ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse294952020.pdf
https://doi.org/10.30534/ijatcse/2020/294952020

A Genetic Algorithm based Key Management Approach for Enhancing Data Security in Cloud Environment

Shahnawaz Ahmad[1], Shabana Mehfuz[2], and Javed Beg[3]
[1,2]Department of Electrical Engineering, Jamia Millia Islamia, New Delhi-110025, India,
shahnawaz98976@gmail.com, smehfuz@jmi.ac.in
[3]Oracle-India
javed.beg@oracle.com

ABSTRACT

More enterprises are moving sensitive data to the cloud, increasing the need to secure that data. With cloud technology becoming a larger and more important part of running a digital business, cloud computing (CC) platforms are rapidly limiting the effectiveness of the traditional security model. Since data and applications in the cloud reside the old enterprise boundaries, they must now be protected in new ways. As more and more users connect directly to the cloud applications, it is imperative to secure cloud assets to meet compliance, privacy and security requirements. Verification and key management are the key challenges within the cloud environment whereas trading the secret data. As of now, security is the main apprehension in the cloud security environment. Ensuring the costumers information may be a basic errand in cloud. Conventional cryptographic symmetric algorithms are reasonable for putting away information in a most secured way. Asymmetric algorithms are favored for encrypting the keys instead of the information since of its fewer speediness. Key management taxonomy comprises of three parts. Part 1 gives common direction and best practices for the administration of cryptographic keying fabric. Part 2 gives direction on approach and security arranging necessities for government organizations. At long last, Part 3 gives direction when utilizing the cryptographic highlights of current systems. The strategy for selecting or producing the key plays an imperative part in securing the data of cloud environment. Genetic algorithm (GA) is a powerful tool for understanding the foremost of the enhancement issues. The proposed Cloud Key Generation Genetic Algorithm (CKGGA) is utilized for producing the finest key which fulfills the required fitness function. The ideal key produced from the proposed CKGGA is encrypted with Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) to form the key solid. This fortified key can be utilized for encrypting information.

Key words: cloud computing; cryptography algorithm; encryption; key management; key generation; genetic algorithm; fitness function; addition chaining.

1. INTRODUCTION

CC can be classified into two categories, i.e. based on cloud location (public, private, hybrid and community cloud) and based on cloud services (IaaS, PaaS, SaaS, DaaS, CaaS and HaaS) as shown by table 1. With the quick increment within the information sharing over the Web, the cloud computing framework is as often as possible utilized in the different information proprietor situation. The cloud computing framework offers different sorts of administrations. Platform as a Service (PaaS) could be a cloud-based benefit that gives more choices to the endorser for choosing the computing platform. Infrastructure as a Service (IaaS) gives the same highlights as the PaaS, but the client is completely capable for controlling the leased foundation. Software as a Service (SaaS) permits the business undertakings to get to the usefulness at a lower taken a toll than the fetched of authorized applications, as the SaaS pricing is based on a month to month fee. Due to the inaccessible facilitating of the program, the clients don't ought to contribute in the extra equipment. The SaaS decreases the exertion of establishment, setup and support by the business enterprises. Data as a Service (DaaS), data services are comparable to SaaS in that the data is put away within the cloud and is open by a wide extend of frameworks and gadgets. Hardware as a Service (HaaS), may be an acquirement show that's comparable to renting or authorizing in which equipment that has a place to a managed service provider (MSP) is introduced at a customer's location and a be service level agreement (SLA) characterizes the obligations of both parties. Communication as a Service (CaaS), is an outsourced endeavor communications arrangement that can be rented from a single seller. Such communications can join voice over IP (VoIP or Web communication), instant messaging (IM), collaboration and video conference applications utilizing settled and flexible contraptions. CaaS has progressed along the same lines as Software as a Service (SaaS). Hence, it is insinuated as basically encouraged applications.

The development of different sorts of computing as personal computing, distributed computing, grid computing, ubiquitous computing, time sharing computing, cluster computing, client computing, for computing as shown by

Figure 1, within the final decade clears the way for a revelation of another modern sort of computing.

In shortsighted terms, cloud gives inaccessible computing and capacity administrations from a pool of shared assets to its shoppers. Much more exact definition is given by NIST [1] as: "*CC is a demonstrate for empowering omnipresent, helpful, on-demand arrange get to a shared pool of configurable computing assets (e.g., systems, servers, capacity, area, applications and administrations) that can be quickly provisioned and discharged with negligible administration exertion or benefit supplier interaction*".

Diverse CC services have been created to show the CC. For illustration, IaaS, PaaS, SaaS, CaaS, HaaS, BaaS, NaaS, OaaS, FaaS, DaaS, and XaaS [2]. Table 1 shows the list of the CC services at the side its space. The sending of assets built on pay-on-demand procedure pulls in most of the customers of information technology firms towards it. Indeed, a non-computer customer is production utilize of the arrangements advertised by cloud, now-a-days. This unused innovation brings out numerous points of interest like fetched effectiveness, expanded storage capacity, reinforcement and recuperation, persistent asset accessibility and area autonomy [3]. In middle of this giant use of assets from most of the CSPs (Cloud Service Providers), cloud clients are still confronting numerous loopholes. Cloud customers who need to store their bulk of delicate information within the public cloud for a passé of time are exceptionally more influenced by this matter. Unauthorized access and revelation could be a main anxiety for ensuring the information. Symmetric and asymmetric cryptography algorithms are for the most part utilized for security the cloud environment. Since security can be a main subject in cloud, these standard calculations can still be utilized for securing fragile data in cloud computing environment.

