Review Article

ACCENTS Transactions on Information Security, Vol 2(7)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2017.27001

Key management infrastructure in cloud computing environment-a survey

Mohan Naik R[1]*and S V Sathyanarayana[2]
Assistant Professor, Department of ECE, SDMIT, Ujire, Karnataka, India[1]
Professor, Department of ECE, JNNCE, Shimoga, Karnataka, India[2]

Abstract

The term cryptography which means "secret writing", has become the foundation primitive in providing security for many communication applications. In many applications, particularly in group communication, there is a need to hide secret data like passwords, encryption key, recipes etc. Here efficient key management protocols are required to provide security for group's secret data. Because it is very challenging to provide security for group's secret data, especially in two scenarios: when the number of group members more and when the group members are present in different locations with diverse mechanisms of protection. The cloud computing where application services are provided through the internet. Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the internet. The cloud computing not only provides additional computing resources, but also network infrastructure which supports group communication scenarios. To interact with various services in the cloud and to store the data generated/processed by those services, several security mechanisms are required. In this context, this paper investigates the basic problem of cloud computing key management and enabling support for interoperability between cloud cryptographic clients and cloud key management servers. Cloud key management includes its creation and its subsequent adoption to reduce the complexity of encryption key management, infrastructure costs and risks and also to enhance the performance of both private and public storage cloud is discussed. This paper deals with the elaborate survey of existing key management techniques in cloud computing security and there by exploring the possible solution for cloud computing security.

Keywords

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

1.Introduction

The term Cryptography is a fundamental object that helps in communication between any two persons over an insecure communication channel. Today most of the communication applications are based on Group Communication where, members of the group are allowed to share information within the group. For instance data communication, video and audio conferences, information sharing and many more. Security is a main aspect for group communication. As a result, group communication security i.e., providing authentication, integrity, and confidentiality of message delivered among the members will become a critical communication issue. Cloud computing is an internet based technology that serves the on demand IT-infrastructure comprises of software, hardware and applications to the users. Cloud computing provides its consumers ease of using the cloud based applications and low equipment requirements at client side. Data can be stored or accessed by user anytime, anywhere over the cloud using internet.

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. Key management covers all the details of how to handle keys carefully enough to ensure that the key should not get compromised. Cloud customers and providers need to guard against

*Author for correspondence

data loss and theft. Encryption of personal and enterprise data is strongly recommended, strong encryption with key management is one of the core mechanisms that cloud computing systems should use to protect data [1].

In Cloud computing there are three core set of services - infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Based on these core set of services, Cloud has enormous benefits but when comes to security it may be vulnerable to different types of attacks [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.

2.Cloud computing architecture

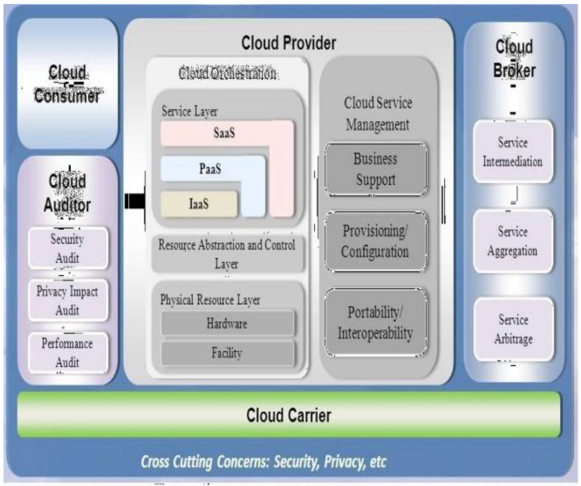

Figure 1 Cloud computing security reference architecture

Cloud Provider:A person, organization, or entity responsible for making a service available to interested parties.

Cloud Auditor:A party that can conduct independent assessment of cloud services, information system operations performance and security of the cloud implementation.

Cloud broker: An entity that manages the use, performance and delivery of cloud services, and negotiates relation-ships between Cloud Providers and Cloud Consumers.

