, y) =0 which maybe a point at infinity. The field k is usually taken as complex number, real, rational algebraic extension of rational numbers or a finite set.

A Weierstrass generalized elliptic curve equation is given in equations 1-3:

$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ ……………………(1)

$(y + \frac{a_1 x}{2} + \frac{a_3}{2})^2 = x^3 + \left(a_2 + \frac{{a_1}^2}{4}\right)x^2 + a_4 x + ({a_3}^2 + a_6)$ ……………… (2)

Or $y^2 = x^3 + {A_2}^1 x^2 + {A_4}^1 x + {A_6}^1,\ x_1 = x + \frac{{A_2}^1}{3}$

$y^2 = x^3 + Ax + B$ ………………………......(3)

A common version of ECC is ECC with Diffie Hellman Algorithm,

With two given points $P, Q\ in\ E\ (F_p)$, there exists a third point, denoted by $P + Q\ on\ E\ (F_p)$, therefore, these relations hold for all $P, Q, R\ in\ E\ (F_p)$

$P + Q = Q + P$ $(commutativity)$

$(P + Q) + R = P + (Q + R)$ $(associativity)$

$P + 0 = 0 + P = P$ $(existence\ of\ an\ identity\ element)$

$There\ exists\ (-p)\ such\ that\ -P + P = P + (-P) = 0\ (existence\ of\ inverse)$

3.2.1 ECC key generation

A selects random integer yA, which is Alice's private key, with Bob as recipient

i. $.\ Alice\ pu\_key := yA * B$

ii. $Bob \rightarrow pr_{key} yB\ and\ Bob\ pu\_key := yB * B$

iii. $Alice\ skey := yA * PB$

iv. $Bob\ skey := yB * P$

3.2.2 Signature generation

i. $For\ signing\ a\ message\ m, using\ Alice's\ pr\_key\ yA$

ii. $e := HASH(m)\ s.t. HASH\ is\ a\ f(SHA - 1, \dots)$

iii. $Rand\ k := [1, n - 1]\ \forall k \in \mathbb{Z}$

iv. $r := i_1\ (mod\ n), where\ (i_1, j_1) = k * B.\ If\ r = 0,\ then\ step\ III$

v. $s := k - 1(e + yA * r)(mod\ n).\ If\ s = 0, then\ step\ III$

vi. $Signature := f(r, s)$

vii. $Finally, Bob \leftarrow Signature\ (r, s)$

3.2.3 Encryption Algorithm

i. $Assume\ Alice\ sends\ an\ encrypted\ message\ to\ Bob$

ii. $Alice\ Plain\_text := f(\ message\ m\ with\ points\ from\ the\ elliptic\ group$

iii. $Alice := Rand\ k\ [1, p - 1]\ \forall k \in Z$

iv. $Cipher\_text := [(kB), (pm + k * PB)]$

v. $Bob := Cipher\_text$

3.2.4 Encryption Algorithm

$Bob\ decrypts\ cipher\_text$

i. $Bob := kB * yB$ $i.e.$ $\{pub\_key\ and\ its\ pri\_key\ yB\}$

ii. $Bob \coloneqq (pm + k * PB) - kB * yB,\ since\ PB : = yB * B,\ so\ the\ difference\ is\ pm$

iii. $Finally, Bob\_message\ \{which\ is\ the\ AES\ cipher\ text\} \coloneqq decode(pm)$

3.3 Hybrid Encryption Level

The unifying of the two different algorithms is to ensure security and to eliminate changes of losing data to hackers.

AES algorithm will first be implemented; the ECC algorithm takes over from the AES encryption by encrypting the AES key in the cloud as shown in the block diagram in Figure 7.