Secrecy of information put away in an open cloud is more concerned with how information is really ensured. The main anxiety is on the determination of encryption algorithms and key quality or key generation, when the customers' information is enthused to the cloud computing environment. These standards are truly depending on which CSP, the client is utilizing. The clients can ensure their information by directing on key determination or key generation with GA [4], since the encryption algorithms are generally selected by the CSPs. Symmetric key algorithms utilize a single key to secure communications and accomplish privacy, astuteness and confirmation. A private key could be a variable that's utilized with an algorithm to scramble and decode code. Whereas the algorithm doesn't ought to be kept secret, the key does. Using different symmetric key algorithms like AES, DES, triple DEA, Blowfish, and modes of operation used by most of the cryptographers or CSPs, Since of their speed and computational proficiency. Generating a key or choosing the key plays a critical part for key management system (KMS). The quantity of keys and their scale select the quality of the safekeeping handle in center of choice of encryption algorithms. In this way, key era is a fundamental errand for encrypting the information some time recently putting away into the cloud environment. Proposed article attempts to make the key utilizing GA for strengthen data security in cloud computing environment.

The taking after segments within the manuscript are organized in the way: Section 2 portrays a brief overview for recommendation of key management. Section 3 explain the related works. In section 4, brief description about genetic algorithm is given. Section 5 shows the working of the ACCA algorithm. Experimental results and discussions are given in section 6. The proposed work is concluded in section 7.

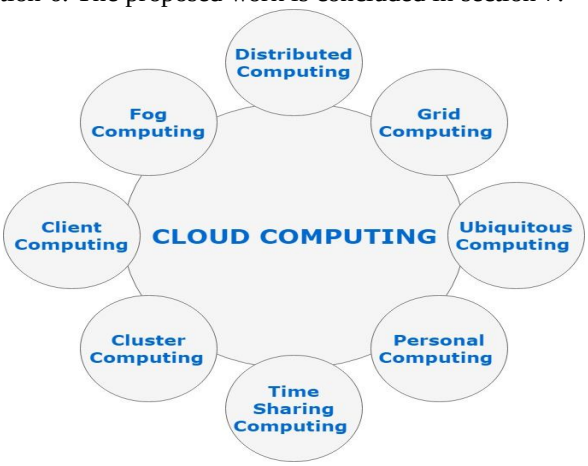

Figure 1: Types of Cloud Computing

Table 1: Cloud Computing Services

S. No.	Domain	Services
1	Computational Resources	IaaS (Infrastructure as a service)
2	Cloud Software Environment	PaaS (Platform as a service)
3	Communication	CaaS (Communication as a service)
4	Storage	DaaS (Database/ Development/ Desktop as a service)
5	Firmware/Hardware	HaaS (Hardware as a service)
6	Software applications	SaaS (Software as a service)
7	Business applications	BaaS (Business as a service)
8	Network applications	NaaS (Network as a service)
9	Organizational structure	OaaS (Organization as a service)
10	Framework	FaaS (Framework as a service)
11	Any other domain	XaaS (Anything as a service)

2. KEY MANAGEMENT

Key management implies securing encryption keys from misfortune, debasement and unauthorized access. Numerous forms can be utilized to control key management, tallying changing the keys regularly, and managing how keys are doled out and who gets them. In development, organizations must evaluate whether one key need to be utilized for all reinforcement sorts or within the occasion that each sort got to have it have key. The centrality of encryption key management cannot be overstated. Unless the creation, secure capacity, managing with and eradication of encryption keys

are carefully checked, unauthorized parties can choose up get to them. When keys are misplaced or debased, it can lead to misfortune of get to systems and data, as well as make a framework totally futile unless it is reformatted and reinstalled.

The correct administration of cryptographic keys is basic to the compelling utilize of cryptography for security. Keys are closely resembling to the combination of a secure. In the event that a secure combination is known to a foe, the most grounded secure gives no security against infiltration. So also, destitute key management may effortlessly compromise solid calculations. Eventually, the security of data secured by cryptography specifically depends on the quality of the keys, the adequacy of components and conventions related with the keys, and the assurance managed to the keys. All keys ought to be secured against adjustment, and secret and private keys got to be secured against unauthorized revelation. Key management gives the establishment for the secure key era, capacity, dissemination, utilize and devastation of keys.

Clients and designers are displayed with numerous choices in their utilize of cryptographic instruments. Improper choices may result in a dream of security, but small or no genuine security for the tradition or application. Fig.2 gives establishment information and builds up frameworks to support fitting choices when selecting and utilizing cryptographic mechanisms. This suggestion does not address the implementation points of interest for cryptographic modules that will be utilized to realize the security prerequisites recognized.

