Secure and Efficient Authentication Scheme for Cloud Computing

Mohamed M. Zarad
Master Student, Elec. & Comm Dep., Faculty of Engineering
ASU, Egypt

Ahmed A. Abdel-Hafez
Communications Department
Military Technical Collage
Egypt

Ahmed H. Hassanein
Egyptian Armed Forces

ABSTRACT
Cloud computing is a new, promising emerging technology which provides a variety of services over the public network. Such as software, hardware, data storage and infrastructure services. It is widely used because it offers high processing power, wide range of storage space and high computational speed. It provides a convenient on demand network access to a pool of shared services and resources via public networks. So enterprises can use the available services and resources to develop, host, and run services over their infrastructure in a flexible way anytime, anywhere with minimal management efforts. This makes cloud computing efficient, flexible and cost effective tool for business development and growth.

On the other hand, the adoption of cloud computing suffers from security and privacy deficiency, which became significant challenge.

In this paper; an efficient and provably secure authentication mechanism is proposed to give a legitimate user the right to access and manage the cloud resources.

Keywords
MDHA, CUA, ECC

1. INTRODUCTION
Cloud computing is a new technology which provides a convenient way for accessing configurable resources among users (e.g., networks, servers, services and applications) by using the concept of virtualization, storage connectivity and processing power[1]. The NIST defines five essentials features for cloud computing which makes cloud computing technology a huge development challenge. These features provide clear understanding for cloud computing technology and the provided services of the cloud, these five features are: [2]

On-demand self-services, resource pooling, broad network access, rapid elasticity and measured service. These features can be offered in different services model to provide convenient and flexible way for efficient services delivery for cloud consumers. These services models can be described as follows:

1.1 Infrastructure as a service (Iaas)
It is the capability provided to the consumer to provision processing storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications.

1.2 Platform as a service
The capability provided to the consumer to deploy consumer created applications into the cloud infrastructure that are created using programming languages and tools supported by the provider. The consumer doesn't manage or control the underlying cloud infrastructure including networks, servers, operating systems or storage spaces but has control only over deployed applications.

1.3 Software as a service (saas)
The capability provided to the consumers to use the provider's applications running on cloud infrastructure. These applications are accessible from various client devices through client interface such as, web browser. The consumer doesn't manage or control cloud infrastructure including network, servers and operating systems. It allows users to run only online applications according to service agreement between users and providers. Figure (1) shows the different service models provided by cloud computing with examples for each service model.

The rest of the paper will be organized as follows: In section II the vulnerabilities and attacks to the cloud computing will be studied; Section III introduces and discusses the existing cloud computing authentication protocols. As an underlying used technology, Elliptic Curve cryptography will be briefly discussed in Section IV. The proposed protocol will be presented and analyzed in Section V, VI respectively. The conclusion and lines for the future work will be presented in section X.

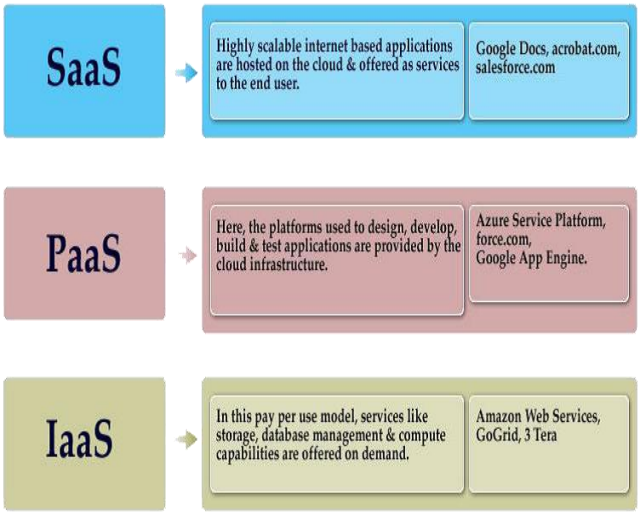

Figure-1 Cloud Computing Service Models

2. VULNERABILITIES AND ATTACKS
Despite the benefits of cloud computing which include large capacity, high processing power, high computational power and the cost effectiveness of cloud computing. There are some challenges that face the users of the cloud. The most sensitive and effective challenge is the security issue. Security in cloud computing protects the rights of each user in using the cloud services and resources and protects the sensitive data of each user in the cloud from attacks or breaching. So there are some

vulnerabilities and attacks that face the users of the cloud which hinder an effective usage of the cloud resources and services; and deprive the service provider from efficient delivery of the resources and services to the users. These vulnerabilities can be described as follow: [3]

