IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 5, Issue 5, May 2025

Impact Factor: 5.731

Improved Cloud Security Analysis and Monitoring Robot Key using Homomorpic Encryption

Dr. K. Thamizhchelvi
Assistant Professor, Department of Computer Science
S.I.V.E.T College, Gowrivakkam, Chennai
thamizhchelvi.k@gmail.com

Abstract: *Cloud computing plays major role in the development of accessing cloud user's document and sensitive information stored. It has variety of content and representation. Security of the documents in the cloud is a challenging aspect. Information security attains a vital part in cloud security management. It involves actions intended to reduce the adverse impacts of such incidents. To access the documents stored in cloud safely and securely, we introduce access control based on cloud users to access user's document in the cloud. To achieve this, we need to combine security components (e.g. Access Control, Usage Control) in the Security document to get automatic information. We are proposing Role Key Homomorphic Encryption Algorithm (RKHEA) to monitor the cloud users who access the services continuously. This method provides access creation of session based key to store the singularized encryption to reduce the key size from random methods to occupy memory space. It has some terms and conditions to be followed by the cloud users and also has encryption method to secure the document content. Hence the documents are encrypted with the RKHEA algorithm based on Service Key Access (SKA). Then, the encrypted key will be created based on access control conditions. Our analytics result shows enhanced control over the documents in cloud and improved security performance.*

Keywords: Cloud Security, Homomorphic Encryption, RKHEA, SKA

I. INTRODUCTION

Cloud computation is capable of accessing a lake of resources maintained by a third party owned via the Internet. It's a new technology but server virtualization is not a way to provide computational devices based on the existing technologies. Cloud computing is a computing long-term dream for a user, making software more attractive to a service and is designed to purchase the way hardware and the ability to transform a large part of the IT industry. But worry is the most important security amongst this and how the service provider is committed to maintaining it. Generally, for example, casual users, analysts, cloud computing companies with different intentions to cloud, which is a cloud of various clients. Cloud clients need to find a way to connect the security and performance. Innovative ideas for new Internet services require developers to continue to pay for their services and the cost of human capital to drive it to the massive capital expenditures. This cryptographic solution application is apparently the application can quickly and easily integrate without any changes. Data privacy in cloud computing is a major security concern. The cloud has kept valuable data on their site rather than the gap.There is no idea of the location of the consumer data the timely transfer, the cloud movement, etc.

Decoding is the resistance of the encryption which changes over encoded information into justifiable frame. Encryption is generally utilized by governments and armed force related establishments which convey an abnormal state of private data. Keeping in mind the end goal to decode the encryption, a key which is frequently called decoding key is required for switch operations. Without a right encrypted key, a message may not be download from service based key access (SKA). In such conditions, decoding must be extricated from the encryption designs be that as it may, lost the decrypted key for the most part result in loss of decoded message. In this way, an unscrambling key must be secured and ensured legitimately. Security is considered one of the most important aspects of daily calculations. Cloud computing infrastructure is not fully dependent on security and most of them use new technologies and services. Cloud

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 5, May 2025
Impact Factor: 5.731

computing concerns about many important issues and data security, hopes, expectations, and arrangements. This provides protection from others to protect their information. Along the improvement of the security, the protection information also high due to storage keys. If the user wants to download any file they want to claim for that particular file, then this request will automatically be supplied to the customer to receive a secret code when checking their mail and download. Their emails will be provided as part of the secret code verification process, and then the file will be downloaded.

Most of the movements do not know about security mechanisms implemented by service providers which occupy more memory space. The main damage can occur, and then the data encryption is not mentioned. To save the keys, a physical key management server can be installed on the user's campus. The encryption ensures that data or keys will protect the keys or they will not be exposed to the user's control. Thus, they do not need to worry about the lack of expensive resources, or a supply that is greatly popular and there is no greater chance for a service that does not expect their reputation for their popularity and disappearance of customers and revenue. Data is sometimes changed before it can be used. One of the reasons is that different attributes can be measured in different sizes, eg, centimeters and kilograms. Whereas in the cases where the value attributes differ widely from the attribute, these different characteristic scales dominate the results of the bunch, all the attributes that are the same at the level of data are common. Dynamic Provision allows to arrange the administrations regarding to present request required. As per, encryption is the change of any sort of information into a frame that is not reasonable.

II. RELATED WORKS

The main advantage of our program is that the balance modules activate servers to update themselves. Also, the client must download the transfer balance modules residing in any data (or balance) servers to prevent tags. Finally, they examine the safety and efficacy of our program [3]. Cloud plat forming has been used on a platform to increase cloud computing prices and utilize a three-tiered web of traditional enterprises, and some video streaming applications cloud data centers require innovative approach in each case [6].

