https://doi.org/10.46335/IJIES.2022.7.7.3 **e-ISSN: 2456-3463**
Vol. 7, No. 7, 2022, PP. 12-19

International Journal of Innovations in Engineering and Science, www.ijies.net

A Study on Key Management Infrastructure in Cloud Computing Environmental Survey for Secured Communication

Mr. Ghanshyam S. Nikhade[1], Dr. Tryambak Hiwarkar[2]

[1]Student, [2]Professor, Sardar Patel University, Balaghat (M.P.)

shyamnikhade777@gmail.com

***Received on**: 15 June ,2022* ***Revised on**: 06July ,2022,* ***Published on**: 08 July,2022*

Abstract – *The term "cryptography," which literally translates to "secret writing," has emerged as the fundamental building block for supplying security for numerous communication applications. There is a need to conceal sensitive information, such as passwords, encryption keys, recipes, etc. in many applications, especially in group communication. Here, effective key management policies are needed to protect the group's confidential information. Because it can be exceedingly difficult to preserve a group's secret information, especially in two situations: when there are more group members and when they are dispersed across different locations with different defences in place. the cloud computing model, where application services are delivered online. A flexible, affordable, and tested platform for delivering commercial or consumer IT services over the internet is cloud computing. Along with more computer power, the cloud also offers network infrastructure that facilitates group communication scenarios. Several security methods are needed to communicate with the various cloud services and to store the data produced/processed by those services. This paper examines the fundamental issue of cloud computing key management in this context and provides support for communication between cloud cryptography clients and cloud key management servers. Cloud key management, including its development and subsequent use to lower infrastructure costs, hazards, and complexity associated with managing encryption keys, as well as to improve the functionality of both private and public storage clouds, is covered. This study explores an extensive assessment of current key management methods used to secure cloud computing.*

Keywords- Key management, Cloud computing, Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS)..

I- INTRODUCTION

A fundamental tool that facilitates communication between any two people over an unsecure communication channel is known as cryptography. The majority of communication programmes used today are built on group communication, which allows group members to communicate information among themselves. For instance, information exchange, video and audio conferences, and data transmission. A key component of group communication is security. Group communication security, or ensuring the authenticity, integrity, and secrecy of messages sent between members, will consequently turn into a crucial communication problem. An internet-based technology called cloud computing gives consumers access to on-demand IT infrastructure, which includes software, hardware, and applications. Customers of cloud computing benefit from the simplicity and low cost of adopting cloud-based apps.

A cryptographic key is much like the combination to a safe: if we have the right combination, it is easy to open a safe, but it's hard to open one without the right combination. Similarly, if we have the right key, decrypting an encrypted data is easy, but decrypting it is impractical without this key. If we are careless with the combination to our safe, someone else can easily use it to open our safe, and the protection provided by the safe is compromised. Similarly, the cryptographic keys that we use to encrypt data need to be handled carefully. If we are careless with them then the protection provided by encryption can be essentially eliminated. The details of how to handle keys properly enough to ensure that they shouldn't be compromised are all covered by key management. Both cloud users and providers must take precautions to prevent data theft and loss. Strong

https://doi.org/10.46335/IJIES.2022.7.7.3 **e-ISSN: 2456-3463**
Vol. 7, No. 7, 2022, PP. 12-19

International Journal of Innovations in Engineering and Science, www.ijies.net

encryption with key management is one of the fundamental processes that cloud computing systems should use to safeguard data, and it is strongly advised that both personal and business data be encrypted [1].

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service are the three main categories of services in cloud computing (SaaS). Based on this basic set of services, cloud computing offers many advantages, but it may also be exposed to many forms of assaults when it comes to security [2]. An analysis of the cryptographic operations that provide those security capabilities reveals that the management of cryptographic keys takes on an additional complexity in cloud environments compared to enterprise IT environments. Because (a) difference in ownership (between cloud Consumers and cloud Providers) and (b) control of infrastructures on which both the key management system (KMS) and protected resources are located in cloud.

The architecture in Figure 1 outlines the five major cloud actors: consumer, provider, broker, carrier and auditor. Each cloud Actor can participate in a transaction or process and/or performs tasks in cloud computing. According to [3] the cloud actors are defined as below:

Cloud Consumer: A person or organization that maintains a business relationship with, and uses service from Cloud Providers.

