© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Two Level Encryption Decryption by Diffie – Hellman and Elliptic Curve Cryptography with Open ID scenario for Securing Cloud Environment

Arti Pandey, Raghvendra Kumar

Department of Computer Science, LNCT, JABALPUR, Madhya Pradesh, India

ABSTRACT

Cloud Computing offers services to end-users rather than a product, by sharing resources, software and other information under a pay per usage model, hence economic benefit is the key for Cloud in terms of capital and operational expenditure. It permits hosting of different types of applications such as business, scientific and social networking because it has key characteristics like multitenancy, scalability, performance and security etc. Cloud Computing is currently facing challenges like Data Security, Energy Consumption, Server Consolidation, Virtual Machine Migration to name a few. Existing approaches of secure data transfer use two tier authentications, either based on OTP (One Time Password) which is static in nature and requires additional software/hardware or Digital Signature which leads to the problem of key management. This research work focuses on the study of secure data transfer by using different combination of mechanisms which not only ensure two tier authenticities without involving any above mentioned overheads but also maintain the confidentiality of data and integrity of message using one time key generation. In this paper, existing secure data transfer techniques have been compared. A mechanism has been proposed and simulated for secure data transfer. This mechanism ensures three way protections in term of authenticity, confidentiality and integrity based on the concept of single key. This technique uses ECC with Diffie Hellman Key Exchange to enhance data security in terms of authenticity and integrity in Cloud Computing environment. In this mechanism Optimally Modified ECC been used to prevent the man-in-middle-attack. An encryption algorithm has been used to maintain the confidentiality of data in transmits. Flow of the execution stages has been described using Flow Diagram and Sequence Diagram while for GCP (google cloud platform) has been used to validate the experimental results of ECC AND DIFFIE HELLMAN KEY EXCHANGE.

Keywords : ECC, GCP, Cloud Computing Diffie Hellman Key Exchange.

I. INTRODUCTION

Cloud Computing Evolution Idea of delivering computing resources using global network was fixed in the sixties by J.C.R. Licklider. This global network so called internet which came into existence in 1969 as a research project at Advanced Research Projects Agency (ARPA) on behalf of the Ministry of Defense, United State (MoD, US) was initially used for military and scientific purposes, its commercialization started since 1988 with services like e-mail and telnet. So internet is the backbone of all these services which are provided by Cloud Service Provider (CSP). Some experts also say that the concept of Cloud computing is the vision of American computer scientist John McCarthy of MIT (Massachusetts Institute of Technology) given in sixties, he stated that "computation can be delivered as a public utility" [1]. Throughout the life span of 60 years, usage of computers has been evolved spirally from centralized and sharable big size computers in 1970 to decentralize and small personal computers in 1999. Computing power has been distributed. In 2010s, again based on the concept of cost effective sharing, industries started to move to distributed center of compact machines for their computational needs. These centers were invisible to the end clients so called Cloud computing [2]. Cloud computing is based on internet computing that relies on the principal of sharing, with the Cloud computing idea of computing-as-a-service comes to true [3][4].

Cloud computing has evolved through various phases which involves Grid computing, Utility computing and Software as a Service (SaaS) as shown in Figure 1.1.
Grid Computing can be defined as a collection of distributed computing resources with heterogeneous and non interactive workload from multiple sites which are used collectively to reach a common aim but scope of grid computing is very limited mostly to scientific and research work [5]. Utility computing [6] involves the concept of metered services where accordingly of usage users have to pay, means commercialization of services (e.g. traditional electricity and telephonic services) which can be seen as a prediction made by Leonard Klienrock, one of the scientist of ARPA network, comes to true about the utilization of computer network which was in very beginning condition during his era of 1969 [7]. So the Grid and Utility Computing are the foundation stones of Cloud computing. Third phase of the Cloud computing evolution`s is "Software as a Service" (SaaS) which gains popularity in 2010, in which applications and data both reside on vendor`s site server, client who want to access the services connects himself with the remote server through internet like social networking. So SaaS offers fully furnished applications using technologies like Java, Ajax etc. SaaS is only a part of services which is provided by Cloud Services Providers [8]. Cloud computing is an umbrella term which in itself also covers Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Figure 1. Evolution of Cloud computing [9]

Salesforce.com took first step in 1999 by putting the idea of Cloud computing in the market, which delivers its enterprise applications over internet using website. 1.1.2 Cloud Computing Services
Cloud computing is typically divided into three levels of service offerings [19] as shown in Figure 2.