2.1 Unauthorized access to management interface

Since on demand characteristics of cloud computing requires a management interface that accessible to cloud service users. So unauthorized access to the management interface is a relevant vulnerability for cloud system since the management function is accessible only to a few users.

2.2 Internet protocol vulnerabilities

Since the cloud services and resources are available anywhere .Theses services and resources are accessed via public network such as internet which considered untrusted. So internet protocol vulnerabilities as Man in The Middle Attack and IP spoofing will hinder the performance of the cloud.

2.3 Data recovery vulnerability

The cloud characteristics of pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at later time. For memory or storage resources it might be possible to recover data written by a previous user.

2.4 Metering and billing evasion

The cloud characteristics of measured services means that any cloud service has a metering capability at an abstraction level appropriate to the service type (as storage, processing, and active user account). Altering data is used to optimize service delivery as well as billing.

2.5 Malware injection attack

These types of attacks are web based attacks in which hackers exploit vulnerabilities into web application and embed a malicious code which change the behavior of its normal execution. Cloud systems are also subjected to malware injection attacks. Hackers design malicious applications, programs, and virtual machine and inject them to target cloud service models. Once this malicious is executed the hackers can do whatever he/she desire such as: eavesdropping, data manipulation and data theft.

So due to aforementioned vulnerabilities, security challenges become the most important and significant issue for cloud computing. Since the consumers of the cloud accessing the cloud services using open network a strict authentication technique and key exchange protocol is required to give the right for the legitimate users to access the cloud services and resources.

In the next sections; different authentication schemes are investigated using different authentication protocols such as Diffie-Hellman, RSA. The presented paper also introduces a comparison between RSA and elliptic curve Diffie Hellman as two authentication protocols and key exchange algorithms.

3 RELATED WORK

Since the rapid growth of using cloud computing services and the tremendous increasing in the number of users of the cloud services and resources, accessing the cloud environment securely is an important and critical issue. Many authentication mechanisms were introduced to control the accessing to the cloud services depending on different authentications protocols. For choosing authentication protocol for the cloud environment many factors must be considered to be efficient and reliable for the security of the accessing process of the cloud services and resources.

In 2014 an authentication scheme was introduced by Faraz fatema et al [4] depending on the concept of agents. Two agents were used in this scheme: client based user authentication agent(CUA): It is an extension that installed in end user web browser to confirm the identity of user before accessing cloud servers, so users need to register their devices to service provider web site downloading an extension with unique code encrypted with AES-192or AES-256 on client side. The user will decrypt the code and set the decrypted code on installed extension. Modified Diffie Hellman agent (MDHA) another agent used for accessing cloud servers with unregistered devices. By using MDHA temporary access permission has been provided for user for accessing from unregistered device. This model uses AES-256 and RSA-2048 during authentication and before Storing data to the cloud servers which improves the rate of trust in the framework.

In 2013; Iman Ghavam et. al. [5] introduce an authentication scheme including two main steps: client based encryption algorithm for encrypting data before uploading to cloud servers and user authentication secure key exchange algorithm for validating user legal identities and control acquiring services from the cloud.Acoording to this model RSA small e algorithm has been chosen for encryption process by using public exponent much smaller than q(n). Using small exponent will decrease the effective cost of encryption process. Using zero knowledge proof modified Diffie Hellman solves the authentication problems and let the owner to upload shared data without any concern about authentication of the sharer.

The main drawbacks of Diffie Hellman &RSA Algorithms are the slower processing time and the requirement of high storage capacity of 1024 bits. The slower of encryption and decryption due the complexity of generation of the keys required for encryption and decryption. The requirement of certificate authority for RSA requires a large storage capacity and verification of certificates slows down the system performance due to complexity of key creation because RSA is limited by the prime and efficiency of generating primes which need a lot of calculations that slow down the encryption and decryption process.

