IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis on Data accountability and data security analysis by using imperialist competitive key generation algorithm

Yanala Gowtham Reddy

Electrical and Electronics Engineering, National Institute of Technology Calicut.

ABSTRACT

People are storing documents in a variety of cloud storage services (CSs). Cloud storage services are used to protect and transfer people's personal data. Before data is stored in the cloud, it is encrypted. To maintain data security, clients manage encryption and decryption operations. Existing members who leave and newly join the organization pose a threat to data confidentiality and privacy. They are more lethal. The researcher concentrates primarily on external adversaries since they place their confidence in internal entities. Numerous security issues can arise as a result of the presence of multiple users in a group. As a result, it is vital to provide users with an effective attack detection approach in order for them to maintain control over their data. Consequently, in order to overcome all of these issues, we've proposed a highly centralised system of monitoring the actual use of users' data in the cloud, based on an imperialist competitive key generation algorithm (CCIAI-ICKGA). Public and private keys are generated independently by each customer. As part of the cypher text-policy attribute-based encryption process, keys are generated (CP-ABE). Key generation is accomplished through the usage of ICKGA and a trapdoor generator.

1. INTRODUCTION

A primary goal of cloud computing is to deliver the best possible service to all of its customers. The safety and privacy of cloud data is a major issue that must be addressed. Traditional database solutions are incapable of perfectly storing and investigating massive amounts of data. Keeping customer data safe and secure on the cloud has become a top priority due to the explosion of startups, small businesses, and huge corporations using the cloud. Encryption of network traffic around virtual machines (VMs) and cloud data centres is essential for security and privacy. When confidential data files and their privacy is breached, the catastrophe process will be severely impacted. During disaster recovery, the security of the hardware and software in the cloud is a top priority. Data and applications in a network are usually stored and retrieved remotely from data centres. As a result, data and virtual computers must be protected during the disaster recovery process. Cloud computing characteristics are designed to provide clients with security and secrecy.

In the field of information technology, cloud computing is sometimes referred to as virtual computing. It's a sort of computing that uses virtual data centres and demands the utmost level

of privacy protection. The data of the owner that is outsourced to the cloud is referred to as "privacy." A breach of data privacy can occur due to a variety of threats, as well as data misuse by attackers. One method of preventing data leaks and misuse is the duplication of data. Keeping data private in the cloud is a major challenge. During the auditing process, the TPA must not be given access to any confidential information. Encryption technology is employed by the cloud service provider to secure cloud data.

Concerns about security and privacy can be found in many different domains, from identity management to data protection to operations. Encryption and decryption of data files in transit and at rest are all part of maintaining privacy in the cloud. The safe storage of confidential data on cloud premises will be helped by strong authentication systems and secure algorithms. Encryption and other security measures such as key management and policy enforcement are all instances of privacy-preserving approaches. Confidentiality relates to safeguarding data against illegal access by third-party users. Cryptographic tools are critical in cloud environments for maintaining the privacy and security of confidential data files.

