Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3874 - 3891
Received 20 January 2021; Accepted 08 February 2021.

Enhancing the Cloud Security with Ecc based Key Generation Technique

Dr. T. Dheepak
Assistant Professor, Department of Computer Science
Government Arts & Science College
(Formerly Bharathidasan University College),
Perambalur-621 107

ABSTRACT

Online servers will in the near future process private user information. In order to prevent this confidential information from reaching the wrong hands, you must ensure security. More broadly, web providers may need to clarify the rules of their customers, which decide in which conditions who can access private information. Cloud computing continually expands the concept used by various IT technology and internet infrastructure. Cloud storage can be interpreted as offering decentralised IT services over the Internet, rather than locally storing and running those items; these features can encompass software, installations and operating networks. The individuals and organisations are not required to own on-demand services provided by suppliers such as customer relationships management (CRM), rather than spend money on software and installation. In this paper, a new authentication scheme is proposed to enhance the encryption technique based on the optimal key generation with Genetic Algorithm for Elliptical Curve Cryptography to enhance the cloud web services. It is used to prevent the unauthenticated access to the cloud web services utilizing enhancing the encryption of the files and password using optimal key management approach.

KEYWORDS: Web Services, Cloud Computing, Cryptography, Encryption techniques, Optimization techniques, Genetic Algorithm, Elliptical Curve Cryptography

1. INTRODUCTION

Cloud computing is a critical paradigm for the efficiency of on-demand network connectivity and more useful for a common pool of configurable computing services that can be accessed easily and discharged with limited management effort [1][2]. In the traditional method, cloud computing is that it incorporates a system, a network that offers database capacity and internet hosting [3]. The cloud computing's main objective is to provide smart quality of service levels with extensible and low-cost on-demand computing infrastructures [4][5]. However, several companies providing and developing cloud computing services and products have not properly studied the implications of processing, storing, and accessing data in a virtualized and shared environment. In case many cloud-based applications developers are compact to include security protection. For certain instances, accurate protection of presently inexpensive technical abilities cannot be given by developers [6] basically. Cloud computing integrates energy more effectively and individually, in a more distributed venue. This cloud resource can be used by the customer such as amazon, google, IBM, Salesforce, Zoho, Rackspace, Microsoft, etc. It also shares key tools and software available on demand through the use of various IT industries. Cloud service is handled tremendously. The most important thing is that customers do not need to buy the resource from access from third parties; instead, they use and pay for the resource as a service that will save the customer money. The cloud is used for small to medium-sized businesses and not just by large corporations [7]. Safety is regarded as one of the core components of digital computing and the value of data processed in the cloud which does not vary regardless of the vulnerability of the data to cloud storage. Modern services and technology are used by cloud computing infrastructure which were not fully checked about safety. Cloud Computing has a range of core problems and issues such as data protection, trust, direction, expectations and efficiency. The main issue with cloud storage is that data protection which might not be entirely trustworthy has generated a large degree of scrutiny from other businesses about vulnerabilities and the possibility of compromising or misrepresenting insiders to secure safety warnings against cloud providers. Thanks to cloud storage, computer and device systems are being migrated to untrustworthy big data centers, other significant security problems emerge. Throughout this respect, the authentication throughout terms of data validity, encryption and secrecy applies to the user authentication as a respondent, certain security issues such as SQL injection (Structured Query Language), web server bugs and cross-site scripting, privacy safety and physical control come from third party access controls on physical data. Many cloud storage solutions utilize specific encryption methods.

2. SECURITY ALGORITHMS AND CRYPTOGRAPHY

Data Storage represents the records of an entity or company that are available and maintainable by many linked and dispersed cloud-based services. Encryption algorithm[8] plays a significant role in maintaining secure contact over linked and dispersed networks through the usage of the fundamental data security method. The Encryption algorithm transformed the data to the scrambled form, to secure them using "the secret," so the operator of the transmitter only requires a key to decrypt the data. Two forms of key encryption methods are in use in authentication algorithms and they are asymmetric and symmetric key encryption.

The single key is used to encrypt and decrypt information in a symmetric key encryption process. For asymmetric key encryption, two keys are commonly used. Private and public are important. This is used for encryption in the public key method. For decryption [9], a further private key is required. Protection of cloud computing is achieved utilizing a set of proven techniques.

Cryptography focuses primarily on generating safe data during transmission across the network. The principle of encryption is that methods of correspondence and cybersecurity must be revamped and exercised in the presence of enemies. Encryption and decryption methods are used in the cryptography framework. An encryption system transforms message or plaintext into cipher text and removes the initial message or plaintext from the decryption method into the same cipher text. Initially, it is important to encrypt and transfer the details using the cryptographic encryption algorithm. Furthermore, the details will be decrypted with the decryption procedure, that enables the user to interpret the original content.

The Greek term "krptos," which means "hidden or restricted," is originated from cryptography and "gram" is "write or read." It is the use and analysis of a strategy that enables effective contact amid so-called enemies. It builds and analyzes protocols that help protect third parties from trying to read private information or personal messages. Cryptography revolves on secrecy, computer security, protection and non-repudiation. For virtually any topic such as algebra, computer science and electricity, modern cryptography occurs.

This requires two types of coding, which are called encryption and decryption. Encryption transforms plain text to the cipher text utilizing encryption algorithms and techniques sense of it by using an algorithm-generated key in the encryption method. The opposite of encryption on the receiving end is decryption. To do so, the recipient has to know the key otherwise he can't make sense from the encrypted message he receives. The two forms of cryptography are: symmetric and asymmetric [10].