In this work, an authentication scheme and key agreement protocol using Elliptic curve Diffie-Hellman will be introduced.

There are many reasons that lead to the using of Elliptic curve Diffie Hellman for authentication of cloud computing compared with RSA & Diffie-Hellman. The following sections will introduce elliptic curve concepts and how it is used in cryptography to provide an efficient and reliable way to control the access to the cloud services and resources.

4 ELLIPTIC CURVE

Elliptic curves in cryptography were discovered in 1985 by Victor Miller and Neil Koblitz as different protocol for implementing public key cryptography [6]. In public key cryptography each communicating party has a pair of keys one is public key and the other is private key. Only the particular user knows the private key whereas the public key is distributed to all users. As some public key algorithm requires a set of predefined parameters to be known by all communicating parties, as an example of this are the domain parameters in ECC. The operations of ECC are defined over the Elliptic curve. $y2= x3+ax+b$.

Where $4a3+27b2 \neq 0$, so that for each value of a&b gives a different elliptic curve so that all points (x,y) which satisfies the

above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and private key is a random point over the same curve.

4.1 Security of elliptic curve

The main issue which describes the security of elliptic curve cryptography is the difficulty of Elliptic curve discrete logarithm problem [7]. For example:

If P&Q are two points on an Elliptic Curve so that KP=Q; where K is a scalar value so that if P&Q are known, it is computationally infeasible to obtain K. If K is sufficiently large; it can be considered as the discrete logarithm of Q to the base Q. Hence the main operation in ECC is point multiplication so multiplying of a scalar k with any point p on the curve the result of this multiplication is another point Q on the same curve.

Point multiplication over ECC defined as the repeated addition of a point along the curve e.g.: KP=P+P+P+P+……. k times where k is a scalar integer and p(x, y) is any point on the curve. Point multiplication over ECC is achieved by two main operations and the result will be another point on the same **ECC.**

4.2 Domain parameter of ECC

Since the elliptic curve is defined by the equation

y2= x3+ax+b[8] so that for a given value of a and b the plot will give a negative and a positive value of Y for each value of X. Rather than a and b there are some domain parameters which define the ECC this domain parameters must be agreed between communicating parties for secure and reliable communications. These parameters differ from the field over which the ECC is generated and defined.

The main attractive features of Elliptic Curve are not limited to security features only. Elliptic curves are more computationally efficient compared with RSA and Diffie Hellman. The smaller key size of ECC improves the computational time and decrease the requirement of the required storage space of the algorithm parameters. In the following section a brief comparison between RSA and elliptic curve Diffie Hellman as two authentication algorithms.

4.3 Methods of generation of Elliptic curves

There are many methods for generating Elliptic Curves which depends on the applications that will use this Curve. Another factor that must be considered on choosing the method of generation is the time efficiency of generating the curve and the available storage resources for the curve parameters.

4.3.1 Random Approach of Generating Elliptic Curve

This approach based on choosing a random curve E. using an efficient point counting algorithm [9] to determine the curve order. Once the group is known it can be determined whether the group can be used in cryptography or not. If the curve is proved that it cannot be used in cryptosystems another curve is chosen.

4.3.2 Complex Multiplication Method of Generating Elliptic Curve

Generating the Elliptic Curve using this method first determines a suitable order for the curve then constructs an EC of that order [10]. The input of this method is a prime P (the order of the prime field) from which complex multiplication discriminate D is computed. The EC is generated by constructing certain polynomials based on D and find their roots. This method is the most familiar and widely used. There are two variations of this method depend on whether Hilbert or Weber polynomials is used for construction of the curve. Hilbert polynomials have huge coefficient as discriminate D increases while a smaller coefficient with the same discriminate for Weber polynomials. So for hardware implementation of CM Method Hilbert polynomials will not be appropriate due to the requirement of large registers and floating point for their construction and storage. Another factor that is considered critical and important for generating of the Elliptic Curve is the Base Point Selection or Generator Point of the ECC.The base point considered the most critical factor on choosing the curve. The efficiency of choosing the base point of The ECC will reduce the time complexity of the algorithm thereby reducing the overall computational cost. There are many methods of choosing the base point. Some chooses a random point on the curve as the base point while others chooses the smallest point on the curve as the generator point of the curve.