II-CLOUD COMPUTING ARCHITECTURE:

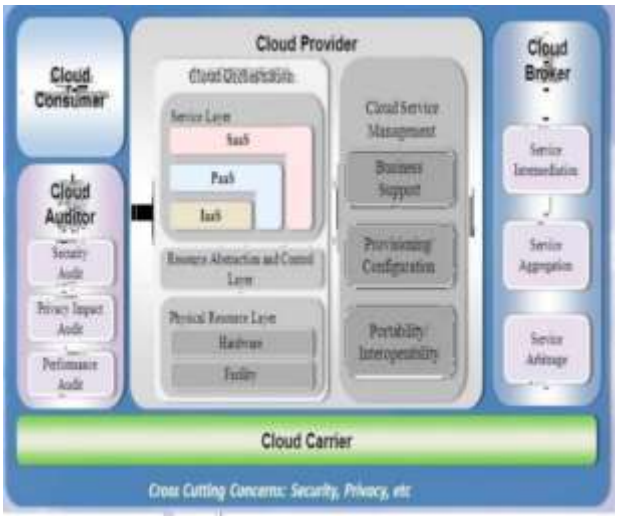

Fig 1- Cloud computing security reference architecture

Cloud Provider: a person, group, or other entity in charge of providing a service to interested parties.

Cloud Auditor: A third party with the ability to independently evaluate the performance of information system operations, the security of the cloud implementation.

Cloud Broker: An organisation that controls the use, performance, and delivery of cloud services as well as mediates agreements between cloud providers and cloud consumers is referred to as a cloud broker.

Cloud Carrier: An middleman that connects and transports cloud services from cloud providers to cloud consumers is known as a cloud carrier.

III-SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing provides efficient, flexible and cost effective alternative to hosting their own computing resources to the organization. However, hackers, attackers and security researchers have shown that this model can be compromised and is not 100 present secure. Cloud computing provides a virtual infrastructure and services to external user according to the requested services. It reflects the idea of IT infrastructure as a service, which enables computing services like water, electricity and other public service, access resource on-demand and pay for use. Security in general, is related to the important aspects of confidentiality, integrity and availability. Thus they become building blocks to be used in designing secure systems. There are many security threats which emerge inside or out-side of cloud providers/consumers environment. The security threats can be broadly classified as below according to [4].

1. Privacy and confidentiality: These concepts refer to only authorised individuals or systems having access to protected data. Because there are more parties, devices, and applications using the cloud, there is a greater risk of data compromise because there are more points of access. As more people have access to the data as a result of data control being delegated to the cloud, there is an increased risk of data compromise.

2. Multitenancy: This term describes resource sharing in the cloud. Shared elements of the IS include memory, software, networks, and data. Hardware is not divided, despite the virtual isolation of users.

3.Object reusability: It is an important characteristic of cloud infrastructures, but reusable objects must be carefully controlled else they create a serious vulnerability.

4.Data reminisce: It is the residual representation of data that have been in some way nominally erased or removed. Data confidentiality could be breached unintentionally, due to data reminisce.

5.Integrity: A key aspect of Information Security is integrity. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication.

https://doi.org/10.46335/IJIES.2022.7.7.3 **e-ISSN: 2456-3463**
Vol. 7, No. 7, 2022, PP. 12-19

International Journal of Innovations in Engineering and Science, www.ijies.net

6.Authorization: It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. Due to the increased number of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.

7.Availability: It refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system must be able to function normally even if there is a chance of a security breach.

8.Service Interruptions Even with cloud architecture, service hijacking is nothing new, but hostile attempts like phishing, fraud, and the exploitation of software flaws still provide hackers an advantage. If an attacker is able to acquire an organization's login credentials, he can change data, eavesdrop on transactions, and steal data. Even worse, an attacker can replay sessions, reroute a company's clients to unauthorised websites, or use botnets to execute a distributed denial of service (DDoS) or denial of service (DoS) assault.

IV-KEY MANAGEMENT INFRASTRUCTURE IN CLOUD COMPUTING

Cloud key management Infrastructure consists of cloud key management client (CKMC) and cloud key management server (CKMS) [5]. CKMC exits in cloud applications, serving for three fundamental cloud service model, including Software, Platform or Infrastructure (as a Service). CKMS interacts with CKMC using cloud key management interoperability protocol, which interacts with symmetric key management system (SKMS) and public key infrastructure (PKI) using symmetric key management protocol and asymmetric key management protocol respectively, as shown in Figure 2.