Key management taxonomy is composed for a few distinctive gatherings of people and is partitioned into three parts:

Part 1: It is aiming to prompt designers and system administrators on "best practices" related with key management as shown by Figure. 2. Cryptographic module designers may advantage from this common direction by getting a more prominent understanding of the key management highlights that are required to back particular, expecting ranges of applications. System administrators may utilize this archive to decide which setup settings are most suitable for their data. Part 1 of the Recommendation:

- Defines the security administrations which will be provided and key sorts which will be utilized in utilizing cryptographic mechanisms.
- Provides foundation data with respect to the cryptographic algorithms that utilize cryptographic keying material.
- Classifies the distinctive sorts of keys and other cryptographic data agreeing to their capacities, indicates the assurance that each sort of data requires and distinguishes strategies for giving this protection.
- Identifies the states in which a cryptographic key may exist amid its lifetime.
- Identifies the large number of capacities included in key management.
- Discusses an assortment of key management issues related to the keying fabric. Themes examined incorporate key utilization, cryptoperiod length, domain-parameter approval, public-key approval, responsibility, review, key management framework survivability, and direction for cryptographic algorithm and key estimate selection.

Part 2: Common Organization and administration necessities, is aiming fundamentally to address desires of framework proprietors and supervisors. It gives a system and common direction to back building up cryptographic key management inside an organization and a premise for fulfilling the key management angles of statutory and approach security arranging necessities for government organizations.

Part 3: Implementation-Specific Key Management direction, is aiming to address the key administration issues related with right now accessible implementations.

3. RELATED WORK

3.A. GA used for Encryption and decryption

"GA-based symmetric key cryptosystem for encryption and decoding" proposed by Sindhuja and Pramela [5]. The basic content and the client inputs are changed over into content network and key framework individually. By applying the straight substitution work, the intermediate cipher is delivered. A matrix is created by including the content matrix and key matrix with an added substance. The GA processes, crossover and mutation are connected on the middle cipher which comes about on last cipher content. Taken after by genetic crossover and mutation, the proposed algorithm does the substitution.

Dutta [6], utilized the idea of GA with algorithm/pseudo arbitrary work for scrambling and unscrambling the information stream. The encryption prepare is connected on a binary record. It can be connected for any sort of content as well as mixed media information. In this pseudo 5 diverse keys are utilized: one is for separating the smooth content into pieces. Moment and third keys are utilized for creating algorithm arbitrary arrangement for hybrid process.

"Encryption and code breaking of picture is done utilizing the concept of GA" by Goyal and Kumari [7]. Anticipation of data from robbery and harm utilizing the genetic operators as crossover and mutation are executed to create modern encryption strategy. There is no critical contrast within the distinctive highlight of both decrypted and encrypted images.

3. B. GA for cloud encrypted data

Pawar and Mathai [8] proposed an algorithm i.e., HVCEGA, gives most safekeeping through "multi-layer encryption and diminishes computation complexity using GA". A securing cloud-based information encryption innovation which encrypt the information utilizing cross breed algorithm is displayed. A crossover approach is more dependable and more grounded sufficient to supply the security of information. Avalanche impact and amount are the limits for which execution has been associated with ongoing encryption method at computation time.