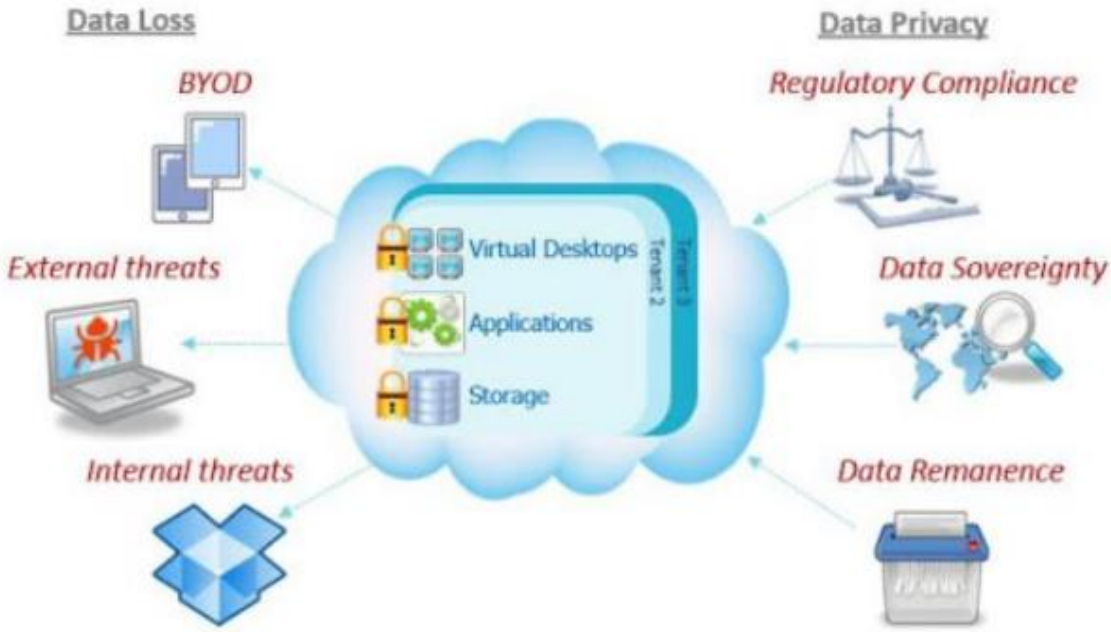

FIGURE 1: Cloud storage data security threads

In above figure illustrating that what are the threads and issues are facing by the cloud storage. Here clearly defining the internal threats, external threats, shared technology vulnerability, etc. that says whatever the data stockpile in cloud storage by people is already in high risk state.

2. LITERATURE REVIEW

To detect DDoS attacks, a machine learning methodology was devised by He and et.al (2017). With the system installed at the Cloud provider's end, early identification of DDoS attacks coming from Cloud virtual machines is made possible. To prevent network packages from being broadcast outside of the Cloud server, statistical data from the hypervisor and virtual machines is used. Detection performance is used to determine which algorithm is best. It is relatively readily enhanced to launch large-scale DOS attacks. It has no adverse effect on the system's performance [1].

The master key is generated by the log harmonizer. It is a verified element. The ICKGA key pair's decryption key is rigorously adhered to. This is due to the accountability of log decryption. On the client side, decryption is

performed in the event that a path exists between log harmonizers. A secure key exchange is used to send keys from the harmonizer to the client. For unreliable paths between the log harmonizer and client, decryption is performed on client side. The harmonizer uses a secure key exchange mechanism to transfer keys to the client. Push and pull auditing approaches are among the auditing methods that are utilised (Punitha and Indumathi 2018) [2].

Bio-inspired anomaly-based application layer for DDoS detection was developed in 2019 by Sreeram and Moore. Based on bio-inspired bat algorithms, DDoS attacks on the Hypertext Transfer Protocol (HTTP) can be identified (HTTP). The system's performance is evaluated using data from the Center for Applied Internet Data Analysis (CAIDA). The frequency with which HTTP fooding attacks are discovered is in line with predictions [3].

S. Atiewi et al., (2020) abstracted an IOT based multifactor authentication and light weight cryptography encryption scheme in cloud storage environment. IOT device are organize as follow of sensitive data and non-sensitive data. The sensitive data is split in two and each part encrypted by separated encryption algorithms (RC6, Fiestel) and data deposit on private cloud storage to ensure the high security. Non-sensitive data is encrypted by single algorithm (AES) as stored in the public cloud. Multifactor authentication ensure through the trusted authority. Using the identification of user’s such as IP, password and biometricsin [4].

X. Wang and Y. Su (2020) proposed a new encryption method for audio which dispense reliability state high. Preliminary value that presents in chaotic controlled by hash value on the audio and then making unpredictable chaotic trajectory, DNA coding is used tomystifying and scatter the data (audio). Encryption scheme is used for single and dual format audio [5].

D. Changet al., (2020) demonstrated a cancelable multi-biometric technique through the use of a fuzzy extractor in conjunction with an unique bit-wise encryption scheme to generate cancelable biometric templates. The protection scheme for biometric template framed as irreversibility, renewability and accurate recognition of biometric scenes. The scheme that safeguard without supplementary noise that means of bit errors is executed in preserved template [6].

J. Mech. Cont.& Math. (2019) responses, similar to that of multi-objective optimization and scheduling problems of existence has it. Evolutionary algorithms are inherently efficient for identifying these multiple responses simultaneously. Bee colony algorithm, ant colony optimization method, genetic algorithm, and imperialist competitive algorithm are all examples of evolutionary algorithms [7].

