Scientific Research Publishing

Circuits and Systems, 2017, 8, 77-92
http://www.scirp.org/journal/cs
ISSN Online: 2153-1293
ISSN Print: 2153-1285

Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing

J. Athena, V. Sumathy

Department of ECE, Government College of Technology, Coimbatore, India
Email: athenaj007@gmail.com

How to cite this paper: Athena, J. and Sumathy, V. (2017) Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing. *Circuits and Systems*, **8**, 77-92.
https://doi.org/10.4236/cs.2017.83005

Received: May 14, 2016
Accepted: May 23, 2016
Published: March 31, 2017

Abstract

Numerous advancements in the Information Technology (IT) require the proper security policy for the data storage and transfer among the cloud. With the increase in size of the data, the time required to handle the huge-size data is more. An assurance of security in cloud computing suffers various issues. The evolution of cryptographic approaches addresses these limitations and provides the solution to the data preserving. There are two issues in security assurance such as geographical distribution and the multi-tenancy of the cloud server. This paper surveys about the various cryptographic techniques with their key sizes, time required for key/signature generation and verification constraints. The survey discusses the architecture for secure data transmissions among the devices, challenges raised during the transmission and attacks. This paper presents the brief review of major cryptographic techniques such as Rivest, Shamir Adleman (RSA), Dffie Hellman and the Elliptic Curve Cryptography (ECC) associated key sizes. This paper investigates the general impact of digital signature generation techniques on cloud security with the advantages and disadvantages. The results and discussion section existing in this paper investigate the time consumption for key/signature generation and verification with the key size variations effectively. The initialization of random prime numbers and the key computation based on the points on the elliptic curve assures the high-security compared to the existing schemes with the minimum time consumption and sizes in cloud-based applications.

Keywords

Cloud Computing, Cryptography, RSA, Diffie Hellman, Elliptic Curve Cryptography, Digital Signature

1. Introduction

Cloud computing enables on-demand services to the users in the pay-as-use ba-

sis with the highest level of scalability and flexibility. The cloud services include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The cloud usage eliminates the burden of system maintenance, software license purchase, and the cost of hardware components. The benefits of cloud computing improve accessibility, automatic software integration, quick deployment, high scalability, low investment cost and flexibility [1]. On the basis of the services offering by the cloud computing, the clouds are categorized into four types such as private, public, hybrid and community clouds.

- Public clouds: The provisions of the services through the off-premise third party to the general public and computing resources fall into this category.
- Private clouds: They enable the large size organizations to achieve the efficiencies with the responsibility constraint of data.
- Hybrid clouds: Some enterprises utilize the public clouds for general computing and private clouds for customer data protection to assure the security.
- Community clouds: Distinct groups of organizations have the compliance and security considerations and the infrastructures offered by the internal and external third party suppliers.

The major characteristics of the cloud computing are self-service, per-usage method, elastic and customizable. When an organization adapts public cloud services, most of the computing system infrastructures will be under the control of cloud service provider. With the aim of achieving the profit, cloud service provider may not store all the data, which leads to incorrect and incomplete data storage. This data loss will be hidden to retain the reputation of the service providers in the market. The storage of data in the third party remote server may be accessed by the unauthorized users. Even though, the process of data outsourcing reduces the storage and maintenance overhead, the resource pooling in a third party data center leads to several security issues.

The creation and the management of secured cloud space are a more challenging task than the creation of classical IT environment. The misunderstanding responsibilities, issues in confidentiality, lack of standards, interoperability issues and malicious insiders in the cloud computing caused the several issues to preserve the data from the attacks. Security issues have been categorized into data breaches, malicious attack, data loss, and inadequate diligence, sensitive data access, data segregation, etc. [2]. The confidentiality, integrity and availability must be ensured to achieve data security.

The data security has become a complex challenge in cloud computing due to the following reasons:

- The necessity to guard the confidential and sensitive data related to government and business organizations.
- The sharing of cloud infrastructure among various clients.
- Legal and regulatory compliances during data mobility.
- Issues in auditing and reporting.
- Lack of backup and storage standards.
- Key management issues and unauthorized access

In order to overcome these security challenges, there are several solutions available in secure cloud storage server. The confidentiality can be attained by applying the access controls, authentication mechanisms, cryptography schemes etc. The access to control and authentication mechanisms allows the authorized user access, whereas the cryptography techniques allows only the specific user, who possess the keys to access the data. Hence, the cryptography schemes are the best way to provide data security, in which the user cannot access the data without the knowledge of key. Generally, most of the cryptography techniques include three major steps as follows:

- Key generation;
- Encryption;
- Decryption.