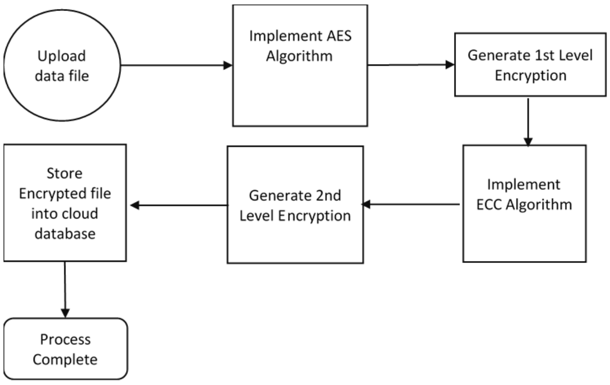

Upload data file
Implement AES Algorithm
Generate 1st Level Encryption
Implement ECC Algorithm
Generate 2nd Level Encryption
Store Encrypted file into cloud database
Process Complete

Fig 7: Multilevel Encryption Block Diagram

While downloading the file, the inverse ECC algorithm decrypts the AES Key and then inverse of AES is implemented on the cipher text to decrypt data. The proposed multilevel decryption is shown in Figure 8

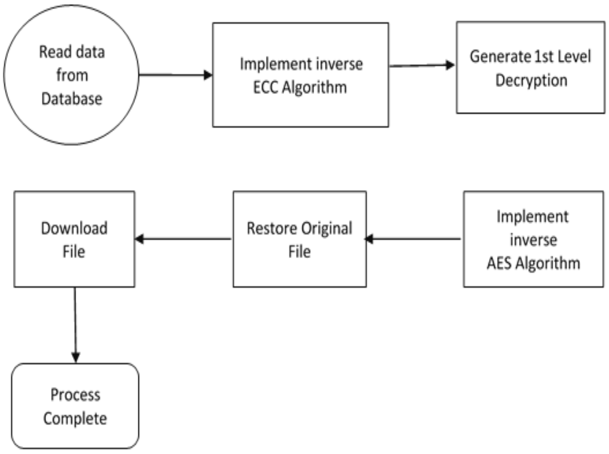

Read data from Database
Implement inverse ECC Algorithm
Generate 1st Level Decryption
Implement inverse AES Algorithm
Restore Original File
Download File
Process Complete

Fig 8: Multilevel Decryption Block Diagram

Figure 9 shows the proposed privacy model for cloud application with the hybrid encryption where AES algorithm first encrypt data and the key to the AES algorithm is thereafter encrypted using ECC, to enhance the cloud data security. The ECC algorithm encrypts only the AES key in a bit to manage the time spend on the multi-level encryption process.

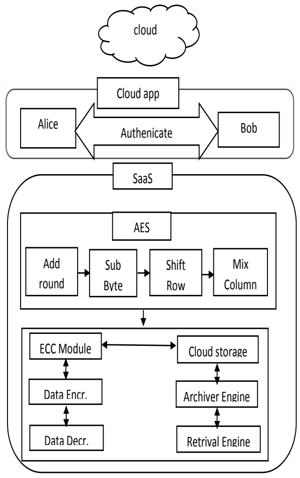


Fig 9: Proposed privacy model for cloud application

4. PERFORMANCE EVALUATION

Cloud computing ensures data storage on external servers with its access via the web. A performance evaluation of the privacy model is computed in order to ascertain the proposed scheme effectiveness, that is, the hybrid encryption of AES symmetric cryptography and ECC asymmetric cryptographic algorithms using these parameters: the encryption and the decryption time, the through put that calculate the efficiency of the algorithm and the cipher-text to plain-text ratio. AES and ECC were selected because using a symmetric and an asymmetric algorithm to enhance the cloud data security is the best practice. The AES algorithm was chosen because the algorithm strength is excellent, it is a faster encryption algorithm compare to other symmetric encryption algorithm, its cost effective, with medium memory size. The ECC algorithm was chosen alongside with the AES because it is a lot better than other asymmetric algorithm in time of speed, key length and computational time. Oftentimes, interference affects the cloud services performance; thus, in the experiment, some virtual machines were dedicated for services provided by ECC. Additional entity in the experimental setup is the Elliptic Curve Admission (ECAs) which is required to handle increased users' application. ECAs receives authentication requests and output authentication tokens made via load balancer. The load balancer of the ECAs sole perform authentication and generate authentication keys with users being connected to the own application

The comparisons were carried out using a 192-bit and 384-bit AES and ECC cipher respectively. The lightweight feature the hybrid scheme requires least probable keys numbers to yield the same result. A total 288 combined keys from 128-bit AES with 160-bit ECC were deployed to get the same task accomplished, this is contrary to the bits of 192 -AES with 384 - ECC to achieve the same task.