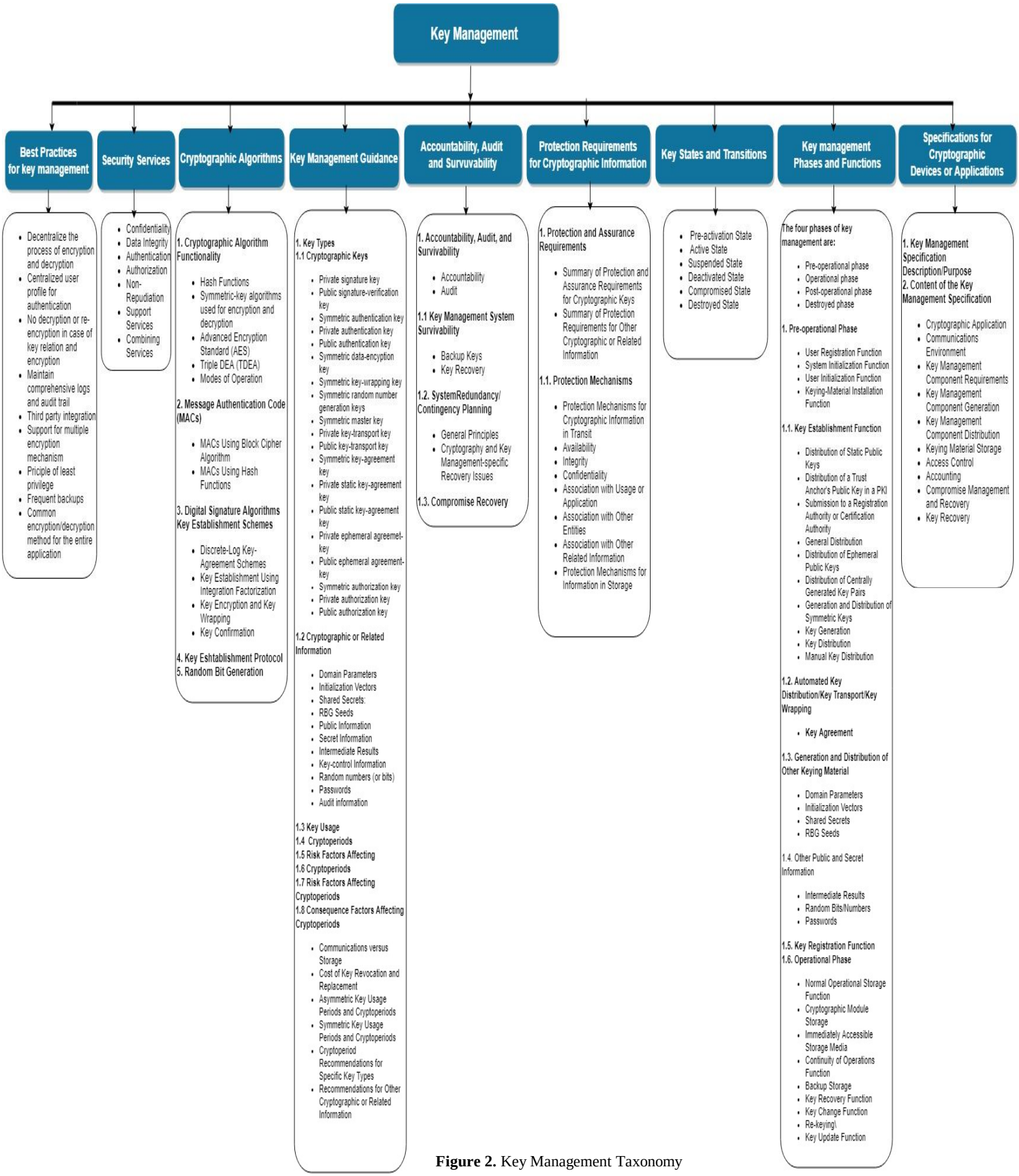

Figure 2. Key Management Taxonomy

Chandrasekaran and Hitaswi [9] planned "a security component for progressing the security of cloud information". The bio-inspired GA is utilized within the process. This process may be a combination of GA and attribute-based encryption. The information has got to be scrambled some time recently it is stored on the cloud. This setting goads to utilize GA for the generation of perfect key for encrypting the sensitive data to be put absent inside the cloud environment. Hence, the CSP (cloud service provider) is uninformed of the information which is put away and there is no data leakage.

3. C. GA for Key generation

Naik and Naik [10] have completed an endeavor to misuse the assertion included in crossover and mutation shapes for making an asymmetric key combine for encryption and decryption of messages. The assess of the secret key and the quality of the calculation lie on the crossover centers and mutation centers. At the side these focuses the alter calculate and unpredictable byte is utilized inside the generation of a private key. In this way, the algorithm utilized four crossover centers, three mutation centers and a single self-assertive byte and a stage calculate.

Jamal and Jawaid [11] conveyed a strategy constructed on the hypothesis of ordinary assortment to create the key solid and nearly unusual. This procedure finds the finest fit component inside the atmosphere which productions GA to attain the over mission. The imaginative strategy of key generation in addition outlined with its utilization. To accomplish in fact more guidelines of safekeeping, DES cipher bundle has been utilized for certification and endorsement.

4. GENETIC ALGORITHM

GA have demonstrated to be a well-suited procedure for tackling chosen combinatorial issues. When solving real-world issues, regularly the most assignment is to discover a legitimate representation for the candidate arrangements. Randomized search and optimization algorithm are also known as GA. The application of GA is inspected to set up the finest and more randomized key for the cryptographic algorithm. GA is a function that reproduces the method of characteristic choice within the field of AI. GA is utilized to investigate and optimize the issues arrangements. Fundamental operations of GA are reproduction, crossover, and mutation. GA is considered as heuristics-based look approach algorithm where chromosomes are treated as the foremost constraint.

There are a few distinctive sorts of crossover operator capacities as shown by Figure.3, but the sorts accessible depend on what illustration is utilized for the people. For the twofold string individuals, one-point, two-point, and uniform crossover work, mutation is connected. The reason of the mutation machinist is to reenact the impact of translation blunders that can happen with a horrendously moo probability when an individual is changed. Mutation administrator for binary strings may be a bit inversion infers '0' would change into '1' and vice versa.

IV. A. Genetic Algorithm/Pseudo Code

Step 1: The preliminary population of chromosomes.

i. generation = 0 Seed population
While not (termination condition) do
Generation = generation + 1

Step2: Do the fitness calculation for the generation iteration.