Figure 1 shows the data flow and message flow in cloud storage server for secure data transmission. Key generation is the process of producing the keys that are used for encryption and decryption. The encryption is the process of converting the original data into an unreadable form known as cipher text by the keys. The decryption is the process of retrieving back the original message from the cipher text using the appropriate keys. The cryptography schemes are classified into two types such as symmetric or conventional cryptography and asymmetric or public key cryptography. The symmetric cryptography uses same key for both encryption and decryption, whereas the public key cryptography uses different keys. The symmetric cryptography schemes are fast but there is no guarantee for secure key distribution. As they use the same key for encryption and decryption, the third party, who is snooping while key transmission may decrypt the data.

In order to overcome this issue, public key cryptography is introduced with a pair of keys, namely, public key and private key. The key advantage of public key cryptography is that the private keys used for decryption is never shared or

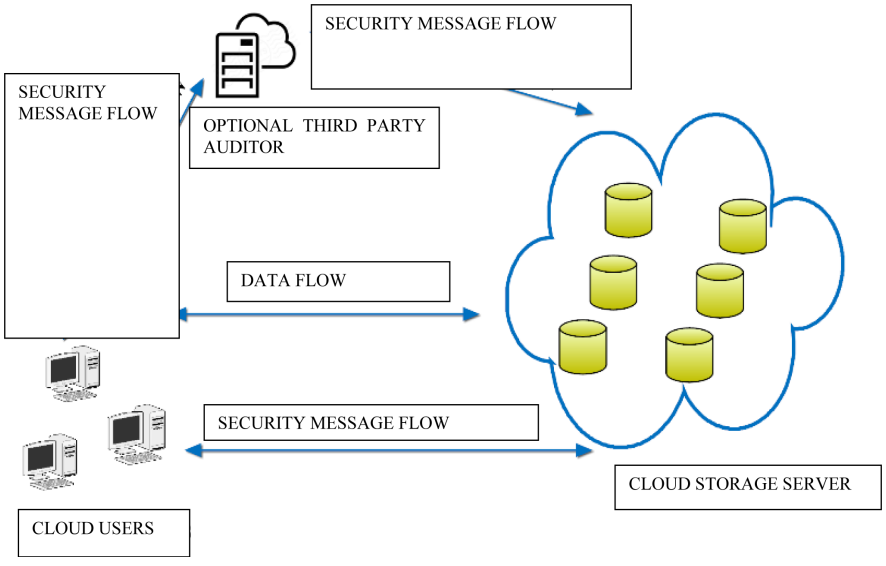

Figure 1. Data transmission in a secure cloud storage server.

transmitted [3]. The public key will be broadcasted, using which the data can be encrypted. The authorized user who possess the private key can only have the right to decrypt the data. The remaining sections of this paper are organized as follows: Section II presents the security challenges in cloud computing. Section III provides the list of cloud security attacks. Section IV describes various public key cryptography techniques to overcome the security issues. Section V shows the results and discussion of the cryptography schemes. The survey is concluded in Section VI.

2. Security Challenges in Cloud

Security is an important concern for several organizations that adopts cloud for data storage and maintenance. A minor mistake in any of the client application will pave a way to the hackers to access the entire data in the cloud storage server. If there is vulnerability in the cloud, the unauthorized user may access, corrupt, modify or delete the records in the cloud. The security challenges arise in the deployment models, service models and in the network [4]. It is the responsibility of the security manager to define the security framework of an organization based on asset, threat and vulnerability risk assessment matrices. Confidentiality, integrity, and availability are the three main are of data security [5]. Data confidentiality is significant in a place, where a critical data is stored in a remote server with multi user access. **Figure 2** shows various security challenges in cloud computing.

In a multitenant cloud infrastructure, the access privileges must be provided to the users to achieve security. Hence, the data of an organization cannot be accessed by the users of any other organization. Integrity is an important factor to maintain the reputation of the service provider. The trust and security can be enhanced by allowing only the authorized person to update the data of an organization. Data loss and data leakage can be prevented by employing integrity. Thus, authentication and identity management is used to provide authorized