3. SYSTEM ANALYSIS

This work discusses the CCIAIICKGA in general. As a result, it also discusses security monitoring, which meets the needs of cloud data owners' security standards. Assaults are detected using a DWENN classifier, a dynamically weighted ensemble neural network For the CCIAI-ICKGA framework and attack detection, please refer to Figure 2. The creation of JAR archives and data conversion are two methods used to convert files. In the JAR file, you'll find a collection of common security policies. It specifies how the cloud server and other parties can gain access to data. Each user's public and private keys are generated by CP-ABE using ICKGA. The trapdoor generator protects data integrity at both the user and cloud levels. The decryption of log files for the purpose of integrity checks is another application of this technology. Detection of attacks is also part of this process. JAR files make it easy to implement scalable data traceability and integrity. Log harmonizers are used to execute audits of files with the help of the data owner or other authorised stakeholders. In the event of log file corruption, the log harmonizer receives the error correction information.

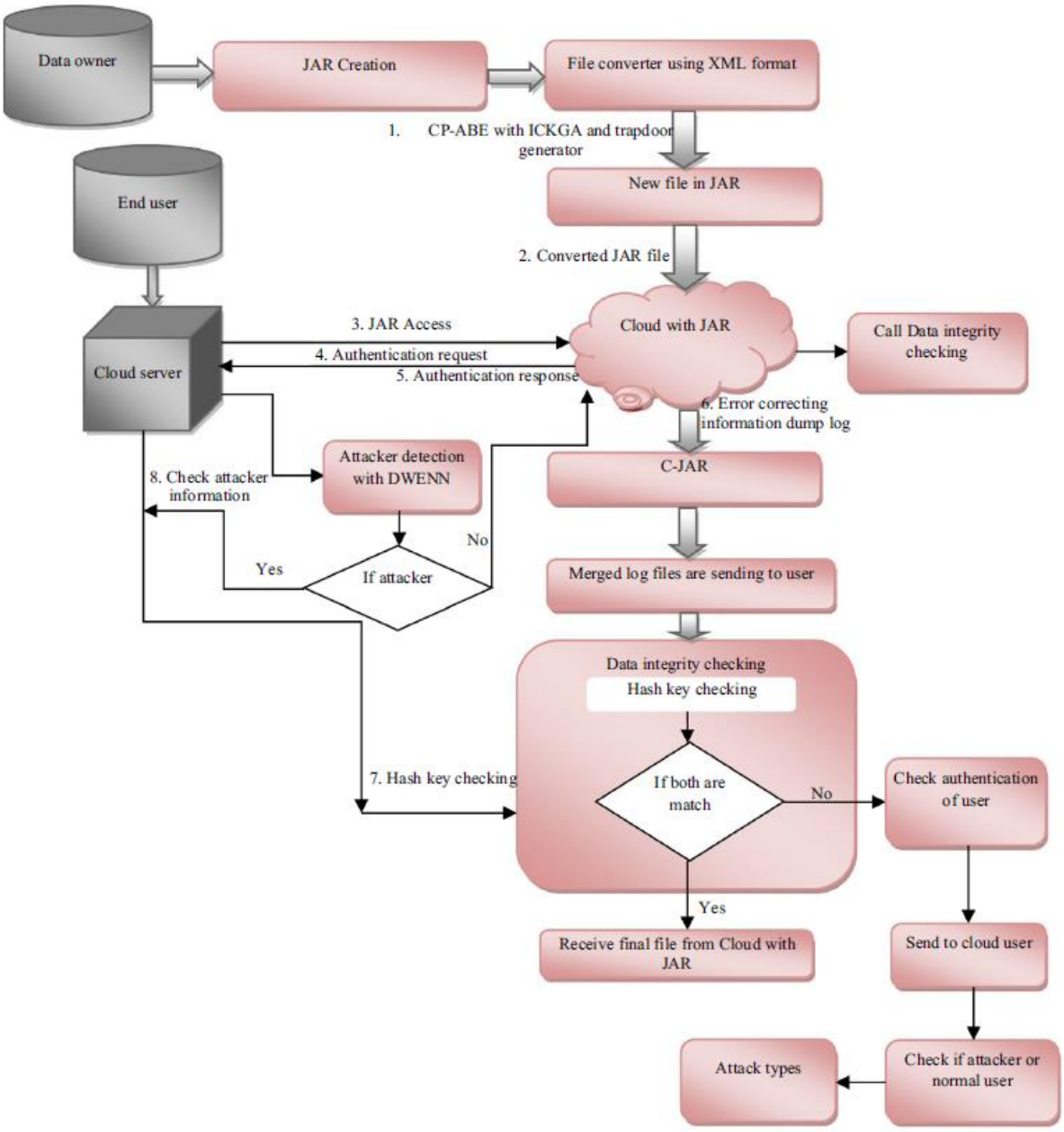

Fig. 2 Overview of the CCIAI-ICKGA threat detection framework.

Privacy is one of the most difficult aspects of cloud computing to address. During the auditing process, the TPA must not be given access to any confidential information. Encryption technology is employed by the cloud service provider to safeguard cloud data. Data files must be encrypted and decrypted at rest or while being transmitted via the cloud in order to maintain confidentiality. The safe storage of confidential data on cloud premises will be helped by strong authentication systems and secure algorithms.

3.1 Imperialist Competitive Algorithm

Optimization difficulties can be solved with the help of the imperialist competitive algorithm. Imperialist competitive algorithms have a number of advantages over other nature-inspired algorithms. Included is a novel concept: it is based on the fact that human social activity is more intelligent than his biological behaviour. Fast convergence: capability of optimising functions with a large number of variables. The matching, competition, and revolution are the algorithm's fundamental pillars. Indeed, this method examines optimization solutions in the

form of countries and attempts to enhance them incrementally and iteratively in order to arrive at the ideal solution.

Parameters

1- Initial Population: Some of these countries will be created as the initial population. Ncountry of initial country

2. Choice: Nimp must be selected as the imperialist of the best members of this population (countries with the least amount of cost function).