The following comparison shows how efficient the ECC compared with RSA in performance and efficiency term.

4.3.3 Advantages of Using Elliptic Curve Over RSA:[11]

a) Smaller key size compared with RSA (163bit of EC gives 1029 RSA).

b) Less computational complexity due to smaller key size.

c) Fast generation due to less requirement of storage space.

d) Fast encryption and decryption process.

In the following a key size comparison among the elliptic curve, RSA and Diffie- Hellman will be showed (table-1) :

Symmetric key size (bits)	RSA and Diffie-Hellman key size (bits)	Elliptic curve key size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1

From the previous table it is obvious that the main advantages of using Elliptic Curve Diffie-Hellamn as an authentication scheme is the smaller key size. This helps in that the implementation of the encryption and decryption process will be much faster than of that of RSA as 1024bits key size of RSA is equivalent to 160 bits of ECC. Consequently, the use of Elliptic Curves can be more efficient and reliable than RSA. Otherwise the implementation of RSA is easier than that of Elliptic Curve.

5 PROPOSED MODEL

Due to lack of trust, efficiency and scalability in user authentication and access process to the cloud environment.

Therefore an efficient and scalable mutual authentication scheme algorithm is proposed. In this paper a mutual authentication scheme is proposed using 160 bits Elliptic Curve

Diffie Hellman to authenticate the users requesting access to the cloud environment and the authentication server according to pre-defined parameters. The smaller key size of Elliptic curve and the lower storage capacity compared with other authentication algorithms enhance the security performance of the authentication process. The proposed model tries to enhance the performance of the authentication process and defend against security attacks as Man-in-The-Attacks and replay attack. The encryption of the generated random numbers from the user and the server protect against replay attacks and using SHA-1as signature algorithm provides a pre authentication tool before accessing the cloud services. The steps of the proposed model are as follows:

1-User calculates the hash value for his password using sha1 generating hash value less than 160 bits. The using of Hash algorithm will verify the message integrity and assure that the message has not been changed or corrupted. This hash value will be used after that as a reference when it compared with the stored hash code in the server to verify user authentication attempts. Since this hash value produced from a one way function so it can't be regenerated. It is only compared with the hash value that will be generated from the server with the function

2-The user then generates random number **R1** from pseudo random generator. The generated random number is used in the proposed protocol to ensure that old communications cannot be reused in any attacks. This random number also can be used in stream cipher to ensure that the key stream is different for every session by generating random nonce for every session.

3-The user generates a timestamp T1. The generated timestamp protect against replay attack. The value of the timestamps must be with acceptable range of time.

A precision time must be identified between the server and the user to make it possible for every communicating parties to determine whether the message timestamp is too old or fresh. By using timestamps concatenated with the hash value of the server.

The user can assure that the message from authorized party.

The user then sends his ID concatenated with the hash of his password concatenated with timestamp T1 concatenated with random number R1 encrypted with AES-256 to the server. The encryption of these parameters over the communicating channel will protect against modification or alteration from unauthorized opponent.

4- The server receives the parameters from the user and starts the checking process by verifying the ID of the user from the pre stored database in the server. This assures the identity of the sender and that the message comes from authorized user

5-The server checks the timestamp to assure that replay attacks doesn't occurs by comparing the received time of the message with the timestamp of sending the message. This assures the freshness of the message by keeping a track of creation and modification time of the message.

6-Server calculates the hash value and compares it with the received value from the user. Since the creation of the hash value in the server from a specific function must be matched with the created value in the server using the same function.

7-Server checks the previous parameters (comparing the received timestamp with the transmitted one, checking the ID of the user and compare the received hash with the computed one) and if the check succeeded.

8- Server will generate random number R2 from its pseudo generator which will assures that old communications and Man in The Middle attack is not involved in communication from the server to the user.