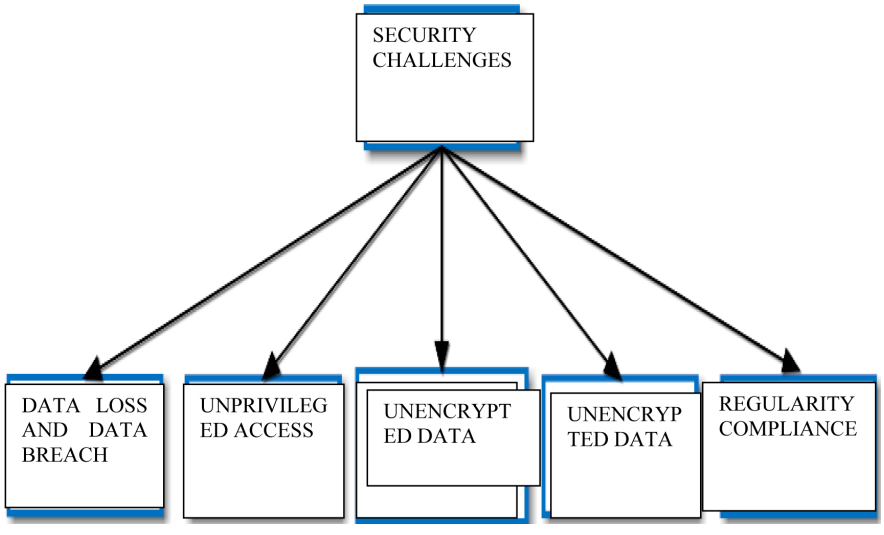

Figure 2. Security challenges in cloud computing.

access. The service level agreement is signed between the vendor and the provider to eliminate the downtime of the server and to make the data always visible [6]. The major security challenges include data segregation and data leakages. The security challenges in cloud computing are listed below.

2.1. Data Breaches and Data Loss

The disclosure of sensitive data to the unauthorized user is termed as data breach. The causes of data breach are lack of authentication, audit, and authorization controls and a few defects in the design of infrastructure and application. It may also take place due to several unfortunate transmissions and insider attacks. When a hacker gets access to the cloud via a single application, then the entire cloud infrastructure will be under attack prone area [7].

Data loss results in the leakage of confidential and sensitive data. This is due to the modification or deletion of data by the hackers with an intention of delivering altered information or to hide the information from the users. Loss of encryption keys, natural disasters and storage system faults will also lead to data loss.

2.2. Regulatory Compliance

The distributed cloud infrastructure stores data in multiple remote servers that are located in different geographical locations. The legal constraints vary from place to place and hence, it is difficult to assign a particular server to be used for data transmission at the borders of a region.

2.3. Unencrypted Data

The unencrypted data leads to data confidentiality, data breaches and data loss by exposing the original data. The cloud users depend on the service provider for encryption and the keys can be either managed by the user or the provider. Key management and distribution is a sensitive process, as the message can be read by any one, who gets the key. In order to improve the security, the keys are split into several units and distributed among the users, provider and the third party service that is responsible for encryption [8].

2.4. Unprivileged Access

The access control mechanisms must be incorporated to prevent the unauthorized users from accessing the data. The sensitive data must be secured by providing access only to a very few important persons of an organization. The data are classified based on its sensitivity and need. The users are mapped only to the required data and they are prohibited to access or view the other unnecessary data [9]. Data abstraction and transparency is implemented for privileged access.

2.5. Service Hijacking

Service hijacking is the illegal access by unauthorized users to certain services. It leads to software exploitation, fraud, criminal activities and phishing through e-

mail. The services must be registered in the service providers to avoid hijacking.

2.6. Lack of Authentication and Identity

The lack of authentication allows malicious users in the storage server. Each and every user must be provided with an identity and authentication password to enter the storage space [10]. Without authentication any one can alter the data of an organization. It is one of the severe concerns to data security.

3. Cloud Security Attacks

3.1. Side Channel Attack

Side-channel attack urges the application of cryptographic techniques to prevent the cloud systems from security threat. Therefore, it is necessary to evaluate the resilience of the cryptographic system against the side-channel attacks.

3.2. Authentication Attack

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and PaaS, there is only IaaS offering this kind of information protection and data encryption.

3.3. Man-In-The-Middle Attack

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can interfere and modify communications.

4. Public Key Cryptography Techniques

Cryptography plays a significant role in securing the data by converting it into an unreadable form during storage and transmission. The asymmetric encryption, which is also known as public key cryptography, applies public and private keys for encryption and decryption respectively. This adds key strength and hence, key exchange is not a problem in this scheme. **Figure 3** shows the various public key cryptography techniques.

4.1. Rivest, Shamir, Adleman (RSA)

RSA algorithm is one of the public key cryptography schemes that is used for secure data transmission. The algorithm is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman [11]. In RSA, a public-private key pair is generated, where the public key is published to all for encryption and the private key is kept safe for decryption. The three major steps are:

- Key generation;
- Encryption;
- Decryption.