The cloud Key Management Interoperability Protocol (CK-MIP) establishes a single comprehensive protocol for communication between cloud key management servers and cryptographic clients. It solves the important need for a thorough key management protocol by proposing a protocol that can be used by any cloud cryptography client, from multi-tenant implementation to cloud storage. It is integrated into the cloud computing system, which can deploy efficient unified key management for all their cryptographic capabilities, including digital signatures, certificate-based device authentication, and encryption. A cloud computing system will be able to combine key management into a single enterprise key management system thanks to vendor adoption of CKMIP. While improving operational controls and security policy governance, it lowers operational and infrastructure expenses.

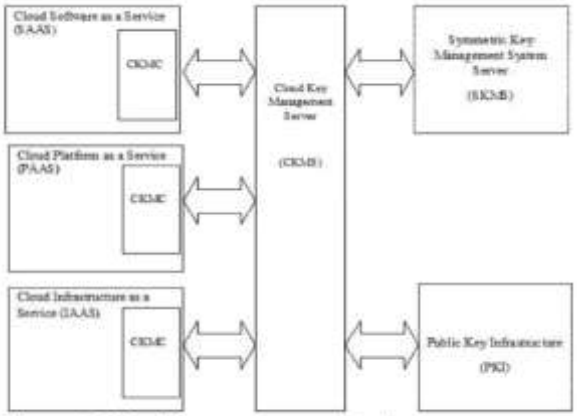

Figure 2 Cloud key management infrastructures

by any cloud cryptographic client, ranging from multi-tenant implementation to cloud storage, it addresses the critical need for a comprehensive key management protocol. It is built in the cloud computing system, which can deploy effective unified key management for all their encryption, certificate-based device authentication, digital signature and other cryptographic capabilities. Through vendor support of CKMIP, a cloud computing system will be able to consolidate key management in a single enterprise key management system. It reduces operational and infrastructure costs while strengthening operational controls and governance of security policy.

V-SURVEY OF EXISTING KEY MANAGEMENT FRAME WORK FOR CLOUD COMPUTING

The authors have taken into account applications involving a number of cloud servers that cycle through a series of online periods during which the servers communicate, followed by offline periods during which the servers are idle in this section describing the solutions that have been suggested in [6]. Servers must safely store important data, such as cryptographic keys, throughout the offline times. Applications like this include numerous instances of outsourcing safe multiparty computing to the cloud, including in particular a number of online auctions and benchmark calculations using private inputs. The author refers to the protocol that emerged from the aforementioned conversation as PCKM, short for cloud key management protocol. It consists of two procedures to be carried out by each server, one before entering an offline period (shutdown) and another before returning to the next online period (wakeup). The entire protocol consists of several rounds, each round r consisting of four phases: An online phase where the application is running, a shutdown phase where the servers run the PCKM shutdown procedure, an offline phase with no computation, and finally a wakeup phase where the servers run the PCKM wakeup procedure to restore the secret files.

In [1] authors describe cloud computing security by using the Key management covers all the details of how to handle keys carefully enough to ensure secrecy. Only difficult mathematics that are beyond the comprehension of the majority is used in encryption. Key management is significantly more challenging because it combines people, processes, and technology. A very high level of protection is offered via encryption. Federation is a term used to explain how several computer systems can cooperate. Federation in the context of key management refers to the process through which several apps can obtain keys from a single key server. This essay also explains the idea behind fully federated key management's necessity for cloud computing. The cloud's federated identity management and hierarchical identity-based cryptography (HIBC) illustrate how the system may produce and give users and servers access to the public and private keys. The proposed method in this research provides advantages over the current Ws-Security methodology in terms of streamlining public key distribution. and reducing [SOAP] header size[7].