Table 2 shows the encryption and decryption runtime for data transferred between Alice and bob with file size stated

Table 2. Multi-Level Encryption Time

Size (kb)	Encryption time (seconds)	Decryption Time (seconds)
20kb	0.25	0.17

65kb	0.92	0.78
40kb	0.41	0.31
45kb	0.58	0.40
30kb	0.4	0.30

The graphical representation of Table 2 is shown in Figure 10 which, indicates the encryption time takes more time than the decryption time.

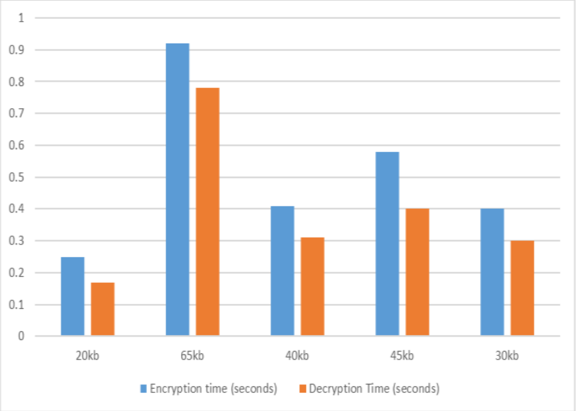


Fig 10: Encryption and Decryption Time

Using 128 AES bits, 160 ECC bits, and 288 bits to achieve the task, equivalently, it takes 192bits AES, and 384 ECC bits to perform a hybrid task. Table 3 shows the proposed hybrid model encryption time compared with, the model using only AES and ECC algorithms separately in the cloud application. Figure 11 presents the time taken on encryption and decryption of the algorithms. The ECC model when used to encrypt takes more time than the proposed AES- ECC system. Even though it was observed that the AES algorithm when implemented alone takes lesser time, the algorithm will not be as secured as the proposed system because if a hacker happens to decrypt one level, it will be difficult to decrypt the second level using the same algorithm.

Table 3. Comparing encryption and decryption time -

Size (kb)	Time (in sec)		
	AES	ECC	Proposed model
20kb	0.25	0.6	0.42
65kb	0.90	1.9	1.60
40kb	0.40	0.82	0.72
45kb	0.55	1.12	0.98
30kb	0.40	0.79	0.70
Average time	0.5	1.046	0.884
Average Size	40	40	40
Throughput	80	38.2	45.42

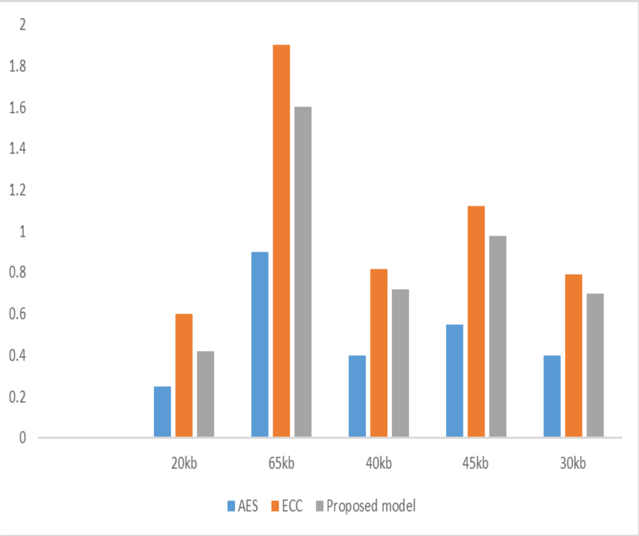


Fig 11: Encryption and decryption time comparison

The encryption speed which is indicated by the throughput computed using the encryption time

The encryption throughput = T_p(kilobytes) /E_t (sec) .4

where T_p is plaintext in kilobytes and E_t is encryption in seconds. As throughput increases the power consumption of the algorithm decreases. Increase throughput means increase functionality.

Figure 11 shows the various input text files with its corresponding encryption: AES, ECC encryption algorithm on cloud application and AES-ECC hybrid encryption algorithm. The algorithms' total time taken was noted. The encryption algorithm performance evaluation is computed based on time spent and throughput. AES was noted to have been the fastest of them. The proposed system was noted to be faster than the ECC algorithm on cloud application. The cipher-text size to plain-text in the proposed hybrid encryption algorithm compared to AES and ECC is on the average. Even though the ratio of cipher-text to plain-text for the proposed model is smaller than the ECC algorithms, but then higher than of the AES presented in Table 4 with Figure 12 as its graphical representation.