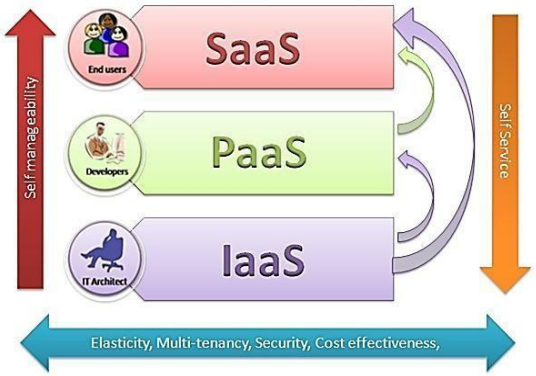


Figure 2. Services of Cloud computing [22]

- **Software as a Service (SaaS)**

Cloud users can access complete application or software remotely as a web service on demand using web browser through internet. Users need not to invest in software license or servers, while for Cloud Services Providers, maintenance costs are lowered because only specific application is hosted. Today Oracle, Salesforce, Microsoft, Google, Amazon have become the giant Cloud Services Providers which deliver Software as a Service business applications. Gmail is an example of Software as a Service.

- **Platform as a Service (PaaS)**

PaaS provides computational resources to the Cloud users through platform. With PaaS, users' gain a platform upon which they can easily create and manipulate applications. With PaaS, developers need not to buy underlying software and hardware; PaaS makes building, testing and delivering of web applications very easy, cost effective and quick. Using PaaS, vendors deal with storage, N/W, server, and operating system, etc but clients handle records and applications. Amazon's AWS Elastic Beanstalk and Google's App Engine are famous PaaS offerings.

- **Infrastructure as a Service (IaaS)**

The basic difference between PaaS and IaaS can be defined in term of degree of control over system resources to the clients. In IaaS, Clients have almost full responsibility to manage the system. With IaaS, Clients decide what configuration of operating system, storage size, networking, type of server and security parameters etc they want. IaaS is suitable for those organizations which have already software packages with themselves and just want to put and run it in the Cloud. Amazon Elastic Compute Cloud (EC2) and Secure Storage

Service (S3), Rackspace, GoGrid are the examples of IaaS offerings.

II. METHODS AND MATERIAL

Related Work

Hybrid Approaches of Security in Cloud Computing

- A single technique can`t provide security in depth in Cloud, it really requires a strong authentication, confidentiality in transit and data integrity. Various approaches have been discussed below which provide different tier of authenticity in order to ensure security.
- Sulochana and Parimelazhagan have described a puzzle based authentication scheme in Cloud computing in which user first registers and solves the puzzle, puzzle solving pattern and time is stored and validated by local server and if user get authenticated, start accessing the Cloud services. Although this scheme ensures 2 tier authentications but static in nature, if attacker once identified the stored pattern, he could easily break the security.
- Yogita et al. have described that not a single technique is enough to provide security in Cloud, she has used Diffie Hellman with digital signature for providing 2 tier authentication. But digital signature uses so many parameter that`s why it is heavy enough and also requires a proper key management.
- Arasu et al. have given a approach of Hash Message Authentication Code (HMAC) in which key, message and hash function is concatenated together for ensuring authentication. This approach describes only single tier authentication which is weak in case of Cloud computing.
- Neha and Ganesan have used Diffie Hellman Key Exchange mechanism for connection establishment and Elliptic curve cryptography for data encryption. In this paper authors used a traditional one tier authentication which is vulnerable to security attacks.
- Govind et al. have provided security using digital certificate authentication method. Here author uses RSA Algorithm for encryption/decryption which is followed by the process of digital certification. This method ensures only single tier authentication using Digital certification which raised a problem of key management.
- Maninder and Sarbjeet have provided an advance multi-tier authentication scheme for enhancing security in financial transactions, in which in first tier, user has to simply pass the traditional login authentication and in second tier a fake screen will appear before user from local server, which is filled by the user by predefined stored pattern, if it is correct then only server will allow access to the resources. Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.
- Satish and Anita have proposed a method of fake screen for ensuring two tier authentication in Cloud computing. In this method of authentication, first user registered himself with Cloud server, and then registered his device. So secret code has been sent to the registered devices which ensure second level of authentication. This method involves additional hardware which is costly and must be along with you every time when you are going to login in the system.
- Parsi and Sudha have proposed method that use RSA algorithm for authentication and data transfer securely. This method involves a phase of key generation, encryption and decryption.
- Timm et al. from Fermi Private Cloud have used a method of X.509 digital certificate for authentication purpose, which is used by many open source Cloud services provider like Eucalyptus and Nimbus. Digital certificate requires both public key and private key for authentication, hence key management is serious issue which needs to be tackled. Apart from this problem, digital certificate requires many others parameters as a purpose of authentication which really makes it heavy enough.