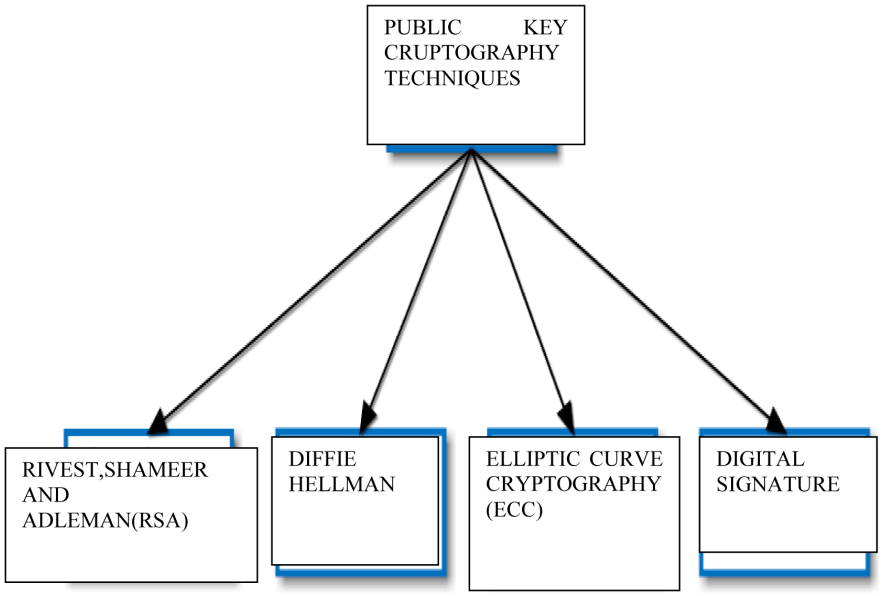

Figure 3. Public key cryptography techniques.

In the key generation phase, each user generates a public key and a private key pair by selecting two large prime in a random order. It uses Euler's theorem, square and multiply algorithm for exponentiation. A repeated squaring is performed on the base number and the exponents are multiplied to compute the result. Figure 4 shows the workflow of key generation process in RSA.

Steps for key generation

Step 1: Two dissimilar large prime numbers are selected in random.

Step 2: The key length of the public and private keys are represented in bits. The modulus of the keys are calculated as $m = a \times b$.

Step 3: The Euler's function is calculated as $\varphi(m) = \varphi(a)\varphi(b) = (a-1)(b-1)$.

Step 4: An integer for public key, namely, $encr$ that lies between 1 and $\varphi(m)\left(1 < encr < \varphi(m)\right)$ is selected, in such a way that $encr$ is a co-prime of $\varphi(m)$.

Step 5: The value of private key, namely, $decr$ is computed as follows

$decr \times encr = 1\left(mod\left(\varphi(m)\right)\right)$.

Step 6: The public that is used for encryption $\left(encr, \varphi(m)\right)$ is published.

Step 7: The private key used for decryption $\left(decr, \varphi(m)\right)$ is kept safe along with the random prime numbers a, b and the Euler's function $\varphi(m)$.

In the encryption step, the sender publishes the public key (m, $encr$) and keeps the private key. The padding scheme is used to convert the original data D to cipher text

$$Cipher = D \ mod \ m.$$

In the decryption step, the original data D is obtained as follows:

$$D = Cipher \ mod \ m.$$

Attacks in RSA

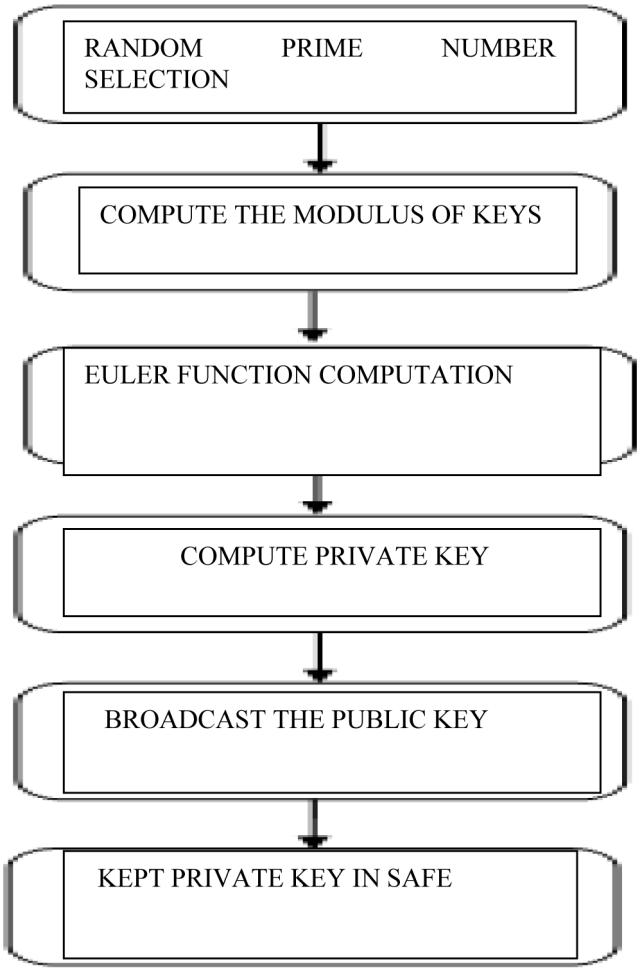

Figure 4. Workflow of RSA.