In [3] author suggested that the security is an important issue to provide a security for this cloud, author introduces a novel method for securing cloud by providing multicast key for each user. It will be a dynamic session key which will vary in the time of period. Whenever a new user enters into the cloud the new key will be generated. It will withstand for a time period. After that time period the user should renew the key for the further usage of the cloud. Multicast Security key management protocols to support a variety of application, transport, and network-layer security protocols. It also defines the group security association (GSA) and describes the key management protocols that help establishing a GSA. The methodology and recommendations presented in this paper allow for a modular and adaptable construction of group key management protocols for a number of situations that are particular to applications demand. In order to provide secure one-to-many, many-to-many, or one-to-one communication,

MSEC key management methods may be utilised. According to the suggested plan in [4], the main security concern with cloud computing is that the cloud provider must make sure that their infrastructure is safe and that they can prevent unwanted access to data from third parties, other clients, or even rogue cloud employees. The author of this study discusses cloud security services, such as key agreement and authentication utilising elliptic curve diffie-hellman (ECDH) and symmetric bivariate polynomial-based secret sharing.. Also describes the designing of the secure cloud computing (SCC), which requires a trusted third party (TTP) and also extends to multiserver SCC (MSCC), where each multi-server system contains multiple servers to collaborate for serving applications [8].

In [9] the characteristics of large scale cloud storage system and the security threats it faces, this paper explores the cloud storage key management mechanism, and focuses on solutions that can meet the demands such as large scale and high performance in the cloud storage key management. Based on the hyper elliptic curve and hypercombined public key technology, a key management scheme in cloud storage is designed. It solves the large-scale key management issues of cloud storage system, and fixes the security vulnerabilities of collusion attack in the existing key management scheme.

In [5], the author present cloud key management infrastructure (CKMI), CKMIs creation and subsequent adoption by cloud computing vendors which will reduce the complexity of encryption Mohan Naik R et al. 56 management by building interoperability into the key management environment. By enabling support for interoperability between cloud cryptographic clients and cloud key management servers, CKMI reduces infrastructure costs and the risks in adopting cryptographic solutions as an essential element of securing information, identities and infrastructure. The cloud storage provides a lot of benefits to its users by significantly reducing the burden of storage and computation [10]. However unlike traditional data storage systems, cloud data is produced, transferred and stored at off-premise multi-tenant storage systems. This increases the vulnerability of unauthorized disclosure and unauthorized modification [10]. Therefore, it will cause some serious data security issues for its users if adequate security and privacy solutions are not in place. [10] addresses the security concerns with using a cloud storage service to store private and sensitive data and proposes a PKI-based cryptography system. Building a safe storage system with some functionality on the cloud is still a difficult task, according to [8] authors.

Because data cannot be transferred to the user without first being retrieved and verified offline, existing techniques are inefficient and slow. It focuses on developing a safe cloud storage system that enables data transfer functionality using elliptic curve cryptography and notifies the data owner when an attacker tries to change the data any malpractice and system gives multilevel security. In [9] author suggested that the cloud storage is a massive and public accessible storage available for use on internet. Since the number of users and data access request will be massive, a good performance improvement algorithm is needed. In this paper a technique of using a smart object placement is presented. Genetic algorithm is used to optimize the placement function in order to gain a better average access speed for any storage object. The experimental results show an obvious performance increases due to a better object placement. Using genetic algorithm generating a random workload for each object and place the storage object uniformly on each storage node. The experimental result also shows that the average access

https://doi.org/10.46335/IJIES.2022.7.7.3 **e-ISSN: 2456-3463**
Vol. 7, No. 7, 2022, PP. 12-19

International Journal of Innovations in Engineering and Science, www.ijies.net

time for the users has been improved. In the future, more detail assumption such as CPU and I/O speed will be taken into consideration which allows, obtaining a better performance enhancement algorithm The weakness in user's authentication process and lack of effective security policy in cloud storage leads to many challenges in cloud computing [13].

This work suggests a method that uses elliptic curve cryptography to authenticate users to cloud servers in addition to providing security for user private data storage and access [13]. The user logs onto the cloud and establishes his identity first in [13]. After authentication, the user encrypts and decrypts the data using the symmetric key algorithm and the ECDH key exchange. With shorter key size and greater algorithm security, the ECC and ECDH algorithms offer the same level of security as existing public key cryptosystems. According to [14], the integration of artificial intelligence in user profile systems enhances security by enabling security systems to operate both pro-actively and reactively.

In [14] authors focus on designing a User Profiling System for Cloud environment using artificial intelligence techniques and studies behaviour of User Profiling System and proposes a new hybrid approach, which will deliver a comprehensive user profiling system for Cloud Computing security. From this analysis there are some research gaps in previous experiments. A new approach by using Fuzzy guided GAGE for designing user profiling system to rectify their respective problem to provide proper information about user's behaviour, which results in not enabling the security mechanism to work in effective way and deliver a comprehensive user profiling system. Whereas GAGE to malicious or highly malicious user will change their characters after some limitation to safe state and present a new behaviour analysis by using Fuzzy guided Genetic Algorithm.