Step 3: Three major steps i.e., Selection, crossover (single point) and mutation are the operators of GA which are implemented in Python

i. Roulette Wheel method is used for the selection of chromosomes for the succeeding generation, which is more possible to be nominated in fitted forms.
ii. Crossover between any two chosen chromosomes is done to generate two relatives.
The probability pc is settled as crossover rate and associated on the arbitrarily selected point of the coordinate of chromosomes.
iii. The mutation rate pm is set for substitution.

Step 4: Chromosomes in the form of new set are swapped in the ongoing population.

Step 5: Jump to Step 2 till it reaches the n^{th} (for example 165^{th}) repetition.

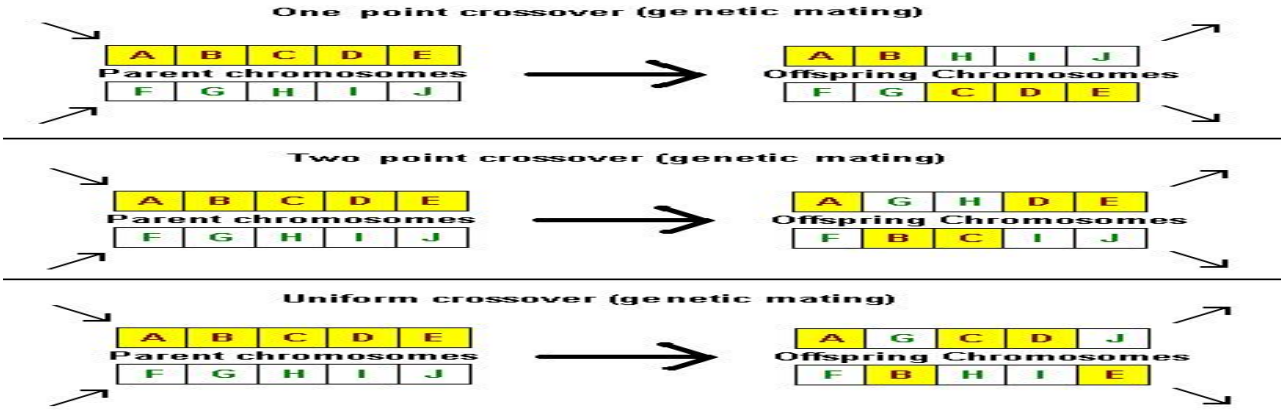

Figure 3. Type of Crossover [12]

4. B. Cloud Key Generation Genetic Algorithm (CKGGA)

Following is the proposed algorithm which is utilized to form the perfect key through the strategy of Genetic algorithm (As shown by Figure. 4).