The RSA algorithm is attacked by brute force key search, mathematical attacks, and timing attacks. The attacks can be resolved by using a constant exponentiation time and by adding random delays.

Some of the three approaches that attack the RSA algorithm are:

Physical Force (Brute Force attack)—it means testing out all the possible private keys.

Arithmetical attacks—the approaches of all equivalent in effect to factoring the product of 2 primes.

Timing incursion (attacks)—these depend on the running time of the decryption algorithm.

Advantages

1. Integrity, authentication, non-repudiation, and secrecy and privacy are the features of RSA algorithm.
2. Private keys are never exposed.
3. Non-repudiation can be achieved using the digital signatures provided by RSA.
4. Key strength is high, as the key size is large.

Disadvantages

1. RSA requires exponential amount of time because of large key sizes.
2. Key generation is complex.
3. No tradeoff between time and security.

Applications

1. Secure Socket Layer (SSL) protocol.
2. Secure Shell (SSH) remote connection.
3. Pretty Good Privacy (PGP) to guarantee security and privacy.

4.2. Diffie Hellman Key Exchange

Diffie Hellman key exchange algorithm is used to share a public and private key pair for encryption and decryption in a secure way. This algorithm is name after its inventors Whitfield Diffie and Martin Hellman [12]. Diffie-Hellman is not an encryption algorithm but it is a secure key exchange algorithm, which accomplishes secure exchange by creating a shared secret key. The symmetric key is encrypted using the shared secret key for secure transmission. The public key is certified by the certificate authority to prevent man-in-the-middle attack. Any number of participants can take part in secure exchanges by performing iterations on the agreement protocol and exchanging intermediate data. Here, two users, who are unknown to each other share secret key via an insecure channel. Initially, both of them share a public key for authentication. The third party may access the keys, while transmission, which is commonly known as man in the middle attack [13]. It may alter the key shared between both the sender and the receiver. The workflow of key exchange process is illustrated in **Figure 5**.

Steps for key exchange

Step 1: Two integers such as a prime number P and a generator G is selected by both the sender and the receiver.

Step 2: Two random numbers a, b that are less than the prime number are selected as private keys.

Step 3: The public keys of the sender and the receiver is computed as follows:

Public key of sender: $G^a mod\ P$;

Public key of receiver: $G^b mod\ P$.

Step 4: These public keys were exchanged between the sender and the receiver via an insecure channel.

Step 5: The private keys are calculated as follows:

Private key of sender: $\left(G^b mod\ P\right)^a$;

Private key of receiver: $\left(G^a mod\ P\right)^b$.

Step 6: Then, the shared secret key of both the sender and the receiver must be same *i.e.*,

$\left(G^b mod\ P\right)^a = \left(G^a mod\ P\right)^b$.

Advantages

1. Improves security for the shared secret key.
2. As the key size is small, the computation is fast.

Disadvantages

1. Messages cannot be encrypted using Diffie Hellman algorithm.

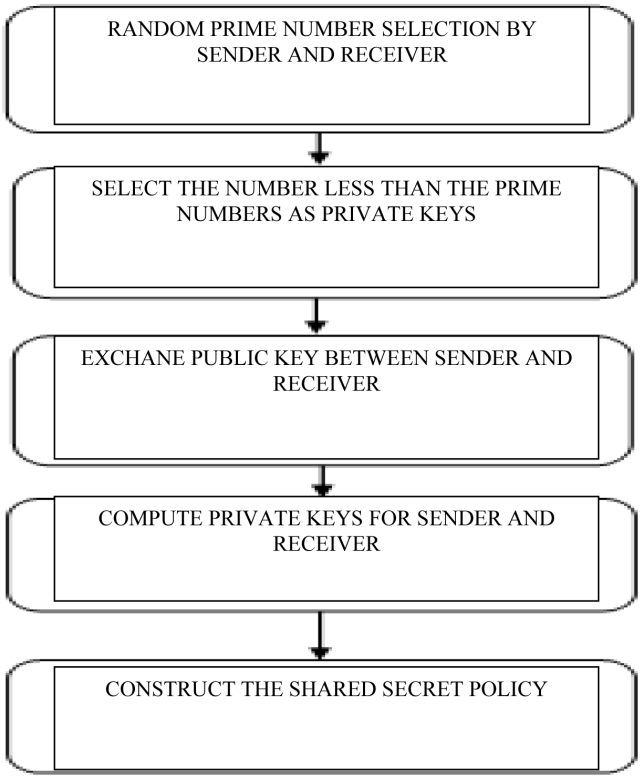

Figure 5. Workflow of key exchange.

2. Prone to denial of service and man in the middle attacks [14].
3. No authentication between the sender and the receiver [14].
4. Lack of forward secrecy [15].