Symmetrical crypt utilizes a common unrevealed key for both encryption and decryption (also known as secret-key encryption). You will hold this key in the network as a password. Yet in open settings where wireless sensor networks are used for health criteria, this is incredibly challenging to do. Several scientists focused on the evaluation of cryptographic algorithms in wireless sensing networks and also offer energy-efficient cipher. Computationally, symmetric key algorithms are much quicker than asymmetric algorithms, as the encryption mechanism is less complicated. Examples include AES etc. Asymmetric encryption (also called public-key cryptography) requires two different keys (public and private) to encrypt and decrypt data, which avoids the possibility of key allocation protection. The secret to privacy is never revealed. A message which is authenticated with the public key can only be decrypted using the same method and the same private key. Likewise, a message which is authenticated using the private key can only be decrypted with the same public key. Examples of this include RSA, ECC etc.

3. RELATED WORKS

Li, Jing, et al[11] presented an efficientoutsourced CP-ABE scheme with checkability, where thenumber of the exponential operations in the encryption canbe reduced to a constant by introducing a blinding algorithm. Furthermore, to guarantee the correctness of the proposed scheme, the authors provided theverification mechanism based on a collision-resistance hashfunction, which allows the users to efficiently check thevalidity of messages and outsourced computation results.

Singh, Gurjeet, and Mohita Garg[12] used the 3 step security mechanism for the keeping the data secure at the cloud. The authors have implemented the strong authentication mechanism using md5 encrypted OTP and enhanced the security of data using Cloud Broker and RSA, Blowfish and AES.

Amalarethinam, DI George, and H. M. Leena[13] described the Encryption and decryption processes of cryptography proposedby various predefined algorithms take much time. Thus, the concentration must begiven to reduce the time of these processes. Many methodologies exist for reducingthe time which is more mathematical in nature. One among them is the concept ofaddition chaining method. The proposed asymmetric cryptographic algorithm usesthe concept of addition chaining to reduce the time spent both in encryption anddecryption processes.

Neela, K. L., and V. Kavitha[14] proposed model followed the decentralized architecture which does not depend on anythird-party system. In this model, the data security can beenhanced by using cyclic shift transposition algorithm. For asecure data transmission and retrieval, the authors used quick responsecode and hash-based timestamp so that the real-time attacksare stopped or prevented.

Goyal, Vikas, and Chander Kant[15] strategiesfollowed include categorization of the data on the basis of their sensitivity andimportance, followed by the various cryptography techniques such as the AES (aSymmetric Cryptography technique), SHA-1 (a Hashing technique), and ECC(Elliptic curve Cryptography (an Asymmetric Cryptography technique). Till date,most of the authors were using a single key for both encryption and decryptionwhich is a weak target of various identified malicious attacks. Hence, in thedesigned hybrid algorithm, two separate keys are used for each encryption anddecryption.

Amalarethinam, DI George, and H. M. Leena[16] proposed genetic algorithm is used for generating the best key which satisfiesthe specified fitness function. The optimal key generated from the proposedgenetic algorithm is encrypted with asymmetric addition chainingcryptographic algorithm (ACCA) to make the key strong. This strengthenedkey can be used for encrypting data.

Tan, Soo Fun, and Azman Samsudin[17] proposed an eXtended HoneyEncryption (XHE) scheme by adding an additional protection mechanism on theexisting user authentication mechanism. When the malicious user attempts tounauthorized access to online bank account by entering his guessed password,instead of rejecting the access, the XHE algorithm generates an indistinguishablebogus bank data, subsequentlyredirects attacker to fake user account, in which theattack could not determine whether the guessed password is working correctly or not.

Mishra, Nishit, et al[18] aimed at the security model for cloud computing which ensures the datasecurity and integrity of user’s data stored in the cloud using cryptography.

Vijayakumar, V., et al[19] presented a planning empowered intermediaryre-encryption method to defeat the security issues. This Technique will allow only limited access rights to an authorized agent toaccess the records for a specific time period. This technique will use a searchable encryption and proxy Re-encryption technique.

ShanmugaPriya, S., A. Valarmathi, and D. Yuvaraj[20] described anenhanced approach for the already used data security model in cloud environment. The proposeddata security model includes generationofOTPusingHMAC(Hashbased message authenticationcode) for user authentication process. This paper also includes a comparativeMD5 and SHAalgorithmsfor the better implementation of the model. This model best suits for any of the layers in it,to achieve this the authors use certain encryption algorithms that convert original text to the form that isnot understood by the third party.

Aghili, Hamed[21] assumed adeduplication storage server and set the blowfish. At 20 Mb block size the time ofblowfish algorithm was (1.7 t) comparing with other algorithms. Also, failure timeof blowfish was 60 t that it was less than DES, AES, and 3DES failure time.

4. PROPOSED ECC WITH OPTIMAL KEY GENERATION ENCRYPTION ALGORITHM

4.1 Elliptical Curve Cryptography

Cryptography with an elliptical curve is a method of public cryptography focused on elliptical curve theory. Rather of utilizing conventional methods of key production using the creator of two very broad prime numbers, this encryption strategy utilizes the property of elliptic curve. At the beginning of the cryptography elliptic curves is used in H.W. The factoring method of Lenstra's elliptical curve. In 1985, N.Kobiltz and V.Miller separately submitted the elliptical curve encryption motivated by this inconsistent usage of elliptic curves.