VI-COMPARISON STUDY OF EXISTING WORK

The architecture of cloud systems is the foundation for the work done on cloud computing security. In this context, [1] derives the result from server communications conducted both online and offline. The author refers to the protocol that came about as a result of his conversation, the cloud key management protocol based on which results in data security without losing any information content while keeping the encryption key hidden from cloud provider. Many products, like CrashPlan4 and CloudFogger5, provide cloud security. Secret sharing schemes with various thresholds can be used to achieve confidentiality and availability. With threshold t = n/2, Shamir's secret sharing strategy provides confidentiality of the files for up to t hostile servers while simultaneously guaranteeing availability of secret files unless t+1 servers are malicious. Optimal confidentiality and better availability hence achieved by using a sharing scheme with full threshold (t = n - 1), such as additive sharing's over a finite field. This ensures optimal confidentiality of the secret files against offline attacks [6]. In [2] describes the Key management in cloud computing to ensure secrecy this paper describes the theory of how cloud computing needs fully federated key management.

The federated identity management and Hierarchical Identity Based Cryptography (HIBC) in the cloud depict that how system can generate and distribute the public and private keys to users and servers. Its advantages is simplifying public key distribution and reducing SOAP header size and author showed how the users and servers in the cloud can generate secret session key without message exchange and authenticates each other with a simple way using identity-based cryptography. In [3], multicast security key management protocols are used to support a variety of application, transport, and network-layer security protocols. It also defines the group security association (GSA) and describes the key management protocols that help establish a GSA.

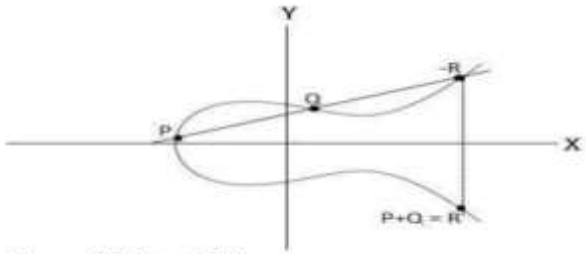

Figure 3 Point addition

In [4], the proposed scheme considers the major security issues of cloud computing and also ensures their infrastructure is secure and prevents illegal data accesses from outsiders, other clients, or even the unauthorized cloud employees. Here the author also describes cloud security services including key agreement and authentication by using ECDH and symmetric bivariate polynomial based secret sharing. What follows are the details of elliptic curve cryptography and elliptic curve diffie hellman key exchange algorithm [15].

Key management in the cloud has a great deal of disadvantages that may be determined depending on these kinds of applications and usage in different contexts. Naturally, a lot of applications only need to compute at specific, predetermined times. For instance, benchmarks and online auctions are frequently planned to be repeated at regular intervals. The majority of cloud service providers also work on a pay-per-use model (pay per CPU cycle spent, pay per byte sent, etc.) It does not increase security because servers must keep secret keys. The majority of apps simply need to store tiny files, like cryptographic keys. To illustrate this, each server in the

https://doi.org/10.46335/IJIES.2022.7.7.3 **e-ISSN: 2456-3463**
Vol. 7, No. 7, 2022, PP. 12-19

benchmark stores and accesses a secret file that is 1 KB in size. The execution time naturally grows with the size