Applications

1. Secure Socket Layer (SSL) protocol [16].
2. Internet Protocol Security (IPSec).
3. Public Key Infrastructure (PKI).
4. Secure Shell (SSH) remote connection [16].

4.3. Elliptic Curve Cryptography (ECC)

Elliptical curve cryptography (ECC) is one of the public key encryption technique that generates best cryptographic keys according to the elliptic curve theory. It creates smaller keys within a short period. Rather than using large prime numbers for key generation, ECC uses the properties of elliptic curves to generate keys. Elliptic curve is a nonsingular cubic curve with two variables in a certain field and an infinite rational point [17]. Each user generates a public-private key pair, where the public key is applied for encryption and signature verification and the private key is applied for decryption and signature generation. The high level of security can be achieved in ECC using a 164 bit key, where the traditional techniques need 1024 bit key. ECC is widely used because of its low computing complexity and better utilization of batter power. Security is attractive feature of elliptic curve cryptography. **Figure 6** shows the key processes in ECC.

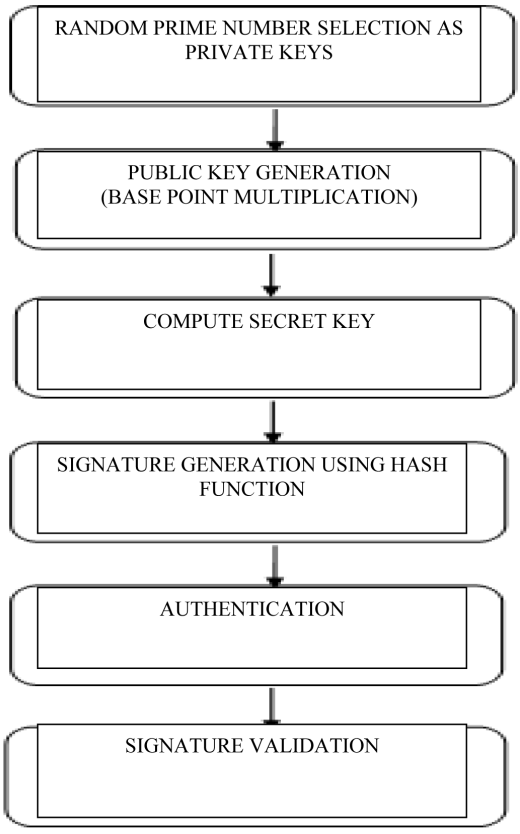

Figure 6. Workflow of ECC.

ECC includes the following major steps [17]:

- Key generation;
- Signature generation;
- Encryption;
- Decryption;
- Signature verification.

Steps for ECC

Step 1: The sender and receiver selects two integers $Pri\ A, Pri\ B$ as private keys.

Step 2: The public keys of both sender and receiver are generated by multiplying the base point B of the elliptic curve with the corresponding private keys.

Public key of sender: $PubA = PriA \times B$;

Public key of receiver: $PubB = PriB \times B$.

Step 3: The security key is generated as follows:

Secret Key of sender: $SK = PriA \times PubB$;

Secret Key of receiver: $SK = PriB \times PubA$.

Step 4: The signature is generated using the hash functions.

Step 5: The signature is sent to the receiver for authentication.

Step 6: At the encryption phase, the message is converted into cipher text using the public keys and a point on the curve.

Step 7: The cipher text is decrypted at the receiver end using the private key.

Step 8: The signature is validated, if the sender's public key is encoded in it.

Advantages

1. Strong security with small keys.
2. Faster performance.
3. Low computational complexity.
4. Increased level of authentication and confidentiality.

Disadvantages

1. Size of the encrypted message is increased.
2. Implementation is difficult.

Applications

1. Secure Socket Layer.
2. Debit/Credit cards.
3. E-mails.

5. Digital Signature

The digital signature standard is used to detect unauthorized modifications and to verify the document's identity. The digital signature is represented as binary digits and computed using a set of rules and parameters. The signature is generated by the use of a private key, which is known only to the user [18]. The signature is verified using a public key that is corresponding to the private key. The signature is generated by the user with the help of the private key, which is never shared. A Secure Hash (SSH) function is used in the signature generation process to obtain a condensed version of the data called a message digest. A digital certificate contains the digital signature of the certificate issuing authority so that anyone can verify the originality of the certificate [19]. The digital certificates will expire after specific duration, which results in insecurity.

Advantages

1. Legal compliance.
2. Less processing time.
3. Reduced overhead.
4. Improved security.

Disadvantages

1. Short life span.
2. Complicates sharing in case of incompatibility.

Applications

1. E-mails.
2. Fund transfers.
3. Data interchange.
4. Software distribution.

6. Results and Discussion

In general public key encryption, or asymmetric encryption, is about 10,000 times slower than private key encryption. This is because of the use of two different keys for encryption and decryption. Even though, they are smaller they provide high degree of security.