3. Remnants: Ncol the remaining states are colonies that each belong to a system.

4. Dividing colonies: Each imperialist is assigned a proportionate number of colonies based on its might. The cost of normalising them, at the expense of all imperialists, is as follows.

$$C_n = \max_i\{c_i\} - c_n$$

Where c_n is the nth imperialist cost, $\max_i\{c_i\}$ is the highest cost between the imperialists and c_i the normalized cost of this imperialist. The imperialist is more expensive and weaker imperialist have less normalization cost. Calculate the relative power of normalization Each imperialist is divided between the imperialist sites at the cost of normalization and division of the colonial countries.

$$P_n = \left| \frac{c_n}{\sum_{i=1}^{N_{tmp}} c_i} \right|$$

4. METHODOLOGY

CCIAI-ICKGA, an imperialist competitive key generation algorithm (CCIAI-ICKGA) and attack detection are proposed in this paper to monitor cloud users' data usage in a highly centralised manner. Both a public and a private key pair are generated for each user. The keys are generated using the CP-ABE (cypher text-policy attribute-based encryption) method. The keys are generated using the ICKGA and trapdoor generators. Users' data and cloud server data are equally safe with the trapdoor generator. Classifiers based on dynamically weighted ensemble neural networks are used to identify threats (DWENN). Updating the log records structure provides further assurances of integrity and validity. By conducting security analysis, further probable attacks are found. The unique experiments' results provide an in-depth analysis of the system's performance.

The distributed network system consists of a large number of data centers and intelligent learning agents that move through the data center. Learning is one of the important capabilities of smart agents, so in many cases an intelligent agent is expected to be able to learn and improve its performance based on its results, in addition to other capabilities. On the other hand, in many cases, a system where learning is possible is often regarded as an intelligent system. Thus, agent learning is one of the characteristics that need special attention. Learning methods in intelligent agents are presented using machine learning methods and their adaptation to operating conditions and multi-agent systems.

BKGA generates a key for the client, which will be used to construct a JAR file to store its client data. Access control rules for cloud servers and other information partners (clients, businesses) are contained in a JAR file that can be opened and read by anybody. It's up to him to get the JAR file out to his Cloud Service Provider (CSP). A trusted certificate expert must verify the CSP using OpenSSL-based declarations before it can be approved for inclusion in JAR stages 3–5 which are discussed in below section.