Cloud carrier: An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

3.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. Confidentiality and privacy: It refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, which leads to an increase in the number of points of access. Delegating data control to the cloud, inversely leads to an increase in the risk of data compromise, as the data becomes accessible to an augmented number of parties.

2. Multitenancy: It refers to the cloud characteristic of resource sharing. Several aspects of the IS are shared including, memory, programs, networks and data. Although users are isolated at a virtual level, hardware is not separated.

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.

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 have the ability to continue operations even in the possibility of a security breach.

8.Service Disruption While service hijacking is not new even with Cloud infrastructure, malicious attacks such as phishing, fraud, and exploitation of software vulnerabilities still help hackers score. In case an attacker gains access to an organization's login credentials, he can eavesdrop the data, transactions or manipulate data. Even worse an attacker can replay sessions, and redirect an organization's clients to illegitimate sites or launch a denial of service (DoS) or distributed DoS (DDoS) attack leveraging bot-nets.

4.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. By defining a protocol that can be use 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.

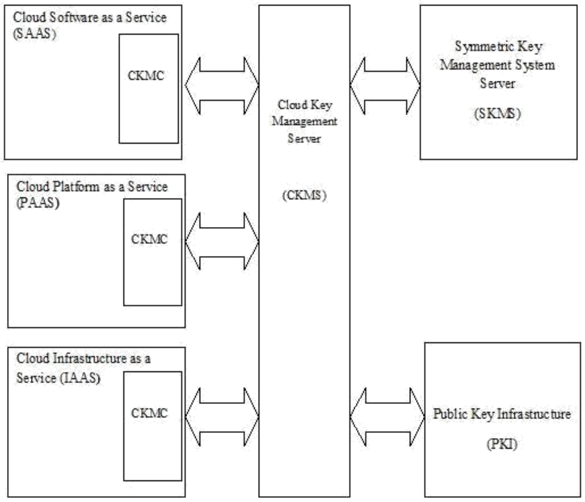
Cloud Software as a Service (SAAS)
CKMC
Cloud Platform as a Service (PAAS)
CKMC
Cloud Infrastructure as a Service (IAAS)
CKMC
Cloud Key Management Server
(CKMS)
Symmetric Key Management System Server
(SKMS)
Public Key Infrastructure
(PKI)

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.

5.Survey of existing key management frame work for cloud computing

In this section describing the solutions that have been proposed in [6], authors have considered that the applications involving a number of servers in the cloud that go through a sequence of online periods where the servers communicate, separated by offline periods where the servers are idle. During the offline periods, servers need to securely store sensitive information such as cryptographic keys. Applications like this include many cases where secure multiparty computation is outsourced to the cloud, and in particular a number of online auctions and benchmark computations with confidential inputs. Author denotes that the protocol resulting from the above discussion as the cloud key management protocol, or just PCKM. 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. Encryption only involves complicated mathematics that is incomprehensible to most people. Key management involves technology, people and processes, so it’s even more difficult. Encryption provides an extremely high level of protection. Federation describes how different computer systems can work together. In the context of key management, federation includes how different applications can get keys from the same key server. This paper also 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 depicts how can the system generate and distribute the public and private keys to users and servers. compared with the current Ws-Security approach, the proposed approach in this paper has advantages in simplifying 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 framework and guidelines described in this paper permit a modular and flexible design of group key management protocols for a variety of different settings that are specific to applications need. MSEC key management protocols may be used to facilitate secure one-to-many, many-to-many, or one-to-one communication.

In the proposed scheme suggested in [4], the major security issue of cloud computing is the cloud provider must ensure that their infrastructure is secure, and that prevent illegal data accesses from outsiders, other clients, or even the unauthorized cloud employees. In this paper the author describes cloud security services including key agreement and authentication using 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 multi-server 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 hyper-combined 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 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]. Hence without appropriate security and privacy solution in place it will cause some critical data security problems to its users. In [10] the author address the security issues of storing private and sensitive data in the cloud storage service and proposed a PKI-based Cryptography scheme for cloud storage.