The biggest advantage of elliptical curve encryption is the usage of smaller keys for the same degree of reliability. ECC will have a 164-bit key to the same protection as the 1024-bit key in other schemes. It is mainly useful in smartphone use, as it is capable of having low processing power and battery capacity with high levels of reliability. ECC is a public key crypto-system for the public key and private key generation to encrypt and decrypt data. The problem of calculating the number of steps or hops it takes to move from one point of the elliptical curve to another is based on the mathematical complexity of resolving the discrete logarithm problem of the elliptical curve. Elliptical curves are symmetrical on the x-axis and are binary curves. The following functions are defined:

$$y^2 = x^3 + ax + b$$

Where x and y are the normal feature variables, while a and b are constant curve determining coefficients. The elliptical curve also changes when the values of a and b vary. For elliptical curves, discriminant. The elliptical cryptography operations are dot extension, dot replication, and dot repetition. The finite field principle is the main function of the elliptical curve. This implies that the values on the curve may be reduced. This "peak" position on the x-axis is defined as "p." The "module value" is also called for any ECC cryptosystem.

This point indicates the minimal duration of the operations on the curve. The modular value in ECC represents the system's key size. The full ECC cryptosystem defining parameters are:

p – Specification of the finite field.

a,b: Coefficients for defining curve

G – Generator points on the curve where the operations starts.

n – Order of G.

h – Division of the total points on the curve and the order of G.

Encryption Process:

Step 1: Obtain the text to be send.

Step 2: Its convert to corresponding ASCII values.

Step 3: The ASCII value partition as [ASCII values, group size 1, this operation group the ASCII values with size known by group size with no overlapping and the sub lists that have size lesser than group size are left as it is without padding]

Step 4: Each group obtained from the above step is converted into big integer values taking base as 65536. From Digits[Group of ASCII values, 65536].

Step 5: Pad with 32 to the end of the list from the above step if the count of the above list is odd, to make it even for performing complete pairing. Each single pair will be an input to the ECC system as „Pm‟. It is pad with 32 because 32 represent blank space in ASCII code.

Step 6:Choose random *k* value, *k* = Random value with range 1 to *n*−1. Calculate *kG* and *kPb* using Point multiplication operation.

Step 7:Compute *Pm* + *kPb* using point doubling or point addition as needed.

Step 8: Transmit *Pc* = {*kG, Pm* + *kPb*} as cipher text to the receiver side.

Decryption Process:

Step 1:The cipher text Pc is obtained.

Step 2: The left part kG and right part of the Pc separately (Pm + kPb).

Step 3:Multiply with nB to the left part and subtract it from the right part to obtain Pm. {Pm + kPb} − nBkG = Pm since Pb = nBG.

Subtraction operation can be converted to addition by multiplying with −1 to the y coordinate. By applying point addition operation can be validated to obtain the mirror image point over the x-axis.

Step 4: By forming set of ASCII values, the above operation will be provide the integer value and then convert it back to list of ASCII values. Integer Digits [n, b] in Mathematics provides a set of the base b digits in the integer n. Digits function and Integer Digits are opposite to each other so that the ASCII values are secured during encryption and decryption.

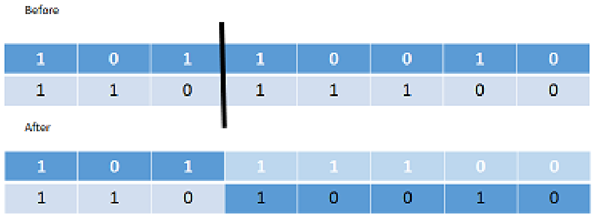
Step 5:The list of ASCII values converts to its corresponding characters.

Received 20 January 2021; Accepted 08 February 2021.

4.2 Genetic Algorithm

GA is an adaptive search algorithm that utilizes human and genetic dynamics. GA forms part of evolutionary algorithms; used with biologic mechanisms, such as selection, crossover and mutation, to solve optimization challenges. The key idea of GA is to imitate the randomness of nature, in which the selection of the natural system and its behavior enable people to adapt to the environment. It can, we can say, be supported by the exclusion of people that are less suited for survival and reproduction. The population is produced in such a way as to most likely replicate the person with the highest fitness value and discard them based on the threshold established by an iterative application of stochastic genetic operators.

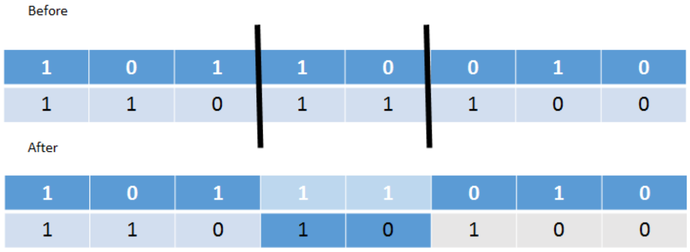
Crossover Operator: Crossover is a genetic operator that links a single chromosome to two chromosomes. The freshly formed infant chromosome comprises of each child's chromosomes. A single point, two points and the uniform crossover are classifying crossover. Crossover. Just one convergence point is selected for creating new children in a single point.



1	0	1	1	0	0	1	0
1	1	0	1	1	1	0	0

1	0	1	1	1	1	0	0
1	1	0	1	0	0	1	0

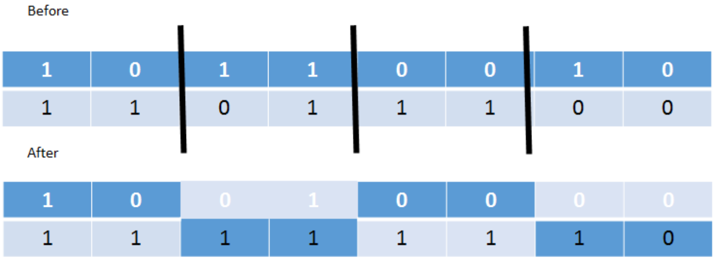
Figure 1.1: Single Point Crossover



1	0	1	1	0	0	1	0
1	1	0	1	1	1	0	0

1	0	1	1	1	0	1	0
1	1	0	1	0	1	0	0

Figure 1.2: Two point Crossover



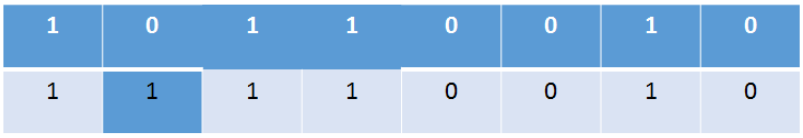
1	0	1	1	0	0	1	0
1	1	0	1	1	1	0	0

1	0	0	1	0	0	0	0
1	1	1	1	1	1	1	0

Figure 1.2: Uniform Crossover

Mutation Operator:

At least one bit in each chromosome is modified in mutation after crossover. It is achieved such that the influence of the normal genetic cycle represents. There are two main forms of Bits and Boundary Mutation mutations. One or more bits are converted to 0 to 1 or 1 to 0 when bits are rotated. The randomly higher or lower component in boundary mutants swapped into chromosomes.



1	0	1	1	0	0	1	0
1	1	1	1	0	0	1	0

Figure 1.4: Mutation Operator

Selection Operator:

Chromosomes for future population production are drawn from the community. The health benefit for the competition is the greater the rating, the higher the chances to be selected. Range of roulette disks, tournament range; Truncation Selection is known as roulette collection.

Fitness Function:

Genetic algorithm is really important since good fitness functions can be useful for quest space exploration effectively and poor fitness functions can be restricted to an optimal local solution. Health may be defined as continuous health and mutable fitness. Key collection is a sort of classification question for cryptography and, if the collection is assumed, the key of maximum fitness and alignment is selected. The applications of genetic algorithms are also heuristic, making GA a reliable key generation and data encryption algorithm.

4.3 Proposed Genetic Algorithm based Optimal Key Generation for ECC (GA-OKG-ECC)

The following are the phases involved in the password encryption for cloud web services. The genetic operators are used in the key generation. Initial population is generated through random number generator. For simplicity one-point crossover and bit filliping techniques are used for Crossover and Mutation respectively. Fitness value of key is calculated through Shannon Entropy because entropy is one of important feature of randomness.

Phase 1: Optimal Key Generation with Genetic Algorithm

Step 1: Sixteen random characters are generated with the help of random number generator from A-Z.

Step 2: Each randomly generated character is converted to binary format (8 bits).

Step 3: The result is stored in 2D array data structure.

Step 4: Eight random numbers from 1 to 7 are generated for crossover points.

Step 5: The numbers are stored in array data structure.

Step 6: One-point crossover is performed by taking one parent from array of random prime number and one parent from array of random characters. The crossover point is identified from the array of random numbers generated in step 5.

Step 7: Step 6 will be repeated until there is parent left for crossover.

Step 8: For Mutation, bit flipping mutation is used in which first and last bit of each chromosome is inverted; means 0 will be converted to 1 and vice versa.

Step 9: Step 8 will be repeated for all the child chromosomes.

Step 10: After Mutation, Fitness function of each chromosome is calculated through Shannon Entropy.

Step 11: Chromosomes with the Shannon Entropy of greater than 0.95 will be merged and selected as key. If there is no any.

Step 12: Chromosome with entropy greater than 0.95 then the whole process will be repeated again until there is no best fit key.

Phase 2: Signature Generation

To sign a message m by the sender, it performs the following steps:-

Step 1: It calculates a cryptographic hash function $e = hash\ (m)$.

Step 2: The sender then selects a random integer k from [1, n-1].

Step 3: Then it computes a pair (r,s).

Step 4: $r = x1\ (mod\ n)$ where $(x1, y1) = k * G$

Step 5: s= k-1(e+ dA*r)

Step 6: This pair (r,s) defines the signature.

Step 7: This signature is sent to the receiver.

Phase 3: Encryption Algorithm

Suppose sender wants to send a message m to the receiver.

Step 1: Let m has any point M on the elliptic curve.

Step 2: The sender selects a random number k from [1,n-1].

Step 3: The cipher texts generated will be the pair of points (B1,B2) where

B1= k*G

B2 = M + (k*G)

Phase 4: Decryption Algorithm

To decrypt the cipher text, following steps are performed: -

Step 1: The receiver computes the product of B1 and its private key.

Step 2: Then the receiver subtracts this product from the second point B2.

$$M = B2 - (dB * B1)$$

Where M is the original data sent by the sender.

Phase 5: Signature Verification

To authenticate the sender's signature, the receiver must have the knowledge about sender's public key PA.

Step 1: For authentication the receiver needs to verify the pair (r,s) are in the range of [1,n-1].

Step 2: The receiver again then calculates the hash function e as in signature generation.

Step 3: Then the receiver calculates w =s-1 mod(n).

Step 4: Then calculate u1= e*w (mod n) and u2 = r*w (mod n).

Step 5: Calculate (x1,y1)= u1*G + u2*PA.

Step 6: If x1 = r (mod n), then the signature is valid.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3874 - 3891
Received 20 January 2021; Accepted 08 February 2021.