4.1 Automated logging mechanism

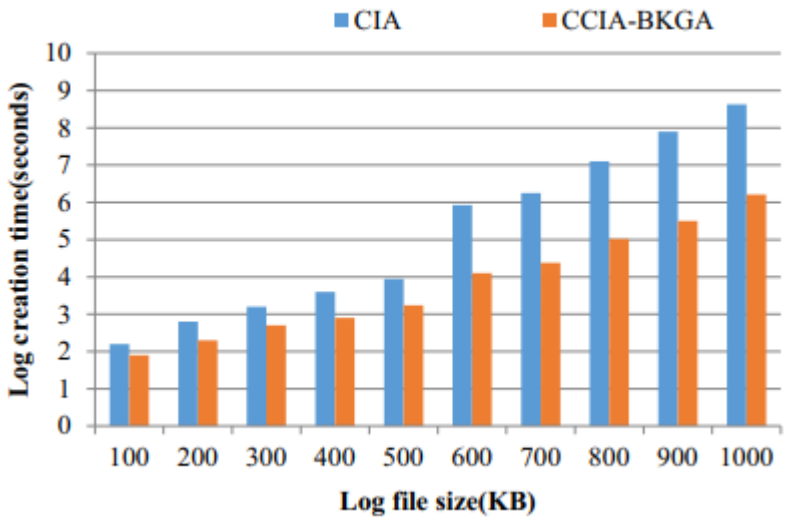

Fig. 3 Time to create log files of different sizes

The logger segment is a standalone Java JAR archive that stores a client's data items and associated log documents. As illustrated in Figure 3, the suggested JAR file contains one external JAR that contains at least one internal JAR.

4.2 JARs availability

To protect against attacks on disconnected JARs, the CCIA incorporates a log harmonizer that performs two critical functions: one is to trade with duplicate JARs and the other is to parse through defiled logs. Each log harmonizer is in charge of replicating logger components that contain the same set of information items. The harmonizer is run as a JAR file. It does not benefit the client's information objects that are being dissected, but it does have class records for both server and client forms used to connect to its logger components. The harmonizer stores the error correction data sent by its logger segments, as well as the client's BKGA decryption key, for the purpose of decoding log records and dealing with any duplicate records. Copies of the client's information JARs were identified as duplicates. Thus, the client's information is capable of being integrated with the logger segment in an information JAR document, and the logger is duplicated alongside the client's information.

4.3 Algorithm steps involved:

Step 1. For the encryption and decryption processes, a hybrid real-binary concatenated coding approach is used.

Step 2. As a technique for constraint handling, the penalty function technique is used.

Step 3. The initial nations are produced and the objective function values for each are computed. According to each nation's power value, which is a normalised formula for the objective function value, the stronger countries are chosen to be imperialists, while the weaker ones are chosen to be colonies. Once colonies are randomly assigned to each imperialist, empires are formed.

Step 4. Within each empire, assimilation occurs. According to the fundamental ICA, imperialists try to absorb their colonies and make them identical to themselves, with the goal of bringing the solutions designated by colonies closer to the solutions represented by imperialists. This demonstrates that the assimilation of real

variables and the actual ICA algorithm are identical.

Step 5. Generally, insurgent administrators are completed on a small number of states in each domain. There are several methods for achieving the transformation, including swap, inclusion, inversion, and annoyance. At the moment, settlements are being displaced by newly formed states. The populace assigns ratings to those revolutions.

Step 6. (Colonialist update). Only in front of a large number of administrators inside each domain, the expenditure of a large number of settlers must be recalculated to determine whether there is any state whose cost is less than the colonialist's cost. Currently, settlements will seek a good pace colonialist in the current realm and vice versa.

Step 7. Process the general expense of each realm.

Step 8. (realms rivalry). The most fragile village among all realms will be chosen and eventually incorporated into a domain. The blessed domain is chosen in an ad hoc manner; that is, the extraordinary realm does not always complete the initiatory.

Step 9. (removal of weakest empire). Imperialism will be eradicated from the human population once it has lost all of its colonies.

Step 10. (termination criterion). If there is just one empire that controls all of the colonies, or if decades have passed, the termination criterion is used.