9- A timestamp T2 is generated as a reference time compared with the received time from the user. The timestamp T2 must be with acceptable range relative to T1. The server will send the generated random number R2 concatenated with R1 and timestamp T2 encrypted with AES-256 to the user. The sending of R1 to the user will give assurance to the user that the message is originated from the server by comparing it with the generated one.

10-The user will check the received message from the server and check the random number R1 to assure that the received message is from the server by comparing the received value with the stored one.

11-The user checks the received value R2 which assures that the received message comes from the server

12-The user checks the timestamp T2 to assure that no message replay occurred and the received time is within acceptable range with the sending time.

13- After the check succeeded, user generates Q_U by multiplying the hash of the random number R_1 by the generating point of the curve G and send Q_U to the server.

$$Q_u=Hash(R_1)*G$$

14- The server also generates Q_S by multiplying the hash of the random number R_2 with the same generating point of the curve and send Q_S to the user.

$$Q_s = Hash(R_2)*G$$

After exchanging the value of Q_S and Q_U between the user and the server a mutual authentication between the server and user is achieved. So that every time the value of the random number changed the hash will be changed and the value of Q will be also changed due to changing the value of hash of the random number. Figure 2 depicts the summary of the proposed protocol.

6 SECURITY ANALYSIS

Evaluation process of the proposed model has been done according to the following parameters:

1- The protection against unauthorized access by the using SHA-1 algorithm to verify that the service request is from authorized user by comparing the hash of the password of the user by the stored hash in the data base of the authentication server.

2 -The use of timestamp between the user and the server protects against replay attack as the time comparison between the user and the server assure that old communication is not replied or take part in communications.

3- The use of AES-256 for encrypting the data between the user and the server will protect against Man in The Middle attack since the opponent cannot compute the key that is used for encryption or decryption.

4-Mutual authentication: The proposed model provides a strong mutual authentication between the user and the authentication

server. The user challenges the authentication server in the authentication request message encrypting his identity by using secret key computed by the user. Only the server can recomputed the secret key and retrieve the user identity.

5- The using of ECC as authentication algorithm provides an efficient and scalable tool for authenticating the user with the server due to its smaller key size. Complex multiplication method is used in generation of the curve due to smaller space storage that is used in storing the field parameters, which improves the computational cost and efficiency. The performance of ECC depends mainly on the efficiency of finite field computations and fast algorithms for elliptic scalar multiplications. In addition to the known algorithms for these computations the performance of ECC can be sped by selecting appropriate finite field and/or elliptic curves.

6- Identity based encryption of the user and the authentication server which allow the sender to encrypt a message to an identity without access to a public key certificate authority. The user uses his id and calculate the hash value for his password and encrypt these parameters then sends these parameters to the server which make the same procedures and make the required comparison using the received parameters from the user to assure the identity of the user. The sending and receiving of these parameters between the sender and server act as the domain parameters which must be agreed between the communicating parties as an initiating step for authentication and generating of the session key between the user and the server.

7-Confidentiality and message integrity between the user and the authentication server which assure that the received messages contain no modification,insertion,deletion or replay is achieved by using the hash function SHA-1 which calculate the hash value of his password generating 160 bits (hash value).This hash value concatenated with other parameters are encrypted using AES 256 before sending to the authentication server this provides authentication it also provides digital signature because only the user can produce the encrypted hash value. This ensure that the access request is from authorized user since this hash value cannot be accessed without having the key .The server decrypt the message and compare the hash value with the received hash value of user password with the stored one to assure the identity of the sender. So encrypting the hash value of the user password increases the difficulty for the attackers to find efficient way for producing collisions for hash function.