6.1. RSA vs. Diffie-Hellman

Diffie-Hellman allows two users A and B, who have never met anywhere, they decide to work together and establish a secret key in order to communicate secretly manner, even in the presence of some intruder. In RSA only the Receiver needs to perform calculations to establish what is called a secret key and a public key. The Receiver doesn't have to necessarily know the Sender of the messages.

6.2. RSA vs. ECC

RSA is commonly used cryptography scheme to provide data confidentiality in cloud storage. As the key size increases, the security also increases and storage capacity required to store key in key management server will be large. Security is attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient RSA and Diffie-Hellman. The computation time of ECC is less when compared to RSA and Diffie Hellman, but it is more complex to implement [20]. RSA and Diffie-Hellman algorithms dominate public-key cryptography and have proved its efficiency in real-world applications. ECC promises particularly in smart cards or other restricted environments. The ECC and RSA are compared in terms of key generation time, signature generation and verification time.

Table 1 compares the key sized of RSA, Diffie Hellman and ECC techniques with the symmetric scheme [20]. The key size for symmetric cryptography ranges from 80 to 256 bits, 1024 to 15,360 bits for RSA and Diffie Hellman respectively. But, the key size variations for ECC are 160 to 521 bits. The public, private key generation and the signature generation through the random numbers on elliptic curve reduces the key size considerably. As the symmetric key size increases, the key size of RSA, Diffie Hellman and ECC also increases. The size of ECC is twice that of symmetric key and the key size of RSA and Diffie Hellman increases in terms of exponents. Table 2 Comparison of key generation time and Table 3 Comparison of signature generation time

Table 2 depicts the comparison of key generation time of RSA and ECC schemes [20]. By varying the key length from 1024 to 15,360 bits, the time required for key generation increases linearly. In RSA, the minimum time required for key generation is 0.16 secs for 1024 bits and the maximum time is 679.06 secs for 15,360 bits. Similarly, the time required for key generation in ECC is 0.08 and 1.4 secs for the key size of 163 and 571 bits respectively. The comparative analysis between the RSA and ECC states that the proposed EC offers significant performance improvement. The key lengths are measured in bits and the key generation time is computed in seconds. The key generation time varies based on the key length. As the key length increases, the key generation time also increases. Table 3 shows the time requires to generate the signature in RSA and ECC techniques [20]. The signature is generated for user authentication and it is measured in terms of seconds. The time required for signature generation depends on the key size.

By varying the key length from 1024 to 15,360 bits, the time required for sig-

Table 1. Key size comparison.

Symmetric key size (bits)	RSA and Diffie Hellman key size (bits)	Elliptic Curve Cryptography key size (bits)
80	1024	160
112	2048	224
123	3072	256
192	7680	384
256	15,360	521

Table 2. Key generation time analysis.

Key length (bits)		Key generation time (s)	
RSA	ECC	RSA	ECC
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	283	9.8	0.27
7680	409	133.9	0.64
15,360	571	679.06	1.4

Table 3. Signature generation time analysis.

Key length (bits)		Signature generation time (s)	
RSA	ECC	RSA	ECC
1024	163	0.01	0.15
2240	233	0.15	0.34
3072	283	0.21	0.59
7680	409	1.53	1.18
15,360	571	9.2	3.07

nature generation increases linearly. In RSA, the minimum time required for signature generation is 0.01 secs for 1024 bits and the maximum time is 9.2 secs for 15,360 bits. Similarly, the time required for signature generation in ECC is 0.15 and 3.07 secs with respect to key length variations. The comparative analysis between the RSA and ECC states that the proposed EC offers significant performance improvement.

Table 4 presents the comparison of signature verification time of RSA and ECC schemes [20]. By varying the key length from 1024 to 15,360 bits, the time required for signature verification increases linearly. In RSA, the minimum time required for signature verification is 0.01 secs for 1024 bits and the maximum time is 0.01 secs for 15360 bits. Similarly, the time required for signature generation in ECC is 0.23 and 4.53 secs with respect to the key length variations. The signature is verified at the decryption stage and it also depends on the key length. As the number of bits in the key size increases, the time required for signature verification also increases.