In [8] authors suggested to build a secure storage system with some functionality is still a challenging task in cloud Existing methods suffer from inefficiency and delay because the data cannot be forwarded to user without retrieving back and offline verification causes delay. It focuses on designing a secure cloud storage system that supports data forwarding function using elliptic curve cryptography and it alerts to data owner as an when attacker tries to modify the data or 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 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 paper proposes a scheme that not only provides security of user's private data of storing and accessing over the cloud but also authentication of the user to the cloud server using elliptic curve cryptography [13]. In [13], user first logins into the cloud and authenticates himself. After authentication user uses two techniques ECDH key exchange and Symmetric key algorithm to encrypt and decrypt the data. ECC and ECDH algorithm that provide same level of security as of other public key cryptosystems with less key size and strengthens the security of the algorithm.

In [14] artificial intelligence for designing user profiling system augments the security system to work in proactive and reactive manner and provides an enhanced security. 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.

6.Comparison study of existing work

The work carried out for the cloud computing security is based on the architecture of cloud systems. In this regard [1] obtains the conclusion based on the online and offline server communications. Author denote the protocol resulting from his discussion, the cloud key management protocol based on which resulting in the data security without losing any content of information keeping the encryption key secret from cloud provider. There are several products such as CrashPlan4 and CloudFogger5 offers cloud security. Confidentiality and availability can be achieved using secret sharing schemes with different thresholds. Using Shamirs secret sharing scheme with threshold t = n/2 ensures availability of secret files unless t+1 servers are malicious, also guarantees confidentiality of the files for up to t malicious servers. 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.

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]. Many of the standards use public key cryptosystem for authentication purpose. RSA is one among them. In case of RSA encryption Scheme, as security increases the key length also increases which leads to high process-ing overhead. Elliptic Curve Systems which are applied in many Cryptographic applications were introduced in 1985 separately [16]. Elliptic curve cryptography (ECC) is one of the challenging systems developed to provide high security with smaller key size. ECC is standardized by IEEE and reported in IEEE P1363 std [17]. Elliptic Curves are easy functions which can be drawn as smooth looping lines in (x,y) plane. In general, cubic equation for Elliptic Curve can be given by using generalized weierstrass equation as given in Equation (1)

$$y^2 + a_1xy + a_3\,y = (x^3 + a_2x^2 + a_4\,x + a_6) \qquad (1)$$

Where a_1,a_2, a_3, a_4, a_5 , a_6 ∈ Fp and p is a prime integer. Equation 1 of elliptic curve over Fq is a set of solutions (x; y) ∈ Fp including special point o, called point at infinity.

If characteristic of field is neither '2' nor '3' then Equation 1 can be written as

$$y^2 = (x^3 + Ax + B) \qquad (2)$$

We generally use Equation 2 for many applications, with discriminant condition given by Equation 3

$$4a^3 + 27b^2 \neq 0 \qquad (3)$$

Elliptic Curves over prime field are used for performing Secret Sharing.

A. Elliptic curves over GF(P)

An elliptic curve defined over Prime Field Z_P is obtained by selecting the variables a and b from the field Z_P . The elliptic curve contains all points (x,y) which satisfy the elliptic curve equation modulo p (where x and y are belongs to Z_P). Elliptic curve over prime field is given by Equation 4

$$y^2 mod\ p = (x^3 + ax + b) mod\ p \qquad (4)$$

Addition and multiplication procedure in an elliptic curve group over Prime field is given as follows. Let the points be P = (x_1; y_1) and Q = (x_2; y_2) in the elliptic group E_p(a; b) and O be the point at infinity. If Q ≠ -P, then their sum P + Q = (x_3,y_3) is given by:

$$x_3 = \lambda^2 - x_1 - x_2\ mod\ p$$

$$y_3 = \lambda(x_1 - x_2) - y_3\ mod\ p$$

Where,

$$\lambda = \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)} & \text{if P} \neq \text{Q} \\ \dfrac{(3x_1^2 + a)}{(2y_1)} & \text{if P} = \text{Q} \end{cases}$$

The multiplication kP is obtained by repeating the elliptic curve addition operation k times by the same addition formula. The scalar point multiplication over A can be defined as kP = P + P +.... +P (k times). If P,Q ∈ A, the addition P + Q is a point R. The line passing through P and Q intercepts the curve at a point called R. The reflection of -R is R with respect to the x-axis. This is known as point addition as shown in *Figure 3*.