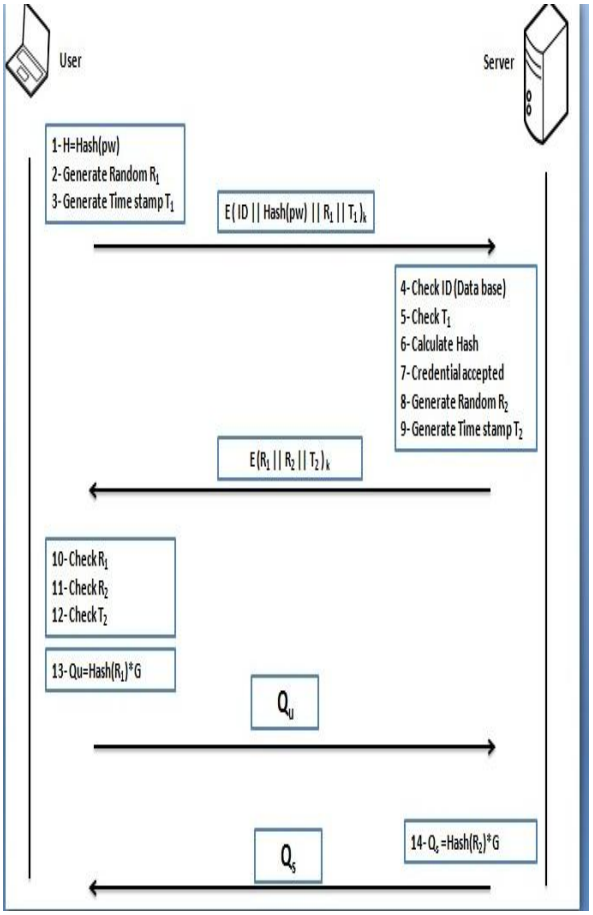

Figure 2 the proposed scheme

7 CONCLUSION AND FUTURE WORK:

With the development of cloud as a new emerging technology and the challenging issue during user authentication and access control in cloud based environment. A strict authentication scheme is proposed to control the access to the cloud services .The proposed authentication scheme and key agreement protocol has been proved to be more secure and efficient than other authentication schemes. Since using small key size of Elliptic Curve will improve the authentication process due to fast processing of the keys. Using AES-256 as an encryption algorithm protects the data exchange between the user and the server from various attacks. ECC will enhance the computational efficiency and enhance the usage of available storage resources which make it an efficient choice as authentication protocol for cloud computing.

There are different lines for future work to be addressed as: using verification and assessment tools like Scyther, Prover and AVISPA in verification and assessment of the security of the proposed protocol. The performance comparison of the proposed model with other authentication protocols will be held by using programming language (c language).

8 REFERENCES

[1] Kawser wazed nafi , Tonny shekha Kar, A newer user Authentication, file encryption and distributed server based cloud computing security architecture, *International Journal of Advanced Computer Science and Application vol.3, No.10, 2012*

[2] Judith Hurwitz , Robin Bloor, *cloud computing for dummies* Wiley Publishing, 2010.

[3] Bernd Grobauer,Tobias Wakkoschek , Elmar Stocker Understanding cloud computing vulnerabilities, *IEEE Computer and Reliability societies , March 2011.*

[4] Faraz Fatemi , Shiva Gerayeli Moghaddam A scalable and efficient user authentication scheme for cloud computing environments, *IEEE 2014 Region10 Symposlum*.

[5] Shorab Rouzbeh,Iman Ghavam, A client -based user authentication and encryption algorithm for secure accessing to cloud servers, *2013 IEEE Student Conference on Research and Development 16-17 December 2013, putrajaya, Malaysia.*

[6] William Stalling, *cryptography and network security 5 th edition* Prentic Hall, 2011.

[7] Bruce Schneier, *applied cryptography second edition* John Wiley&sons,1996.

[8] Veerraju Gampala , Data security in cloud computing with elliptic curve cryptography, *International Journal of Soft Computing and Engineering, vol-2,July 2012.*

[9] Leonidas Deligiannidis "Implementing Elliptic Curve Cryptography" International Conference Frontiers in Education:CS and CE /FECS 2015

[10] Moumita Roy , Point generation and base point selection In ecc, *International Journal Of Advanced Research in computer and communication research vol.3, Issue 5, MAY 2014*.

[11] Debajoyoti Mukhopadhyay, Architecture to implement secure cloud Computing with elliptic curve cryptography, *Published June 30,2015, https://www.researchgate.net/publication/279534252*