The solution is stimulated by the Sri Lankan military's support from the large scale and distributed cloud system in the creation and use of the application for use. This complex specialized platform requires ASM & A Services to describe a high level performance, and existing procedures require real-time warranties to implement software and real-time warranties, except for real resources, but automation is required, and requires always loaded servers and network These ratings are used to guide the cloud manager to the clouds distributed to use [3]Upload and download performance is based on the principles that take place simultaneously by distributing a subset of the file across multiple cloud providers that they consider [1]. Reliability tray [7] another important feature. To improve reliability, they propose a solution that is copied to the same subset of the file across various providers. Because the file is seated, a full file is distributed using the distribution, [9]. In our testing, performance improvements were provided and retirement was restored when retrieving files compared to a standard approach [10]. The upward time can run up to eight seconds for storage to run the results. With the expansion of cloud providers, the results are expected to improve. Cloud computing cloud servers enables outsourced users (customers) to their data. Safely distributed cloud storage plans make sure that many servers store these data on a reliable and unhampered [8] fashion. The idea of expanding this idea is to append only when they accommodate data and they identify some of the challenges. And then, they effectively address the challenges addressed to our secure distributed cloud storage plan not only as append [2].

III. METHODS AND IMPLEMENTATIONS

Homomorphic Cloud computing can protect the privacy of users of the encrypted user while performing the user's data. But it is not practical to use the wide range of cloud computing data and varied types of services. The service seems to be a good way to safeguard privacy by using encryption, especially outsourcing applications when dealing with data types, data size, etc. But as cloud computing data varies, how is it more challenging to use the simplest encryption in other ways. Particular defective encryption algorithm in a bid to simultaneously save its secrecy, a special property has an encryption system that has implemented computing on encrypted data; specifically, it encrypts input (ciphertexts) which allows computation, the secret key to secretly reconciling with any decryption or access, and returns to encrypt

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 5, May 2025
Impact Factor: 5.731

the desired result. There is a secure multi-party calculation based on an alternate secret sharing or other forms of encryption (possible non-formal encryption processes) for the simplified encryption. Provides a method to estimate a Boolean function without any party that can monitor circuit bits during protocol evaluation.

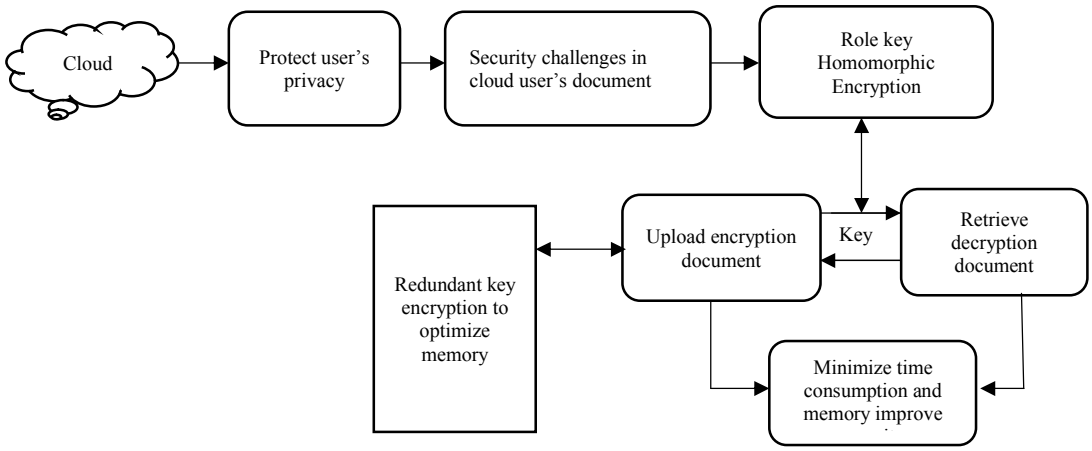

Fig: 3.1 Role key Encryption in cloud

We proposed Role key Homomorphic Encryption Algorithm to monitor the cloud users and who access the services continuously. In this method have some terms and conditions for cloud users and also developed encryption method to secure the document content for anonymous cloud users.

3.1 Redundant singularized Memory Optimized Secrete Key

First, a secrecy of cryptographic data encrypted was built. It can effectively work on encoding floating numbers to suit data service. However, many public key encryption schemes cannot be used to encrypt events such as a chip or cloud to be used to obtain partial information leaks on the secret information. Do not resist this kind of attacks side-by-side attacks, public key cryptography traditional protection model. In this analysis, we present a method to build key encryption and removal plans against key weak-leak attacks and linear-related attacks from both extractable hash source modes. The secret key is redundant to store uploading document as singularized storage on reduced pattern length to optimize memory storage.