III. RESULTS AND DISCUSSION

Proposed Algorithm and Result

Today, the scientific efforts are looking for a smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments. For any cryptographic, there is an analogue for Elliptic Curve. One of these systems is Diffie – Hellman key exchange system. The proposed methods to encrypt and decrypt the message, by using the Diffie–Hellman Exchanging key which is a secrete point in the proposed

methods (M1) and (M2) we will apply these algorithm for securing cloud environment.

1– Diffie – Hellman key exchange system
This system is merely a method for exchanging key; no massages are involved. The following algorithm illustrates this system. Suppose two communications Alice and Bob, want to agree upon a key.
They first fix a finite field Fq, an elliptic curve E defined over it and a base point B E (with high order). To generate a key, first Alice chooses a random a Fq (which is approximately the as the number N of point of E) which he keeps secret. Next, he calculates aB E that is public and sends it to Bob. Bob does the same steps, i.e. she chooses a random integer b (secret) and calculates bB, which is sent to Alice. Their secret common key is then P = abB E. The following algorithm illustrates this system.

1–1 The Algorithm of Diffie–Helman key exchange system

- Alice and Bob first choose a finite field Fp and an elliptic curve E defined over it (E(Fp)).
- They publicly choose a random base point BE.
- Alice chooses a secret random integer e. He then computes eBE. In addition, send it to Bob.
- Bob chooses a secret random integer d. She then computes dBE. And send it to Alice.
- Then eB and dB are public and e and d are secret.
- Alice computes the secret key edB = e(dB).
- Bob computes the secret key edB = d(eB).

There is no fast way to compute edB if only knows B, eB and dB.

After these setups, Alice and Bob have the same point (only Alice and Bob know it). Then to start with (M1) and (M2), let us consider the following algorithms:

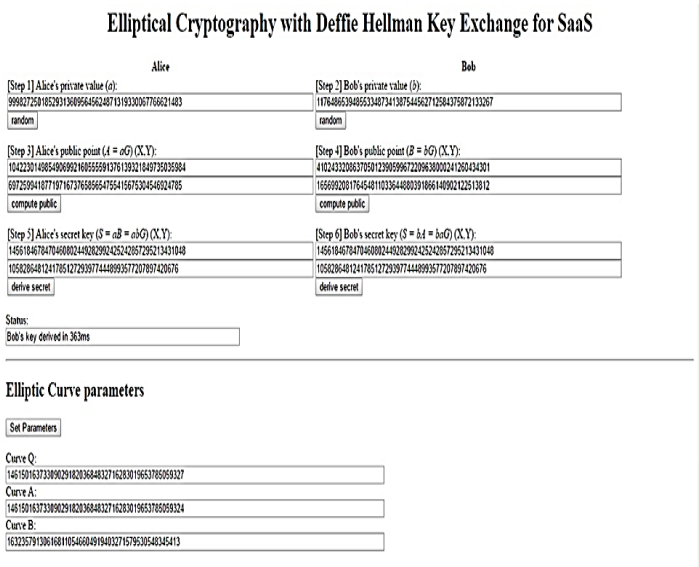
Algorithm of (M1)

Alice and Bob Compute edB = S = (s1, s2). (Using Diffie – Hellman Scheme)
Alice sends a message M E to Bob as follows:
Compute (s1 * s2)modN = K.
Compute K*M = C, and send C to Bob.
Bob receives C and decrypts it as follows:
Compute (s1 * s2)modN = K.
Compute (K–1)modN. (where N = #E)
K–1*C = K–1*K*M = M.