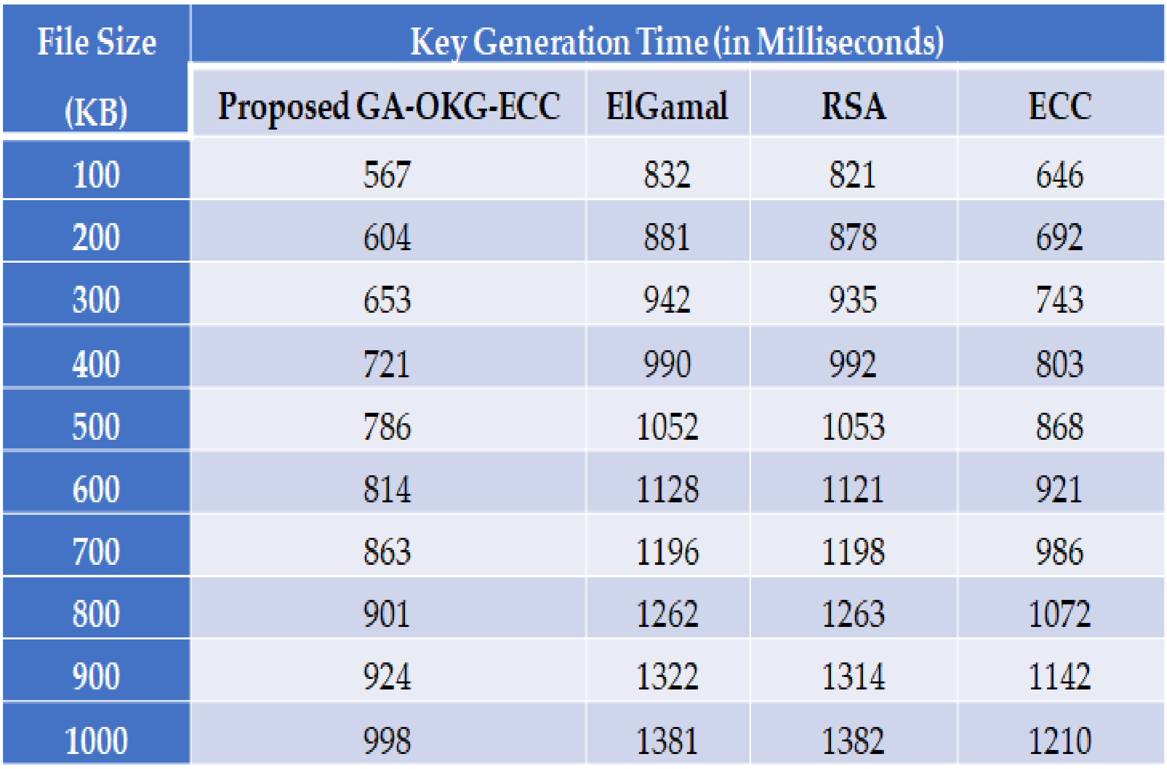
5. RESULT AND DISCUSSION

5.1 Assumptions

The performance of the proposed GA-OKG-ECC are evaluated with the existing encryption techniques like Key Generation Time (milliseconds), Encryption time (in Milliseconds), Decryption time (in milliseconds), total time taken for encryption and decryption and Throughput (in mbps) for varying file sizes from 100 (kilobytes (KB)) to 1000 (KB).

Table 1 depicts the key generation (in Milliseconds) by the proposed GA-OKG-ECC, and existing encryption techniques like RSA, ECC, and ElGamal for varying file sizes increasing from 100kb to 1000kb. Figure 2 depicts the graphical representation of the key generation (in Milliseconds) by the proposed and existing encryption techniques for cloud web services. From the table 1 and figure 2, it is observed that the proposed GA-OKG-ECC method consumes less time for key generation than the existing techniques like ElGamal, RSA and ECC.

Table 1: Key Generation (in Milliseconds) by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques



File Size (KB)	Key Generation Time (in Milliseconds)			
	Proposed GA-OKG-ECC	ElGamal	RSA	ECC
100	567	832	821	646
200	604	881	878	692
300	653	942	935	743
400	721	990	992	803
500	786	1052	1053	868
600	814	1128	1121	921
700	863	1196	1198	986
800	901	1262	1263	1072
900	924	1322	1314	1142
1000	998	1381	1382	1210

Received 20 January 2021; Accepted 08 February 2021.

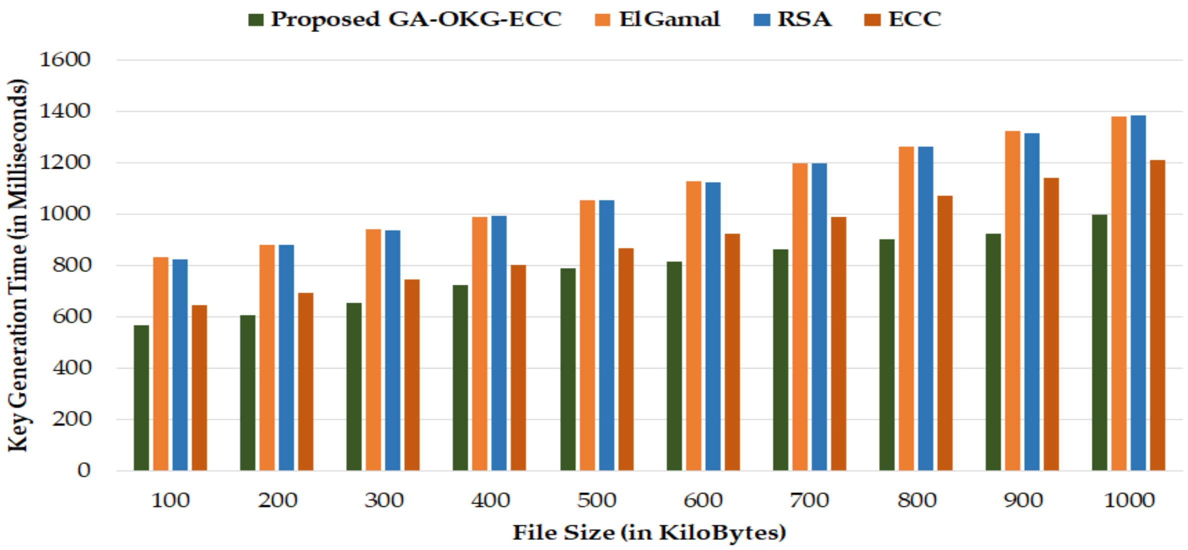


Figure 2: Graphical representation of the Key Generation time (in Milliseconds) by the proposed and existing encryption techniques

Table 2 depicts the Encryption time (seconds) by the proposed GA-OKG-ECC, and existing encryption techniques like RSA, ECC, and ElGamal for varying file sizes increasing from 100kb to 1000kb. Figure 3 depicts the graphical representation of the encryption time (in Milliseconds) by the proposed and existing encryption techniques for cloud web services. From the table 2 and figure 3, it is observed that the proposed GA-OKG-ECC method consumes less time for encryption than the existing techniques like ElGamal, RSA and ECC.