3.2 Role key Homomorphic EncryptionAlgorithm

Step 1:

Encryption and Decryption (no of keys in Generated)
Start
Number and alphabetic formal [0-9, a-z], Formal = in

Step 2:

If (id==0)
{
Add Round Key (formal, w [0, Key-1])
For pattern key= 1 step 1
Split Number and alphabets (formal)
Data Rows Shift (formal)
Mix data columns and rows (formal)
Add pattern Key (formal, W [pattern key* (pattern Key +1)-1])
End for
Add pattern Key (formal, [w *NA, with doc(NA+1)*NA-1])
}

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 5, May 2025
Impact Factor: 5.731

Else
{
Out = formal
}
Step 3:
End

Extensive function of the encrypting algorithm varies depending on the variable and the key. Without the key, the document cannot be improved or decrypt.

3.3 Steps of proposed algorithm

Step 1: Key-based access document. Its functionality is similar to usernames and passwords, but the keys are primarily used by automated processes and single logon system administrators and power users.

Step 2: When user upload a document the encryption key will be generated through Role key Homomorphic Encryption Algorithm. Encryption key management Encryption keys protect the entire life cycle and protect them from loss or abuse also check the repeated bits of key resultant on storage be indexed in singular key.

Step 3: Singularized key storage reduce the security time consumption as well, memory optimized to reduce the storage memory space.

Step 4: When used retrieve document, the proposed algorithm used. After the encryption is completed the text will be changed to the cipher text. The cipher text should be decrypted, the proposed algorithm retrieved the original data obtained and the end.

IV. RESULT AND DISCUSSION

4.1 Analysis of time complexity

The time complexity parameter has been calculated by using upload and the request retrieve based on the number of users and the execution time of the individual are represented below: Time represented by T, Data analytics by DA, Trust Accuracy represented by TA

$$T = \frac{Doc\ upload\ + Doc\ retrive}{no\ of\ users\ a}$$

The figure given below shows the Time complexity by different comparisons as follows

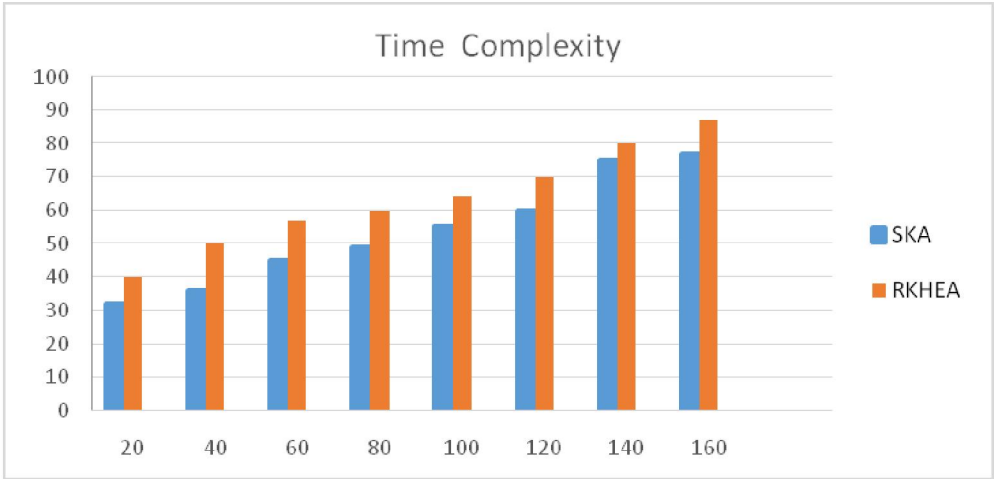

Figure: 4.1 Comparison of time complexity

Figure It has been shown to be a comparative result in a variety of systematic times, and suggests that the proposed RKHEA produced less complicated time.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 5, May 2025
Impact Factor: 5.731

USERS	SKA	RKHEA
20 users	32	40
40 users	36	50
60 users	45	57
80 users	49	60
100 users	55	64
120 users	60	70
140 users	70	75
160 users	77	87

4.1 Tableprocessed data, UN Processed data and Efficiency

Table represents the throughput and efficiency ratio of the different algorithmsSKA as 57 % and Hashing 87 % and the overall the proposed algorithm have the high throughput ratio and efficiency as compared with other techniques.

The resultant algorithm has been implemented and evaluated for its performance using the data being considered with previous clarification. The method has produced efficient results in all the factors considered.

4.2 Analysis of Integrity to security provision

The figure given below shows the false ratio accuracy by different comparisons as follows

4.2 Figure various dissimilar in Integrity to security provision

Figure 4.2 shows the comparative result on different methods. The proposed algorithm has produced high performance in integrity to security dissimilar than other methods.