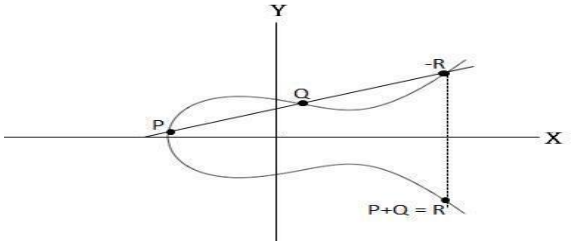

Figure 3 Point addition

B. Elliptic Curve Encryption/Decryption

Suppose user A wants to send message Pm to user B then user A randomly chooses a positive integer k, private key dA.

The public key of A is generated as PA= dAG and the cipher text Cm is produced with consisting of pair of points.

Cm =(kG,Pm) + kPB
Where G is the base point selected on the elliptic curve,

PB =dB G is the public key of B and dB is the private key of B. A will send the cipher text C_m as encrypted message to B. To decrypt the cipher text, B multiplies the first point in the pair by its private key d_B and subtracts the result from the second point to get the original message P_m [13].

$$P_m + kP_B\text{-}d_B\ (kG) = P_m + k\ (d_BG)\text{-}d_B(kG)= P_m$$

C. Elliptic curve diffie-hellman (ECDH) key exchange

Generally, to encrypt/decrypt the bulk of data Symmetric-key (also known as secret-key) cryptosystems are used due to its faster computation than public-key cryptosystems. To generate a secret key between two users for a single session elliptic curve diffie-hellman key exchange technique on elliptic curve can be applied which is described below: Suppose that users A and B want to agree upon a secret key, which will be used for secret key cryptography. A will generate private key d_A and a public key $P_A = d_AG$, where G is the generator of the elliptic curve. A sends P_A to B. Similarly, B will generate private key d_B and a public key $P_B = d_BG$. B sends P_B to A. On receipt of As message, B Computes d_B $(P_A\ ) = d_Ad_BG$ On receipt of Bs message, A computes d_A $(P_B\ ) = d_Ad_BG$ Now, both A and B can use d_Ad_BG, which is a point on the given elliptic curve, as a common secret keys. The user first logins into the cloud and authenticate himself. After authentication user uses two techniques ECDH key exchange and Symmetric key algorithm to encrypt and decrypt the data [13].

In Paper-5, to solve the problem of collusion attack and realize efficient maintenance of large-scale Key, a hyper-combined public Key scheme based on the hyper elliptic curve cryptosystem is designed. Operation characteristics of addition and scalar multiplication in Jacobian quotient group of elliptic curve are introduced.

In [6] proposes PKI based cryptography scheme for cloud storage. The scheme has the following advantages: First it can ensures the users have the identity they claim in the virtual cloud storage world, Second it secures the data during its entire life cycle the whole process doesn’t reveal the clear data to any third party including the cloud provider, Third it offers controlled data access and sharing among users, so that unauthorized users or untrusted servers cant access or search over data without data owners authorization. ECC provides low computation and communication cost as well as less key-size to provide same level of security as of RSA.

In [8] focuses on designing a secure cloud storage system that supports data forwarding function using elliptic curve cryptography. The paper also concentrates on Online Alert methodology which indicates the data owner when any attacker tries to modify the data or any malpractice happens during data forwarding. Moreover, this method ensures multi-level security. In [9], the model for cloud storage and object placement is discussed. Then, genetic algorithm is used to optimize the placement function to gain a better average access speed for any storage object. Here author also proposes the performance improvement of cloud storage using a genetic algorithm based placement.