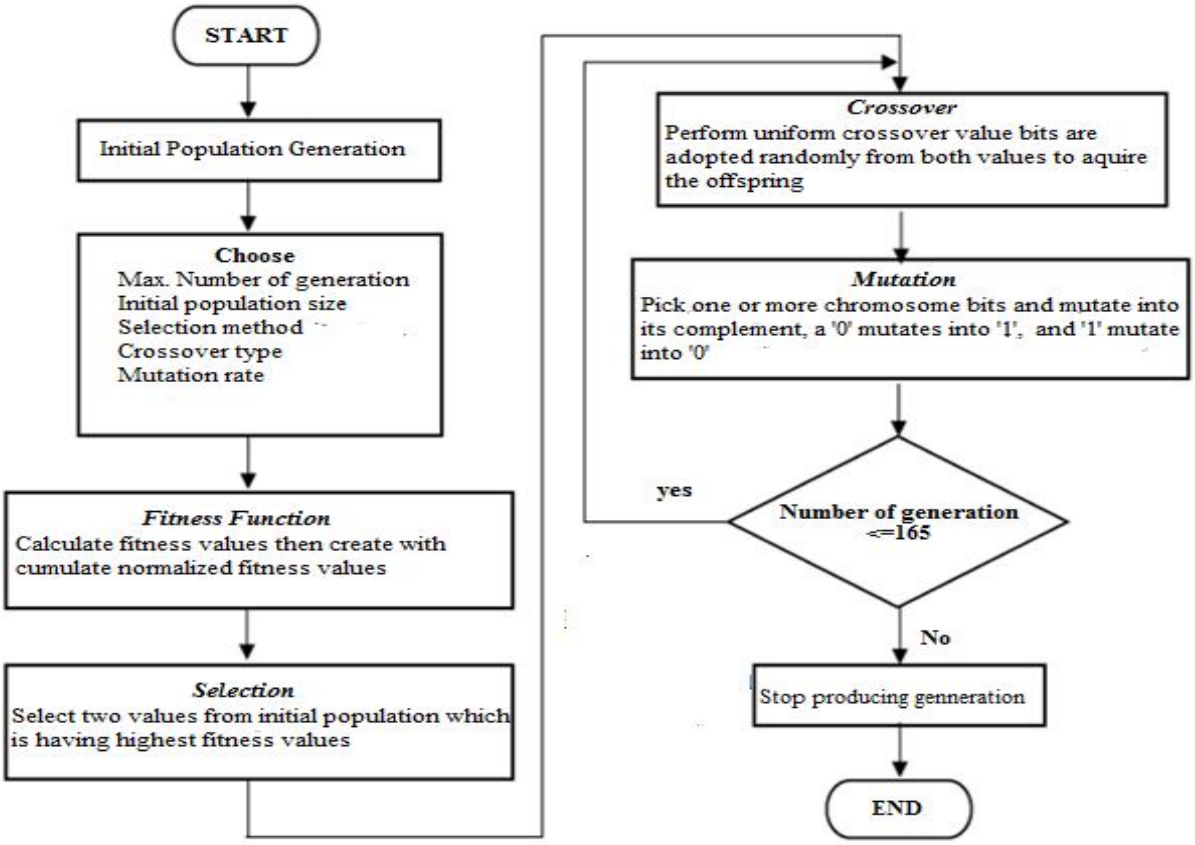

Figure 4. CKGGA-A flow diagram

Key generation may be a critical task within the handle of encryption. It is too hard to decrypt the cipher content, the more grounded the key, i.e., encrypted content. Genetic algorithm could be a portion of developmental calculations uncommonly utilized for advancement issues. To discover the leading fit key in GA is used for the cryptographic algorithm [11]. To bring ideal arrangement within the given arrangement space the 3 major phases included within the handle of GA makes it more less demanding. The ACCA algorithm is used to encrypt the key instead of the information. The symmetric key algorithms as AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, and Triple DEA etc., is lookup the encrypted key by ACCA algorithm. the key produced or selected for encrypting customers information is vital, since cloud clients store expansive volume of delicate information.

4. C. Representation of GA

Keys or chromosomes of the proposed algorithm CKGGA is spoken to as binary numbers (0's and 1's). Mostly, the keys lie to the chromosomes as machine number or binary numbers. Keys may be a decimal number, hexadecimal number, octal number and a set of character, etc. [13]. A previous setup a few time as of late conducting the investigate is done. Table 2 shows the exploratory setup.

Table 2: Exploratory Setup

Domain	Ranges and selection method
Population size	10
Selection method	RWS
Crossover method	Single point crossover
Crossover rate	0.5
Mutation rate	0.25
No. of iterations	165

5. THE WORKING OF ACCA ALGORITHM

The upgraded form of RSA deviated key algorithm is the ACCA algorithm which employments the numerical idea called addition chaining to diminish the period went through for encoding and decoding. To advance the individual measured duplications is the main objective of using addition chaining concept [14]. The ACCA concentrates on limiting the measured duplication individually.

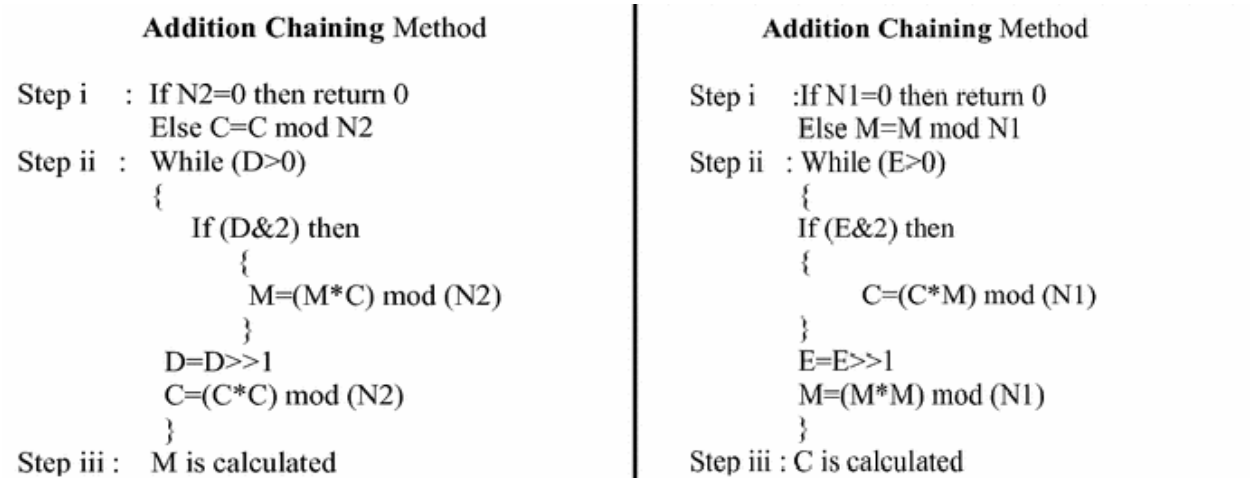

Figure 5. Working of ACCA algorithm

The ACCA shows the working of addition chaining method as shown by Figure.5. For encryption and decryption there are two keys i.e., E and D are produced by using ACCA. $C = M^E$ mod (N1) is a generalized equation using to encrypt the plain text, is succeeded through expansion chaining method in ACCA. Explained idea is additionally utilized for decoding procedure. GA created a key i.e., given as input to the ACCA algorithm for encryption and decryption process. This procedure of creating the key reinforces the procedure of encryption.