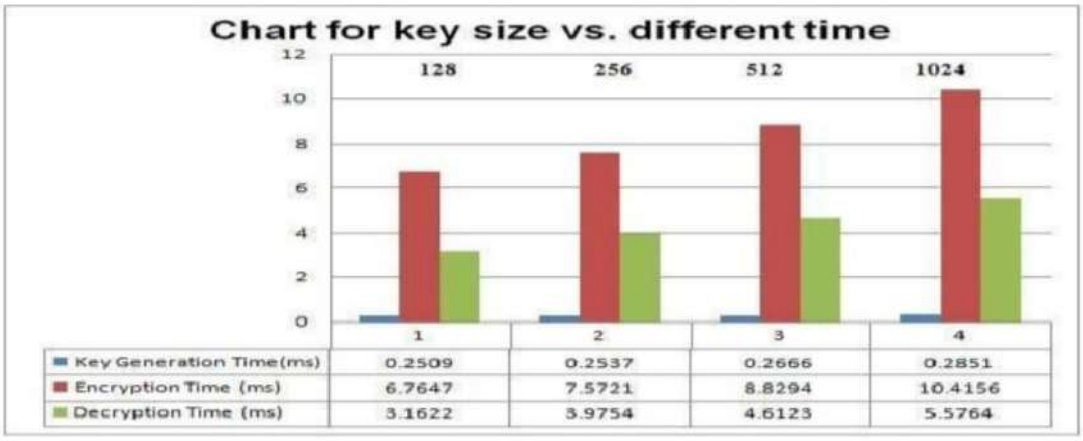

Figure 4 Chart for key size vs different time

Table 1 The comparative study of cloud computing key management infrastructure

Papers	Basic theory for cloud computing security	Data in-tegrity	Authentication	Scalability	Data confi-den-tiality
[6] Ivan Damgrd et al.	Secure multiparty computation	yes	No	Highly scalable	yes
[1] Dr. Atulbhai Patel et al.	Federated Key Management	no	Yes	Moderate	yes
[7] K.Sriprasadh et al.	Multicast Key Management	no	Yes	Highly scalable	yes
[8] Ching-Nung Yang et al.	Based on Secret Sharing Scheme	no	Yes	Moderate	yes
[9] SONG Ningning et al.	Hyper Elliptic Curve Cryptosystem	yes	Yes	Moderate	-
[5] Sun Lei et al.	Key Management Interoperability Protocol (KMIP)	no	Yes	Moderate	yes
[10] XiaoChun Yin et al.	Public Key Infrastructre Based ECC	yes	Yes	Moderate	yes
[11] S.V.Divya et al.	Data Forwarding ECC	no	Yes	Moderate	-
[12] Kanatom Jindarak et al.	Genetic Algorithm based Placement	yes	Yes	Moderate	yes
[13] Shilpi Singh et al.	Elliptic Curve Cryptography	yes	Yes	Scalable	yes
[14] Sahil et al.	Artificial Intelligence and Genetic algorithm	yes	Yes	Scalable	yes

Table 2 comparison of security analysis in cloud computing

Popular attacks in cloud computing	Papers [19]	[20]	[10]
Identity Theft	X	0	0
Man-in-the-Middle Attack	0	0	0
Snooping Attack	0	0	0
Guessing Attack	X	0	0
Compromised-Key Attack	X	X	0
Unauthorized Modification	X	X	0
ImpersonationAttack	X	X	0

Table 3 key size v/s different time in literature [18]

Key size	Key generation time(ms)	Encryption time (ms)	Decryption time (ms)
128	0.2509	6.7647	3.1622
256	0.2537	7.5721	3.9754
512	0.2666	8.8294	4.6123
1024	0.2851	10.4156	5.5764

of the secrets stored, yet the size of secrets was found to have relatively little impact.

For example, storing 100 Mb instead of 1 Kb secrets roughly costs 2 seconds extra. The reason for this is that the encryption and decryption of secrets take place locally and only the encryption keys are shared [1]. Table 2 represents comparison of security analysis with respect to popular attacks in cloud computing. In paper[10] has more advantages in defending popular attacks in cloud storage systems comparing with [19] and [20]. Because author in [10] uses PKI-based Cryptography scheme for cloud storage it ensures the users identity they claim in the virtual cloud storage and process doesn't reveal the clear data to any third party including the cloud provider. The author uses ECC for all the cryptographic operations which provides low computation and communication cost as well as less key-size to provide same level of security as of RSA. Table 3 describes the amount of time required in encryption, decryption and key generation based on the key size in paper [18]. The author proposes key management and encryption by using SDC homomorphic cryptosystem for data storage in cloud. Considering this method the model of ECDH with the combination of genetic algorithm can be used in order to minimize time required in encryption, decryption and key generation based on the key size. Figure 4 represents the chart for key size vs different time which represents the amount of time required in encryption, decryption and key generation will be increases as the key size. Cloud storage and key management in the cloud can be proposed by using genetic algorithm in order to improve in the average access time for the users. In the future, more detail assumption such as CPU and I/O speed will be taken into consideration for any cloud computing application.