Table 2: Encryptiontime (seconds) by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption technique

File Size (KB)	Encryption Time (in seconds)			
	Proposed GA-OKG-ECC	ElGamal	RSA	ECC
100	28	69	68	43
200	34	88	83	68
300	49	98	96	81
400	63	128	118	102
500	82	145	138	123
600	98	175	167	142
700	109	192	181	168
800	122	214	203	185
900	141	245	234	204
1000	156	275	263	235

s

Received 20 January 2021; Accepted 08 February 2021.

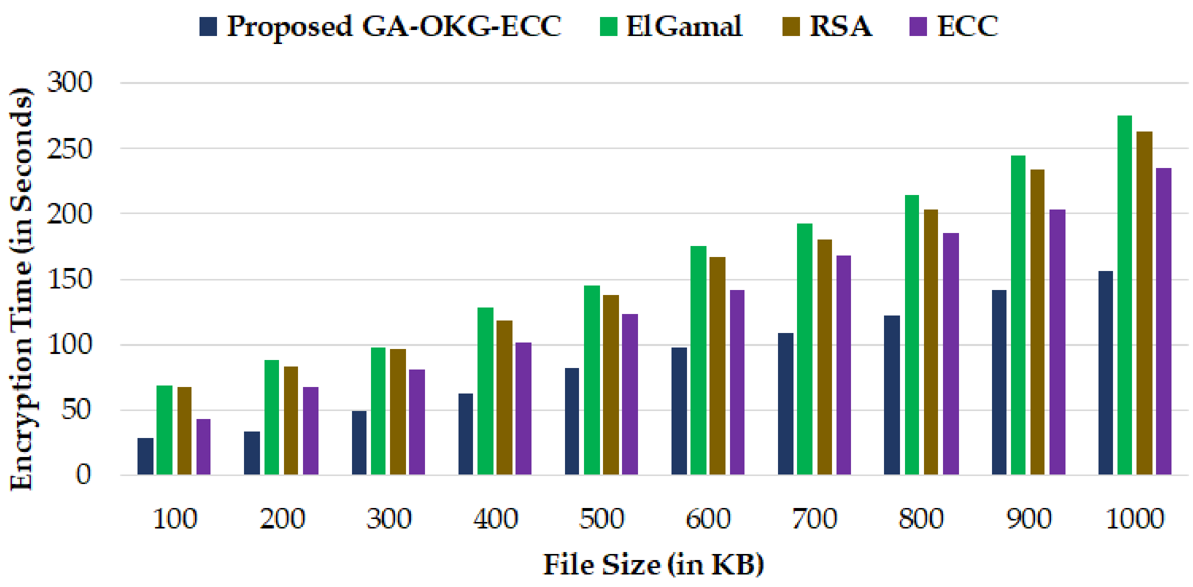


Figure 3: Graphical representation of the encryption time (in seconds) by the proposed and existing encryption techniques

Table 3 depicts the Decryption time (seconds) by the proposed GA-OKG-ECC, and existing encryption techniques like RSA, ECC, and ElGamal for varying file sizes increasing from 100kb to 1000kb. Figure 4 depicts the graphical representation of the decryption time (in Milliseconds) by the proposed and existing encryption techniques for cloud web services. From the table 3 and figure 4, it is observed that the proposed GA-OKG-ECC method consumes less time for decryption than the existing techniques like ElGamal, RSA and ECC.

Table 3: Decryptiontime (seconds) by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques

File Size (KB)	Decryption Time (in seconds)			
	Proposed GA-OKG-ECC	ElGamal	RSA	ECC
100	21	53	44	32
200	29	60	53	48
300	42	75	72	67
400	54	90	83	75
500	69	102	95	92
600	82	128	123	118
700	96	150	145	134
800	112	173	165	156
900	128	192	187	178
1000	132	204	198	192