6. DISCUSSIONS AS WELL AS EXPERIMENTAL RESULTS

The CKGGA, a proposed pseudo code is executed by Python 3.7.4 stage. The RWS (Roulette wheel selection) is a selection method for initial population based on the wellness check. For crossover operation after the determination strategy, two chromosomes are selected in arbitrary.

Table 3: Key generation at Generation # 0

S. No	Chromosome	Key Generation	Fitness
1.	0	[1, 1, 0, 1, 0, 1, 0, 1, 0, 0]	7
2.	1	[1, 1, 0, 0, 1, 0, 1, 1, 0, 0]	7
3.	2	[0, 0, 1, 1, 0, 0, 1, 1, 1, 1]	6
4.	3	[1, 1, 1, 1, 0, 0, 0, 0, 0, 0]	6
5.	4	[0, 0, 0, 1, 1, 0, 1, 1, 0, 1]	5
6.	5	[0, 0, 1, 1, 0, 0, 0, 1, 1, 1]	5
7.	6	[0, 0, 1, 0, 1, 0, 1, 0, 1, 0]	4
8.	7	[0, 1, 1, 0, 0, 1, 1, 0, 0, 1]	3
9.	8	[0, 0, 1, 0, 1, 0, 1, 0, 0, 0]	3
10.	9	[0, 0, 1, 1, 0, 0, 0, 0, 0, 1]	3

Table 3 shows the fittest chromosome fitness i.e., 7 at generation 0 for the target chromosome [1, 1, 0, 1, 0, 0, 1, 1, 1, 0].

Table 4: Key generation at Generation # 1

S. No	Chromosome	Key Generation	Fitness
1.	0	[0, 1, 0, 1, 1, 0, 1, 1, 1, 0]	8
2.	1	[1, 1, 0, 1, 0, 1, 0, 1, 0, 0]	7
3.	2	[0, 0, 0, 1, 0, 1, 1, 1, 1, 0]	7
4.	3	[1, 1, 0, 0, 0, 0, 1, 1, 0, 1]	7
5.	4	[1, 0, 0, 1, 1, 0, 0, 1, 1, 0]	7
6.	5	[0, 1, 0, 0, 0, 1, 0, 0, 1, 0]	5
7.	6	[0, 1, 0, 1, 0, 1, 0, 0, 0, 0]	5
8.	7	[1, 0, 1, 1, 1, 0, 1, 0, 0, 0]	5
9.	8	[0, 1, 1, 0, 0, 1, 1, 0, 1, 1]	4
10.	9	[1, 0, 1, 0, 1, 0, 0, 1, 0, 0]	4

Table 3 shows the fittest chromosome fitness i.e., 8 at generation 1 for the target chromosome [1, 1, 0, 1, 0, 0, 1, 1, 1, 0].

Table 5: Key generation at Generation # 165

S. No	Chromosome	Key Generation	Fitness
1.	0	[1, 1, 0, 1, 0, 0, 1, 1, 1, 0]	10
2.	1	[1, 1, 0, 1, 0, 0, 1, 1, 0, 0]	9
3.	2	[0, 0, 0, 1, 0, 0, 1, 1, 0, 0]	7
4.	3	[1, 1, 0, 0, 0, 0, 0, 0, 1, 0]	7
5.	4	[0, 1, 0, 1, 1, 1, 0, 1, 1, 1]	5
6.	5	[0, 0, 1, 1, 0, 0, 1, 0, 0, 1]	4
7.	6	[0, 1, 1, 0, 1, 1, 0, 0, 1, 0]	3

8.	7	[0, 0, 0, 1, 0, 1, 0, 0, 0, 1]	3
9.	8	[0, 0, 0, 0, 1, 1, 0, 0, 0, 0]	2
10.	9	[0, 0, 0, 0, 1, 1, 0, 0, 1, 1]	2

Table 5 shows the fittest chromosome fitness i.e., 10 at generation 165 for the target chromosome [1, 1, 0, 1, 0, 0, 1, 1, 1, 0], which is our target chromosome. After 1st and the 165th iteration the keys which are generated as shown by table 3 and table 5 correspondingly. This key is continuously the ideal arrangement within the look space. Generated key [1, 1, 0, 1, 0, 0, 1, 1, 1, 0] by CKGGA is given to the ACCA for encryption. It is exceptionally clear that the Key [1, 1, 0, 1, 0, 0, 1, 1, 1, 0] is joined after the last iteration as shown in table 3 and table 5 with the help of three GA steps i.e., crossover, mutation, and selection.

6. A. ILLUSTRATION

Input	Encoded key value	Decoded key value
[1, 1, 0, 1, 0, 0, 1, 1, 1, 0]	[0, 0, 0, 1, 1, 0, 1, 0, 0, 1]	[1, 1, 0, 1, 0, 0, 1, 1, 1, 0]

The encrypted values of the key [1, 1, 0, 1, 0, 0, 1, 1, 1, 0] depicts by table 5. Decrypted key is given as input to the ACCA algorithm, which encrypt the key [1, 1, 0, 1, 0, 0, 1, 1, 1, 0] with diverse key sizes of it possess. The mixed regard of the key done by ACCA is utilized as key for any one of the symmetric key algorithms like triple DEA, AES, DES, and Blowfish, etc. Since key plays an important part in encryption handle particularly for enhancing data security in cloud environment, the idea of GA is utilized for producing the key in a more secure manner. Table 5 uncovers the truth that indeed the key [1, 1, 0, 1, 0, 0, 1, 1, 1, 0], when it is encrypted it generate a number depending upon the key bits of ACCA. It is more grounded sufficient for encrypting a bigger capacity of delicate information of the cloud customers.