VII-CONCLUSION AND FUTURE WORK

Key management, data loss, data leakage, and user authentication are the main security issues of cloud computing. This study examines ways to allay security worries about the public cloud's private data storage and suggests a plan to create a reliable cloud storage system. One of the fundamental strategies that cloud computing systems should use to protect data is strong encryption with key management. ECC and ECDH algorithms, as well as ECC and genetic algorithms and their combinations with fuzzy logic, offer the same level of security as other public key cryptosystems with smaller keys. By combining these methods, the cloud computing industry can reduce the amount of time needed for encryption, decryption, and key creation based on key size.

Conflicts of interest

The authors have no conflicts of interest to declare.

REFERENCES

[1] *Patel A, Soni K. Cloud computing security using federated key management. International Journal of Engineering and Computer Science. 2014; 3(2): 3978- 81.*

[2] *Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security & Privacy. 2011; 9(2):50-7.*

[3] *Chandramouli R, Iorga M, Chokhani S. Cryptographic key management issues and challenges in cloud services. In secure cloud computing 2014 (pp. 1-30). Springer New York.*

[4] *Kulkarni P, Khanai R. Addressing mobile cloud computing security issues: a survey. In international conference on communications and signal processing 2015 (pp. 1463-7). IEEE.*

[5] *Lei S, Zishan D, Jindi G. Research on key management infrastructure in cloud computing environment. In ninth international conference on grid and cloud computing 2010 (pp. 404-7). IEEE.*

[6] *Damgård I, Jakobsen TP, Nielsen JB, Pagter JI. Secure key management in the cloud. In IMA international conference on cryptography and coding 2013 (pp. 270-89). Springer Berlin Heidelberg.*

[7] *Sriprasadh K, Pandithurai O. A novel method to secure cloud computing through multicast key management. In international conference on information communication and embedded systems 2013 (pp. 305-11). IEEE.*

[8] *Yang CN, Lai JB. Protecting data privacy and security for cloud computing based on secret sharing. In international symposium on biometrics and security technologies 2013 (pp. 259-66). IEEE.*

[9] *Song N, Chen Y. Novel hyper-combined public key based cloud storage key management scheme. China Communications.2014;11(14):185-94.*

[10] *Yin X, Liu Z, Lee YS, Lee HJ. PKI-based cryptography for secure cloud data storage using ECC. In 2014 international conference on information and communication technology convergence 2014 (pp. 194-9). IEEE.*

[11] *Divya SV, Shaji RS. Security in data forwarding through elliptic curve cryptography in cloud. In international conference on control, instrumentation, communication and computational technologies 2014 (pp. 1083-88). IEEE.*

[12] *Jindarak K, Uthayopas P. Performance improvement of cloud storage using a genetic algorithm based placement. In eighth international joint conference on computer science and software engineering 2011 (pp. 54-7). IEEE.*

[13] *Singh S, Kumar V. Secured user's authentication and private data storage-access scheme in cloud computing using Elliptic curve cryptography. In international conference on computing for sustainable global development 2015 (pp. 791-5). IEEE.*

[14] *Sood S, Mehmi S, Dogra S. Artificial intelligence for designing user profiling system for cloud computing security: experiment. In international conference on advances in computer engineering and applications 2015 (pp. 51-8). IEEE.*

[15] *Shalini IS, Naik M, Sathyanarayana SV. A comparative analysis of Secret Sharing Schemes with special reference to e-commerce applications. In international conference on emerging research in electronics, computer science and technology 2015 (pp. 17-22). IEEE.*

[16] *Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987; 48(177):203-9.*

[17] *Miller VS. Use of elliptic curves in cryptography. In conference on the theory and application of cryptographic techniques 1985 (pp. 417-26). Springer Berlin Heidelberg.*

[18] *Todkar A, Sutar S. Secure Role Based Access Policy for PHR using Homomorphic Cryptosystem. Inventi Impact: Cloud Computing, 2016:1-4.*

[19] *Wu X, Xu L, Zhang X. Poster: a certificateless proxy re-encryption scheme for cloud-based data sharing. In proceedings of the 18th ACM conference on computer and communications security 2011 (pp. 869-72). ACM.*

[20] *Jenefa N, Jayalakshmi J. A cloud storage system with data confidentiality and data forwarding. International Journal of Soft Computing and Engineering. 2013; 3(1): 391-4.*