In [10], author proposes Secured users Authentication and private data storage access scheme in cloud computing using elliptic curve cryptography. In [11] focuses 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. *Table 1* describes comparative study based on data integrity, authentication, scalability and data confidentiality in various literatures. In paper [1] federated key management and [7] multicast key management approach is discussed which provides authentication, data confidentiality with moderate scalability factors. In paper[10,11] and [13] by considering Elliptic Curve Cryptography approach for security in data forwarding, secure user authentication and private data storage in cloud computing which provides data integrity, authentication, data confidentiality and moderate scalability factors. In paper [12] considering genetic algorithm based performance improvement of cloud storage which gives better average access speed for any storage object. In paper [14] user profiling system for cloud environment using Artificial Intelligence techniques and studies behavior of User Profiling System and proposes a new hybrid approach. User Profiling System is a program, which logs user activities and provides analysed, in-depth information about the user behavior by profiling user's activities. Profiling of user's character through evaluating its usage patterns (activities) helps a security mechanism to take appropriate control measures based on the profile history of user. In this way the combination of artificial intelligence techniques and genetic algorithm based approach will provide cloud computing security which gives data integrity, authentication, data confidentiality with good scalability factors.

In cloud computing key management so many drawbacks that can identified based upon these types of applications and uses in various environments. Naturally many applications only require computation at certain well-defined points in time. For example, online auctions and benchmarks are often designed to be repeated at regular time intervals. Furthermore, most cloud providers operate on a pay-per-use basis (pay per CPU cycle spent, pay per byte sent, etc.) It requires servers to store private keys and therefore does not add extra security.

Most applications will only require storage of small files such as cryptographic keys. To reflect this, the servers in the benchmark all store and retrieve secret files of size 1 Kb. Storing larger secrets of course increases the execution time, but 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.

7.Conclusion and future work

Users authentication, data leakage, loss of data, key management is the important security concerns in cloud computing. This paper is a survey of removing these security concerns over the private data part of the public cloud and proposed a scheme to develop a trusted cloud storage system. Strong encryption with key management is one of the core mechanisms that cloud computing systems should use to protect data. ECC and ECDH algorithm that provide same level of security as of other public key cryptosystems with less key size and ECC and genetic algorithm and also by using the combination of ECC and fuzzy logic.

By using these combination amount of time required in encryption, decryption and key generation based on the key size of cloud computing can be improved and also improves in the average access time for the users in the cloud.

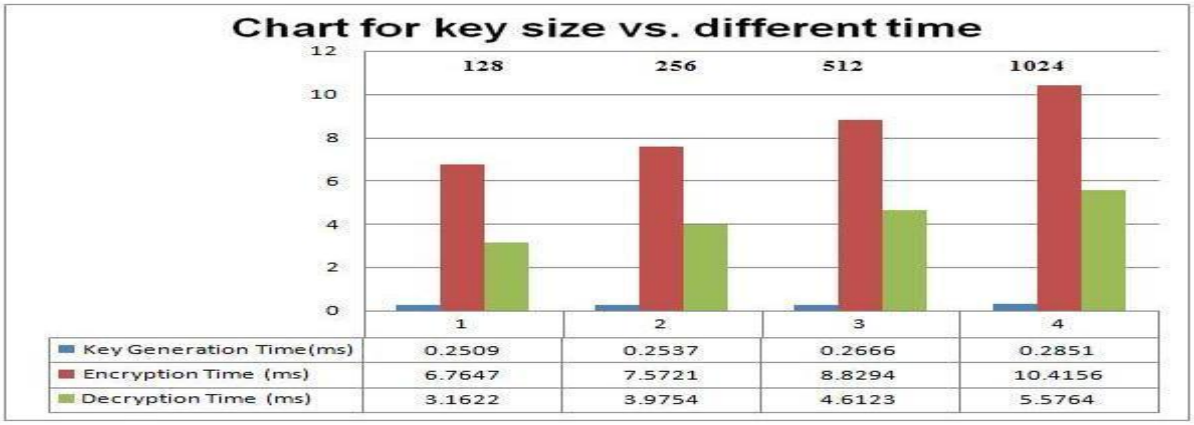

Figure 4 Chart for key size vs different time

Table 1 The comparative study of cloud computing key management infrastructure

Papers	**Basic theory for cloud computing security**	**Data integrity**	**Authentication**	**Scalability**	**Data confidentiality**
[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

Acknowledgment

None.

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.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.