7. CRITICAL ASSESSMENT AND CONCLUSION

The utilization of CKGGA produces a perfect key from the course of action space. ACCA algorithm generates the uncommonly long encrypted key which is utilized for encrypting the data. The comes almost of both CKGGA and ACCA propose that the key period and security level of encryption handle is overhauled. Clarified concept cleared the means for the cloud client to store their encrypted information in cloud capacity in a most secure manner. The key bit gage of ACCA can still be expanded to incite a more noteworthy and secured encrypted key. Key management taxonomy comprises of three parts. Part 1 gives common direction and best practices for the administration of cryptographic keying fabric. Part 2 gives direction on approach and security arranging necessities for government organizations. At long last, Part 3 gives direction when utilizing the cryptographic highlights of current systems. At long last, the algorithm is executed in Python 3.7.4 stage and connected for the encryption and decryption of a content record and a Word Document. From the execution investigation, it is concluded that the proposed algorithm accomplishes least encryption and decoding time than the existing cryptographic algorithms. By utilizing proposed algorithm, the time required in encryption, decoding and key era based on the key degree of cloud computing can be progressed and as well makes strides inside the typical get to time for the clients inside the cloud. Future direction contains the following steps:

1. Strengthen the proposed algorithm i.e., CKGGA with fuzzy logic to enhance the data security in cloud environment.
2. Utilize Machine Learning (ML) with fault to set the strategy for the malware attacker to find the mystery key, and to permit legitimate security affirmation on our organization.
3. Identifies the states in which a cryptographic key may exist amid its lifetime.
4. Identifies the large number of capacities included in key management.

REFERENCES

1. P. Mell and T. Grance, **"The definition of cloud computing",** NIST Special Publication, Washington, 2011.
2. C. N. Hofer, and G. Karagiannis, **"Cloud computing services: taxonomy and comparison",** J Internet Sev Appl, 2011, 2:81-94.
3. Fera M.A., Manikandaprabhu, C., Natarajan, I., Brinda, K. and Darathiprincy, R., **"Enhancing security in cloud using trusted monitoring framework",** Elsevier Procedia Computer Science, Vol. 48, pp.198–203, 2015.
4. Mather, T., Kumaraswamy, S. and Latif, S., **"Cloud Security and Privacy",** 1st ed., O'Reilly Media, Inc. Sebastopol, 2009, California.
5. Sindhuja, K. and Pramela, D.S., **"A symmetric key encryption technique using genetic algorithm",** International Journal of Computer Science and Information Technologies, Vol. 5, No. 1, 2014, pp.414–416.
6. Dutta, S., Das, T., Jash, S., Patra, D., and Paul, P., **"A cryptography algorithm using the operations of genetic algorithm & pseudo random sequence generating functions",** International Journal of Advances in Computer Science and Technology, Vol. 3, No. 5, 2014, pp.325–330.
7. Kumari, A. and Goyal, S., **"Encryption and code breaking of image using genetic algorithm in MATLAB",** International Journal of Advance Research in Computer Science and Management Studies, Vol. 4, No. 7, 2016, pp.357–361.

8. Pawar, S. and Mathai, J.K., **"A novel approach to design hybrid vigenere caesar cipher encryption with genetic algorithm (HVCEGA) for data security in cloud computing",** International Journal of Computer Science and Network, Vol. 5, No. 4, 2016, pp.699–705.
9. Hitaswi, N. and Chandrasekaran, K., **"A bio-inspired model to provide data security in cloud storage",** IEEEXplore Digital Library, 2017, pp.203–208.
10. Naik, P.G and Naik, G.R., **"Asymmetric key encryption using genetic algorithm",** International Journal of Latest Trends in Engineering and Technology, Vol. 3, No. 3, 2014, pp.118–128.
11. Jawaid, S. and Jamal, A., **"Generating the best fit key in cryptography using genetic algorithm",** International Journal of Computer Applications, Vol. 98, No. 20, 2014, pp.33–39.
12. Rajat Jhingran, Vikas Thada, Shivali Dhaka, **"A Study on Cryptography using Genetic Algorithm",** International Journal of Computer Applications (0975 – 8887), Volume 118 – No.20, May 2015.
13. Zomaya, A.Y., Lee, R.C. and Olariu, S., Schedulers that Evolve, Technical Report 96-PCRL-02, **"The University of Western Australia",** Perth, 1996, Western Australia.
14. Schneier, B. (1996) Protocols, **"Algorithm and Source Code in C"**, 2nd ed., John Wiley & Sons, Inc, USA.