Table 4. Signature verification time analysis

Key length (bits)		Signature verification time (s)	
RSA	ECC	RSA	ECC
1024	163	0.01	0.23
2240	233	0.01	0.51
3072	283	0.01	0.86
7680	409	0.01	1.80
15,360	571	0.03	4.53

7. Conclusion

This paper addressed the limitations in the security assurance and the data privacy limitations with increase in size of the data on cloud. The evolution of cryptographic approaches addressed these limitations and provided the solution to the preserving process. Due to the multi-tenancy property of the cloud, server and the geographical factors limited the security of the cloud data access and storage. This paper surveyed about the various cryptographic techniques with their key sizes, time required for key/signature generation and verification constraints. The survey discussed the architecture for secure data transmissions among the devices, challenges raised during the transmission and attacks. This paper presents the brief review of major cryptographic techniques such as RSA, Dffie Hellman and the ECC associated key sizes. This paper investigated the general impact of digital signature generation techniques on cloud security with the advantages and disadvantages. The results and discussion section existing in this paper investigated the time consumption for key/signature generation and verification with the key size variations effectively. Finally, the results of these approaches were compared in terms of key size, key generation time, signature generation time and signature verification time. The initialization of random prime numbers and the key computation based on the points on the elliptic curve assured the high-security compared to the existing schemes with the minimum time consumption and sizes in cloud-based applications.

References

[1] Vuyyuru, M., Annapurna, P., Babu, K.G. and Ratnam, A. (2012) An Overview of Cloud Computing Technology. *International Journal of Soft Computing and Engineering*, **5**, 2231-2307.

[2] Asma, A., Chaurasia, M.A. and Mokhtar, H. (2012) Cloud Computing Security Issues. *International Journal of Application or Innovation in Engineering & Management*, **1**, 141-147.

[3] Agrawal, M. and Mishra, P. (2012) A Comparative Survey on Symmetric Key Encryption Techniques. *International Journal on Computer Science and Engineering*, **4**, 877.

[4] Kaur, M. and Kaur, K. (2016) A Comparative Review on Data Security Challenges in Cloud Computing. *International Research Journal of Engineering and Technology*, **3**, 334-339.

[5] Chen, D. and Zhao, H. (2012) Data Security and Privacy Protection Issues in Cloud Computing. 2012 *International Conference on Computer Science and Electronics Engineering*, Hangzhou, 23-25 March 2012, 647-651. https://doi.org/10.1109/ICCSEE.2012.193

[6] Rao, R.V. and Selvamani, K. (2015) Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, **48**, 204-209. https://doi.org/10.1016/j.procs.2015.04.171

[7] Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S.U., Buyya, R., *et al.* (2015) Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues. *ACM Computing Surveys*, **47**, 65. https://doi.org/10.1145/2764465

[8] Bhore, R.S. and Sheikh, R. (2015) Technical Review on Security Issues & Cryptographic Algorithm in Cloud Computing.

[9] Ren, K., Wang, C. and Wang, Q. (2012) Security Challenges for the Public Cloud. *IEEE Internet Computing*, **16**, 69-73. https://doi.org/10.1109/MIC.2012.14

[10] Wu, L., Zhou, S., Zhou, Z., Hong, Z. and Huang, K. (2015) A Reputation-Based Identity Management Model for Cloud Computing. *Mathematical Problems in Engineering*, **2**, 1-15. https://doi.org/10.1155/2015/238245

[11] Mahajan, S. and Singh, M. (2014) Analysis of RSA Algorithm Using GPU Programming. arXiv:1407.1465 [cs.CR]

[12] Gola, K.K., Rathore, R., Sharma, V. and Kandpal, M. (2015) Secure Key Exchange in Diffie-Hellman Key Exchange Algorithm.

[13] Chaturvedi, A., Srivastava, N. and Shukla, V. (2015) A Secure Wireless Communication Protocol Using Diffie-Hellman Key Exchange. *International Journal of Computer Applications*, **126**, 126-132.

[14] Boni, S., Bhatt, J. and Bhat, S. (2015) Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm. *International Journal of Computer Applications*, **130**, 7-10.

[15] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J.A., *et al.* (2015) Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, 12-16 October 2015, 5-17. https://doi.org/10.1145/2810103.2813707

[16] Garg, V. and Ri, S.R. (2012) Improved Diffie-Hellman Algorithm for Network Security Enhancement. *International Journal of Computer Technology and Applications*, **3**, 1327-1331.

[17] Setiadi, I., Kistijantoro, A.I. and Miyaji, A. (2015) Elliptic Curve Cryptography: Algorithms and Implementation Analysis over Coordinate Systems. 2015 2*nd International Conference on Advanced Informatics: Concepts, Theory and Applications*, Chonburi, 19-22 August 2015, 1-6. https://doi.org/10.1109/icaicta.2015.7335349

[18] Pornin, T. (2013) Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA).

[19] Poulakis, D. and Rolland, R. (2015) A Digital Signature Scheme Based on Two Hard Problems. Springer International Publishing, New York, 441-450. https://doi.org/10.1007/978-3-319-18275-9_19

[20] Sinha, R., Srivastava, H.K. and Gupta, S. (2013) Performance Based Comparison Study of RSA and Elliptic Curve Cryptography. *International Journal of Scientific & Engineering Research*, **4**, 720-725.