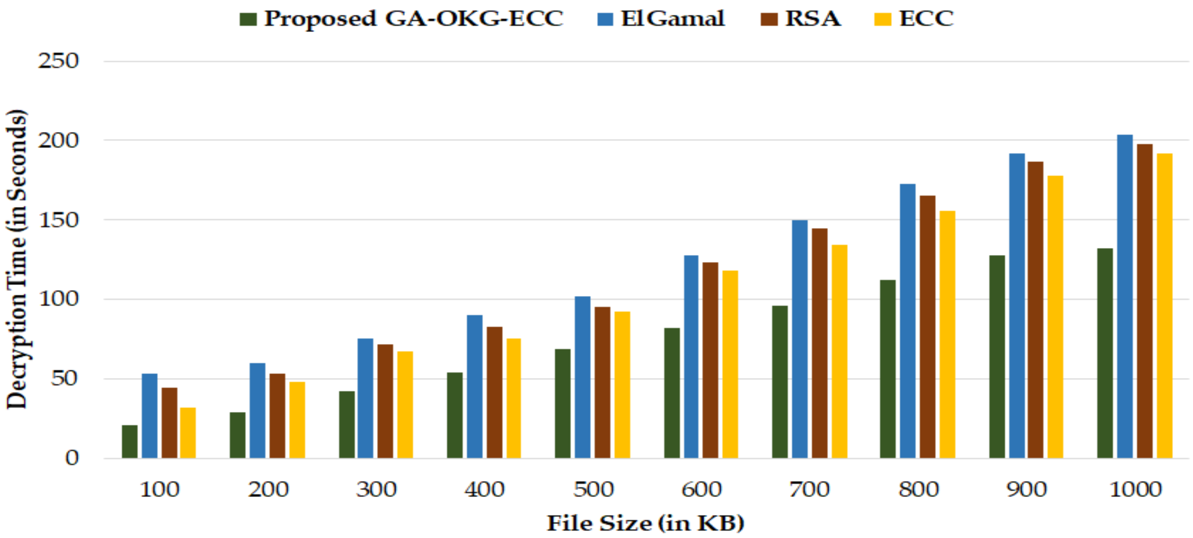


Figure 4: Graphical representation of the decryption time (in seconds) by the proposed and existing encryption techniques

Table 4 depicts the total time taken (seconds) for encryption/decryption by the proposed GA-OKG-ECC, and existing encryption techniques like RSA, ECC, and ElGamal for varying file sizes increasing from 100kb to 1000kb. Figure 5 depicts the graphical representation of the total time taken (in Milliseconds) for encryption/decryption by the proposed and existing encryption techniques for cloud web services. From the table 4 and figure 5, it is observed that the proposed GA-OKG-ECC method consumes less total time for encryption and decryption than the existing techniques like ElGamal, RSA and ECC.

Table 4: Total time taken (in seconds) for encryption/decryption by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques

File Size (KB)	Total time taken (in seconds)			
	Proposed GA-OKG-ECC	ElGamal	RSA	ECC
100	49	122	112	75
200	63	148	136	116
300	91	173	168	148
400	117	218	201	177
500	157	247	233	215
600	180	303	290	260
700	205	342	326	302
800	234	387	368	314
900	264	437	421	382
1000	294	479	461	427

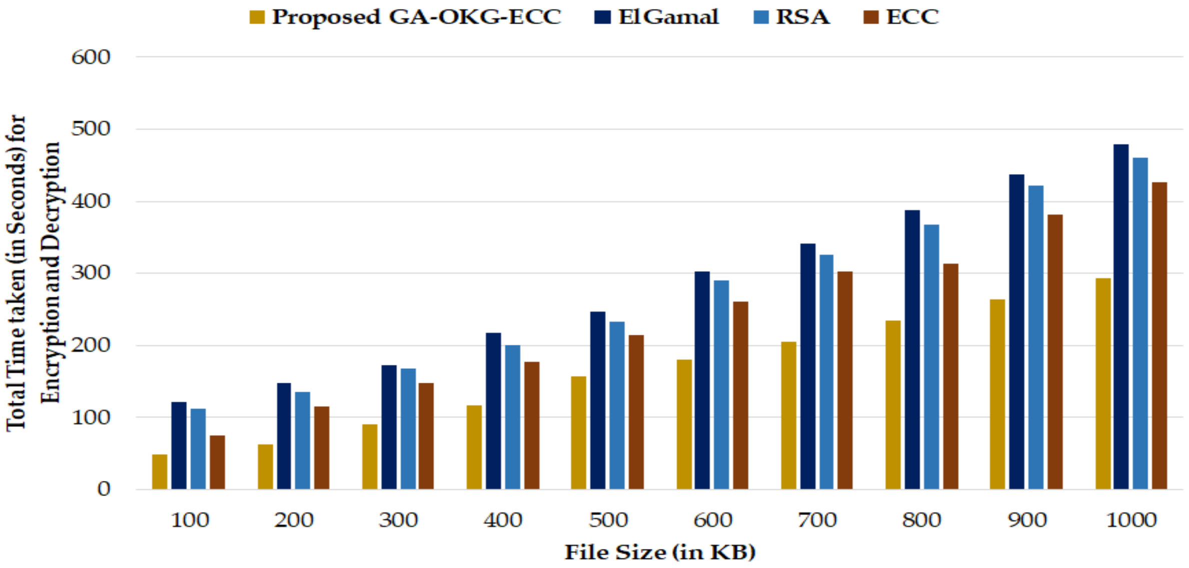


Figure 5: Graphical representation of the Total time taken (in seconds) for encryption/decryption by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques

Table 5 depicts the throughput (in mbps) for encryption/decryption by the proposed GA-OKG-ECC, and existing encryption techniques like RSA, ECC, and ElGamal for varying file sizes increasing from 100kb to 1000kb. Figure 6 depicts the graphical representation of the throughput (in mbps) by the proposed and existing encryption techniques for cloud web services. From the table 5 and figure 6, it is observed that the proposed GA-OKG-ECC method gives more throughput (in mbps) than the existing techniques like ElGamal, RSA and ECC.

Table 5: Throughput (in mbps) by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques

File Size (KB)	Throughput (in mbps)			
	Proposed GA-OKG-ECC	ElGamal	RSA	ECC
100	1436	1113	1128	1342
200	1487	1172	1186	1381
300	1521	1230	1245	1415
400	1545	1273	1288	1464
500	1598	1314	1326	1532
600	1628	1368	1378	1583
700	1675	1426	1432	1641
800	1708	1467	1483	1692
900	1734	1518	1535	1714
1000	1789	1575	1590	1728

Received 20 January 2021; Accepted 08 February 2021.