USERS	SKA	RKHEA
100 Users	92	95
300 Users	112	110
500 Users	120	150

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 5, May 2025
Impact Factor: 5.731

4.2 Table Processed Data and Efficiency of packet processing.

4.3 Analysis of memory consumption under security key storage

The graph given below shows that,

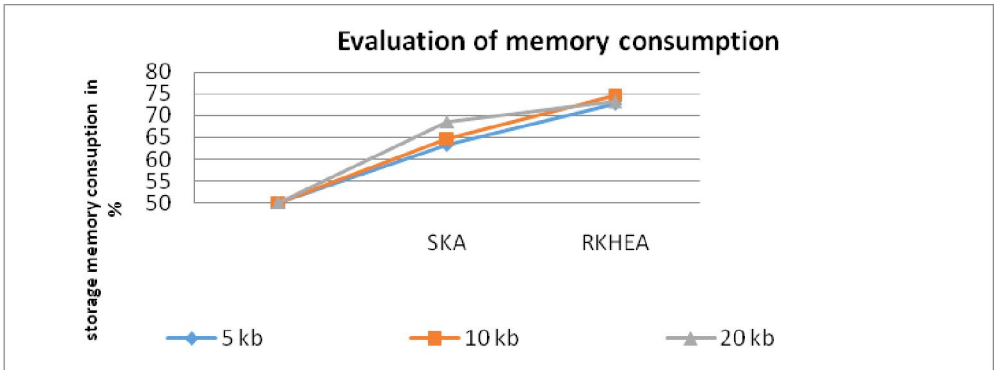

Figure 4.3: Memory consumption measure

Figure 4.3 presents the results of consumption in memory of performance analysis by various methods. The proposed method, by minimizing data replication and reducing memory consumption

Table 4.3: Memory consumption measure

Memory consumption measure in %		
Storage /methods	SKA	RKHEA
5kb	63.2	72.6
10kb	64,8	74.8
20kb	68.6	73.2

The above table 4.3 shows the key storage memory measures measures were compared, analyzing the performance of the amount of memory consumption.

V. CONCLUSION

Conventionally, Cloud computing is not widely advised because of the large size of data and different types of services. Homomorphic encryption protects the user's privacy when running user data in cloud computing. We proposed Role key Homomorphic Encryption Algorithm to monitor the cloud users and who access the services continuously. In this method have some terms and conditions for cloud users and also developed encryption method to secure the document content for anonymous cloud users as well as singularized key storage along security information to be stored in redundant memory to optimize the storage, So that the encryption of document creation will be combined with access control for better security.

REFERENCES

[1]. "Modeling and Optimization of Resource Allocation in Distributed Clouds," Atakan Aral, IEEE 2016.

[2]. "Handling Performance Sensitive Native Cloud Applications with Distributed Cloud Computing and SLA Management," CalinCurescu, Hjalmar Olsson, Dimitri Mazmanov, Andrew Ton, James Kempf. IEEE 2013.

[3]. "Distributed Shared Memory Programming in the Cloud," Tarek El-Ghazawi ,Vikram K. Narayana, and, Ahmad Anbar, IEEE 2012.

[4]. "Augmenting Performance for Distributed Cloud Storage," Carlos A. Varela, Matthew B. Hancock, IEEE 2015.

[5]. "An Efficient Secure Distributed Cloud Storage for Append-only Data," NishantNikam, Srinivasan Narayanamurthy,SushmitaRuj, BinandaSengupta,Siddhartha Nandi, IEEE 2018.

[6]. "Improving Hadoop Service Provisioning in A Geographically Distributed Cloud," Ling Liu, Kisung Lee, Sandeep Gopisetty, Yang Zhou, Aameek Singh, Qi Zhang, NagapramodMandagere, IEEE 2014.

[7]. "An Approach for Cloud Resource Scheduling Based on Parallel Genetic Algorithm," Rui Wang, HaiZhong, Xuejie Zhang,ZhongniZheng, IEEE 2011.

[8]. "Analysis of MapReduce Scheduling and Its Improvements in Cloud Environment," Sofia D'Souza, K. Chandrasekaran, IEEE 2015.

[9]. "Scheduling Parallel Tasks onto Opportunistically Available Cloud Resources," Lang Tong, Ting He, Shiyao Chen and Hyoil Kim, Kang-Won Lee, IEEE 2012.

[10]. "Workflow Tasks Scheduling Optimization Based on a Genetic Algorithm in Clouds," Zhang Xiaoqing, Yang Cui, IEEE 2018