Table 4. Ratio of the encrypted text to plain text -

Encryption Algorithm	Ratio of cipher size to plain text
AES	5:2
ECC	4:1
Hybrid Encryption	3:1

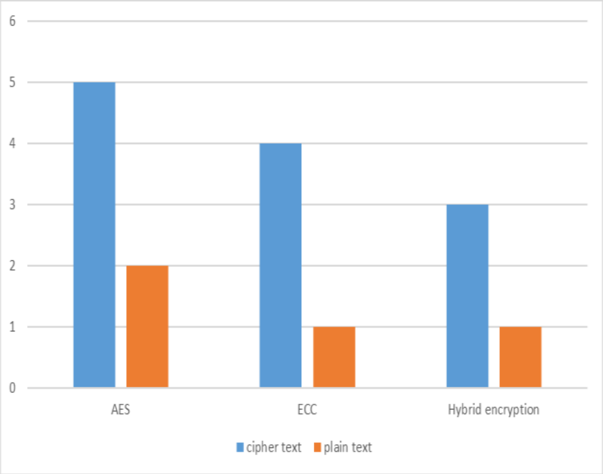


Fig 12: Ratio of the Cipher to plain text

5. CONCLUSION

Cloud computing provides unlimited infrastructure to store and execute data online with less maintenance and high scalability. It is evident that the continuous vulnerability in the Cloud remains tractable with the adoption of cryptographic schemes for secure computation. Security and data confidentiality are obtainable by utilizing data encryption to secure data from unauthorized users. A hybrid encryption model guarantees data privacy was proposed. The proposed model used AES algorithm with its key encryption using ECC, leveraging its feature as a fast-symmetric scheme and less computationally complex robust cryptosystem algorithms respectively. Future study focus will be on the surety analysis of cloud data in a quantum computing environment.

6. REFERENCES

[1] Sultan N. (2010) Cloud Computing for education: A new dawn International Journal of Information Management, International Journal of Information Management, doi: 10.1016/j.ijinfomgt.2009.09.004

[2] Buyya R., Chee S.Y., and Venugopal S. (2008) Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities in 10th IEEE International Conference on High Performance Computing and Communication., pp.5-13

[3] Alese B.K, Philemon E.D, and Falaki S.O. (2012) Comparative analysis of public key encryption scheme. International Journal of Engineering and Technology volume 2 No.9

[4] Priyadarshini P., Prashant N., Narayan D. G., and Meena S. M., (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, Procedia Computer Science 78 (1): 617 – 624.

[5] Ankita, V, Paramita G, and Sunita M. (2016) Comparative Study of Different Cryptographic Algorithms, International Journal of Emerging Trends & Technology in Computer Science, 5 (1): 58-63.

[6] Hirani, S. (2003). Energy Consumption of Encryption Schemes in Wireless Devices Unpublished Thesis, university of Pittsburgh.

[7] Chandramouli, R. (2006). Battery power-aware encryption - ACM Transactions on Information and System Security, 9 (2): 12-25.

[8] Kumar N. (2012) A Secure communication wireless sensor networks through hybrid (AES+ECC) algorithm. von LAP LAMBERT Academic Publishing, vol. 386.

[9] Rachmat N., and Samsuryadi S. (2019) Performance Analysis of 256-bit AES Encryption Algorithm on Android Smartphone. IOP Conf. Series: Journal of Physics: Conf. Series 1196 (2019) 012049

[10] Omotosho O.I (2019) A Review on Cloud Computing Security International Journal of Computer Science and Mobile Computing, Vol.8 Issue.9, September- 2019, pg. 245-257

[11] Manju S. A., and Neema M., (2016) Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Thing. Published by Elsevier Ltd.

[12] Alowolodu O.D, B. K Alese, Adetunmbi A.O, Adewale O. S, and Ogundele O.S (2013) Elliptic curve cryptography for securing cloud computing application. International Journal of Computer Applications (0975 – 8887) Volume 66– No.23.

[13] Thompson A. F., Iyare O. and Alese B.K. (2013): Towards Preserving the Confidentiality of Information in a Local Area Network (LAN) Messaging System, Journal of Applied Computer Science and Mathematics, 14 (7):27-33.