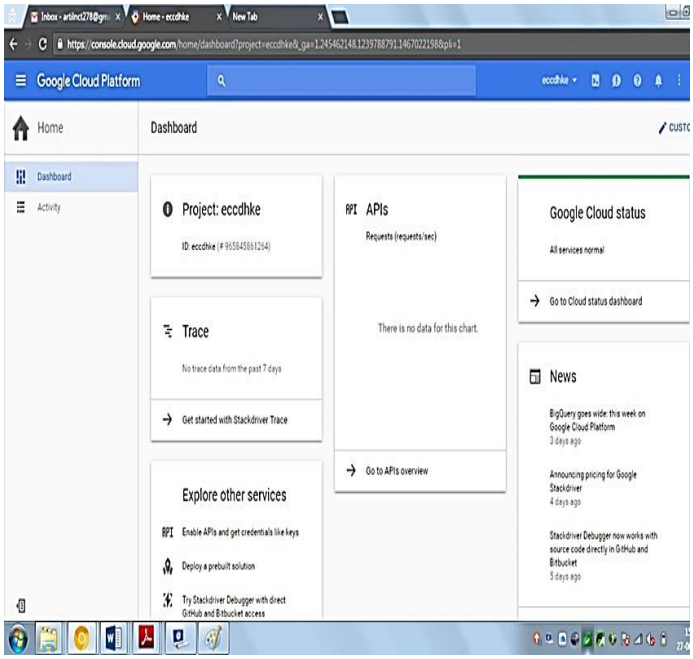
Algorithm of (M2)

Alice and Bob Compute edB = S = (s1, s2). (Using Diffie – Hellman Scheme) Alice sends a message M to Bob as follows:
Compute ()modN = K.
Compute K*M = C, and send C to Bob.
Bob receives C and decrypts it as follows:
Compute ()mod N = K.
Compute (K–1) mod N.
K–1*C = K–1*K*M = M.

(a)this indicate the ECC and diffie Hellman key exchange algorithm working for generating secret key and elliptic curve parameters which acts as SAAS for cloud environment of Google cloud platform(GCP) for IAAS and PAAS.



(b)this indicates the ECC and diffie Hellman key exchange algorithm is deployed as a SAAS in google cloud platform(GCP).



IV. CONCLUSION

This paper gives an introduction to Cloud computing and background of various secure data transfer mechanisms to manage the authenticity, confidentiality and integrity of messages. In this work a secure data transfer mechanism has been proposed which uses Diffie Hellman key exchange algorithm for 3 way protection. Execution stages have been presented using flow and sequence diagram while encryption/decryption working and experimental result of ECC and Diffie Hellman key exchange has been collected using JavaScript which shows proposed parallel execution of Modified ECC and diffie Hellman key exchange algorithm takes less time 1.2seconds as compared to existing one 1.9seconds.

V. REFERENCES

[1] "Cloud Computing Evolution," onlineAvailable: www. computerweekly.com/feature/A-history-of-Cloud-computing. Feb. 20, 2014].

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing", Communications of the ACM, vol.53, no.4, pp. 50-58, 2010.

[3] M. Creeger, "Cloud computing: an overview," ACM Queue, vol.7, no.5, pp. 2, 2009.

[4] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, no. 6, pp. 599- 616, 2009.

[5] I. Foster and C. Kesselman, "The grid 2: blueprint for a future computing infrastructure," Waltham: Morgan Kaufmann Publishers, 2004.

[6] M. A. Rappa, "The utility business model and the future of computing services," IBM Systems Journal, vol. 43, no. 1, pp. 32-42, 2004.

[7] L. Kleinrock, "A vision for the internet," ST Journal of Research, vol. 2, no. 1, pp. 4-5, 2005.

[8] M. Turner, D. Budgen and P. Brereton, "Turning software into a service," Computer, IEEE, vol. 36, no.10, pp. 38-44, 2003.

[9] "Evolution of Cloud computing," onlineAvailable: www.tech.gaeatimes.com/index.php/archive/top-10-Cloud-computing-service- providers-in-2010. Feb. 20, 2014]

[10] "Cloud Watch Hub," onlineAvailable at: http://www.cloudwatchhub.eu/glossary. Oct. 4, 2013].

[11] "Seeding the Clouds: Key Infrastructure Elements for Cloud Computing," onlineAvailable: http://www-935.ibm.com/services/in/cio/pdf/oiw03022usen.pdf. Feb. 20, 2014]

[12] Vaquero, M. Louis, R. Merino, Luis and Maik, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.

[13] "Gartner says contrasting views on Cloud computing are creating confusion," onlineAvailable: www. gartner.com/newsroom/id/766215. Feb. 20, 2014]

[14] M. Brown, "White paper: Cloud computing," Maximum PC, Jan. 12, 2009.

[15] R. Buyya, C. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype and reality for delivering it services as computing utilities", Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, HPCC-OB, IEEE CS Press, Los Alamitos, CA, USA,pp. 5-13, 2008.

[16] P. Mell and T. Grance, "The NIST Definition of Cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, 20