4.4 Disassembling attack

The security of the suggested technology is demonstrated in this section. JAR file's logger can be dismantled by identifying the most likely assaults. It also removes or destroys any log records that provide useful information. This is a particularly serious attack in the context of the CCIAI-ICKGA system. Once the JAR fles are undone, the attacker has access to the public CP-ABE key used to encrypt the logs. In order to read log records, an attacker must have access to a private key or be able to decipher encrypted data. Selective plaintext attacks can be used to gain access to encrypted log records connected with an attacker's activity, as well as simple texts, in order to compromise log fles confidentiality. Using a random oracle model, the CCIAI architecture protects cypher text and some plaintext.

5. RESULTS AND DISCUSSION

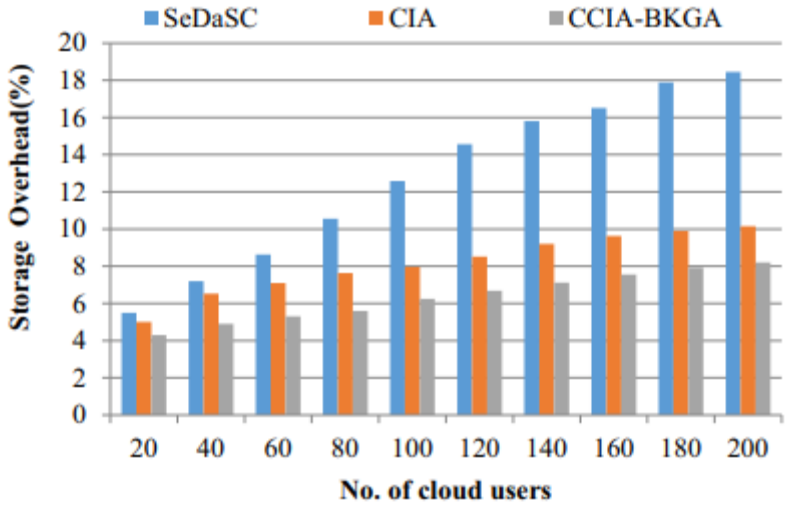

Fig. 4 Storage overhead at different cloud users.

The proposed CCIA-BKGA system for authentication has a low storage cost because all that needs to be accumulated is the data contained in the files themselves and the linked logs. Compressing input documents into the compressed format (XML) is another function of JAR.

Figure 4 depicts the findings. There is an 8.21% overhead for 200 cloud users of the CCIA-BKGA framework, a 10.15 percent overhead for the CIA framework and an 18.45 percent overhead for the SeDaSC algorithm.

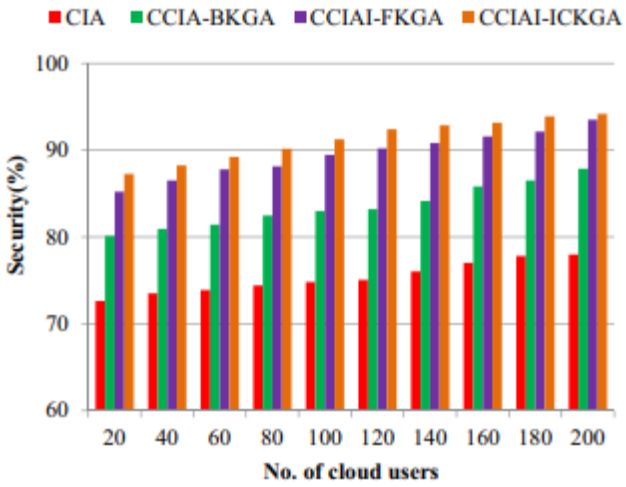

Fig. 5 Cloud security at diferent cloud users vs. key generation methods

Fig. 5 depicts the various levels of security provided by various authentication methods. To put this in perspective, the proposed CCIAI-ICKGA system has an overall security level of about 6.2% for 200 cloud users, whereas the existing CIA framework has a security level of about 10.15%, the CCIA-BKGA algorithm has an overall security level of about 8.21% and CCIAI-FKGA has a security level of about 6.7%.