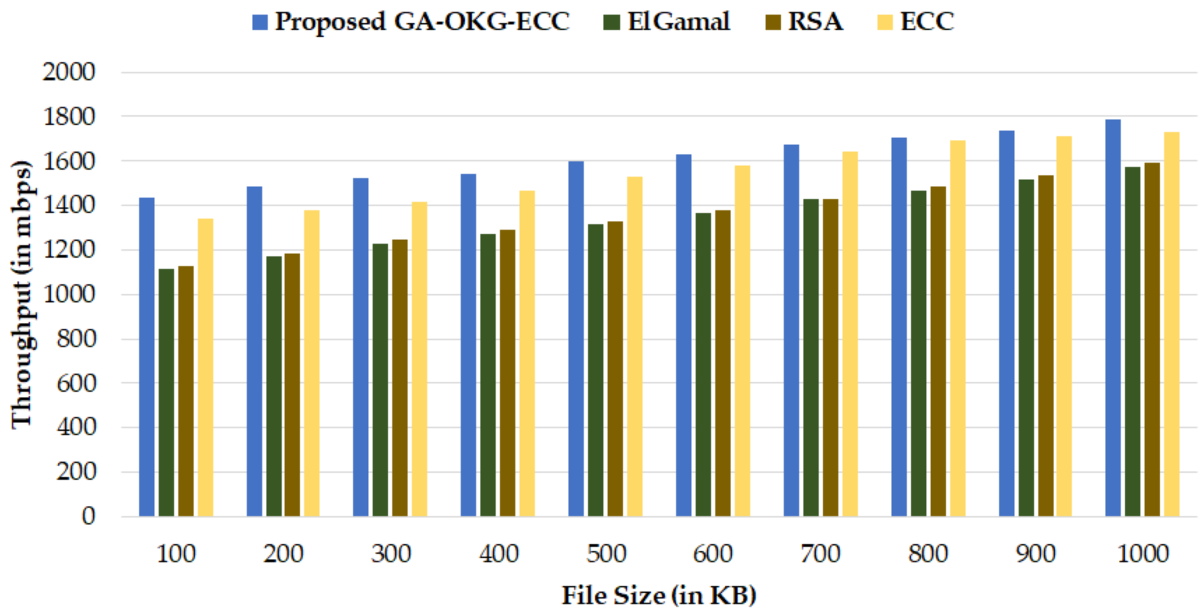


Figure 5: Graphical representation of the Throughput (in mbps)by the proposed GA-OKG-ECC, ElGamal, RSA and ECC encryption techniques

6. CONCLUSION

Cloud storage is a centralized database network pool that can be used to exchange data, infrastructure and knowledge mostly across the internet with individuals. There are various protection issues, such as verification, anonymity and honesty. Data encryption is widely used for the protection and security of data over the internet. Numerous algorithms have been developed for data protection, which is protected and avoid hackers or perpetrators from sharing data over the Internet. In this report, the automated key generation using a Genetic Algorithm to boost the protection of cloud web services is proposed with ECC for the current authentication method.From the result obtained, it is observed that the proposed GA-OKG-ECC method performs well in the aspects of Key Generation time, Encryption, Decryption and Total time taken for encryption and decryption, throughput for the given increasing file size ranging from 100 KB to 1000KB.

REFERENCES

[1] http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud Benefitsand-drawback.

[2] Michael glas and paul Andres, “An Oracle white paper in enterprise architectureachieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3] Harjit Singh Lamba and Gurdev Singh, “Cloud Comuting-Future Framework for e-management of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM- Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5] Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST, Germany.

[6] Tackle your client’s security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues withcloud- computing-in-10-steps.

[7] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[8] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248- 9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[9] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[10] Mahajan, S. and Singh, M. (2014) Analysis of RSA Algorithm Using GPU Programming. arXiv:1407.1465 [cs.CR].

[11] Li, Jing, et al. "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption." *Soft Computing* 22.3 (2018): 707-714.

[12] Singh, Gurjeet, and Mohita Garg. "Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP." *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY* 18 (2018): 7364-7380.

[13] Amalarethinam, DI George, and H. M. Leena. "Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) for Data Security in Cloud." *Advances in Big Data and Cloud Computing*. Springer, Singapore, 2018. 331-340.

[14] Neela, K. L., and V. Kavitha. "Enhancement of data confidentiality and secure data transaction in cloud storage environment." *Cluster Computing* 21.1 (2018): 115-124.

[15] Goyal, Vikas, and Chander Kant. "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security." *Big Data Analytics*. Springer, Singapore, 2018. 195-210.

[16] Amalarethinam, DI George, and H. M. Leena. "A new key generation technique using GA for enhancing data security in cloud environment." *International Journal of Cloud Computing* 7.1 (2018): 4-14.

[17] Tan, Soo Fun, and Azman Samsudin. "Enhanced Security of Internet Banking Authentication with EXtended Honey Encryption (XHE) Scheme." *Innovative Computing, Optimization and Its Applications*. Springer, Cham, 2018. 201-216.

[18] Mishra, Nishit, et al. "Secure Framework for Data Security in Cloud Computing." *Soft Computing: Theories and Applications*. Springer, Singapore, 2018. 61-71.

[19] Vijayakumar, V., et al. "E-health cloud security using timing enabled proxy re-encryption." *Mobile Networks and Applications* 24.3 (2019): 1034-1045.

[20] ShanmugaPriya, S., A. Valarmathi, and D. Yuvaraj. "The personal authentication service and security enhancement for optimal strong password." *Concurrency and Computation: Practice and Experience* (2019): e5009.

[21] Aghili, Hamed. "Improving Security Using Blow Fish Algorithm on Deduplication Cloud Storage." *Fundamental Research in Electrical Engineering*. Springer, Singapore, 2019. 723-731.