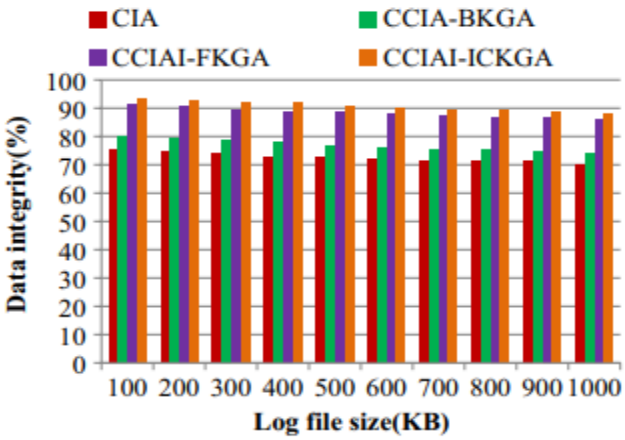

Fig. 6 Data integrity at diferent cloud users vs. key generation methods

To demonstrate the impact of log file size on data integrity, consider the results shown in Figure 6. While the proposed CCIAIICKGA system boasts a data integrity level of around 93.52 percent for a 100-KB file, other methods like the CIA framework, CCIA-BKGA algorithm, and CCIAIFKGA system all boast data integrity levels around 80.15 percent and 91.25 percent, respectively, for the same 100-KB file size.

CONCLUSION

Cloud providers should not be able to access sensitive data without compromising the data. The cloud data storage is protected by the use of cryptographic techniques. Accessing data files in the cloud relies heavily on cloud encryption and decryption. This study proposes an attack detection and CCIAIICKGA mechanism for automatically logging any attempts to access cloud data. Owners of data can verify its accuracy with CCIAIICKGA's process, which also emphasises the importance of strong back-end security when necessary. CCIAI-ICKGA architecture has been shown to be vulnerable to a variety of non-trivial attacks, including those launched by malicious users or compromised by flaws in Java's running environment (JRE). When an attack is detected, DWENN classifier is used to identify it within the Java Runtime Environment (JRE). For the most common assault, DWENN classifer automatically secures. By encrypting the log file, attackers can't make any unauthorised changes. In the proposed CCIAI-ICKGA architecture, unauthorised copies of users' data can be detected and prevented by the CCIAI-ICKGA design.

REFERENCES

1. He Z, Zhang T, Lee RB (2017) Machine learning based DDoS attack detection from source side in Cloud. Proceedings of the IEEE 4th international conference on cyber security and cloud computing (CSCloud), pp. 114–120
2. Punitha AAA, Indumathi G (2018) Centralized cloud information accountability with bat key generation algorithm (CCIA-BKGA) framework in cloud computing environment. Cluster Computing, pp. 1–12
3. Sreeram I, Vuppala VPK (2019) HTTP food attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Appl Comput Inf 15(1):59–66
4. S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.
5. X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," in IEEE Access, vol. 8, pp. 9260-9270, 2020, doi: 10.1109/ACCESS.2019.2963329.
6. D. Chang, S. Garg, M. Hasan and S. Mishra, "Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3152-3167, 2020, doi: 10.1109/TIFS.2020.2983250.
7. J. Mech. Cont.& Math. Sci., Vol.-14, No.-6 November-December (2019) pp 205-225
8. Hosseini S, Al Khaled A (2014) A survey on the imperialist competitive algorithm metaheuristic: implementation in engineering domain and directions for future research. Appl Soft Comput 24:1078–1094
9. Hwang K, Li D (2010) Trusted cloud computing with secure resources and data coloring. IEEE Internet Comput 14(5):14–22
10. Jaeger PT, Lin J, Grimes JM (2008) Cloud computing and information policy: computing in a policy cloud. J Inf Technol Politics 5(3):269–283
11. Khabbazi A, Atashpaz-Gargari E, Lucas C (2009) Imperialist competitive algorithm for minimum bit error rate

beamforming. Int J Bio-Inspired Comput 1(1–2):125–133
12. Khan AN, Kiah MM, Madani SA, Ali M, Shamshirband S (2014) Incremental proxy re-encryption scheme for mobile cloud computing environment. J Supercomput 68(2):624–651
13. Kiraz MS (2016) A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing. J Ambient Intell Hum Comput 7(5):731–760
14. Ko RK, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS (2011) Trust Cloud: a framework for accountability and trust in cloud computing. IEEE World Congress on Services (SERVICES), pp. 584–588
15. Maqsood I, Khan MR, Abraham A (2004) An ensemble of neural networks for weather forecasting. Neural Comput Appl 13(2):112–122