Cloud Computing Security Improvement using Diffie Hellman and AES

Rameshwari Malik
M.Tech Scholar
Gurgaon College of Engineering,
Gurgaon, Haryana

Pramod Kumar
College Guide
Gurgaon College of Engineering,
Gurgaon, Haryana

ABSTRACT
Security is often cited as one of the most contentious issues in Cloud computing. It is argued that as the Cloud is intended to handle large amounts of data, attackers can be sure of a high pay-off for their activities.. In addition, to benefit from the Economies of scale, the applications and operating systems are homogenized to a few images restricting the variations of products used within the Cloud. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services. The future of cloud, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. We propose a simple data protection model where data is encrypted using AES and Authenticated by Diffie Hellman algorithm before it is launched in the cloud, thus ensuring data confidentiality and security.

Keywords
Cloud computing, AES, D-H Algorithm, Security.

1. INTRODUCTION
Cloud computing is emerging as a key computing platform for sharing resources that include infrastructure, software, applications, and business processes. Gartner predicts by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud, with focus on messaging, web security and remote vulnerability assessment. Other focus areas will include data-loss prevention, encryption, and authentication, as technologies aimed to support cloud computing mature [1]. The notion behind cloud computing is that work done on the client side can be moved to some unseen cluster of resources over the internet. Cloud Service Provider (CSP) maintains database and applications for the users on a remote server and provides independence of accessing them from any place through a network. There are three major cloud service categories: software-as-a-service (SaaS), platform-as-aservice (PaaS) and infrastructure-as-a-service (IaaS).

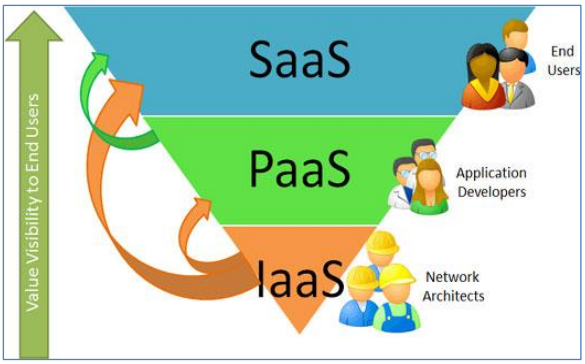

Fig1: Cloud Services

Cloud computing [10] is the broader concept of infrastructure convergence. This type of data center environment allows enterprises to get their applications up and running faster, with easier manageability, and less maintenance to meet business demands. For example, we can manage and store all smartphones or tablets apps at one location i.e. cloud. So we do not require any memory space at our end. This also gives the security of data and applications in case device is damaged or lost. Most of the large companies have promoted their own cloud computing platforms and infrastructures for users to deploy their web applications on these platforms. Within the cloud computing world, the virtual environment lets user access computing power that exceeds that contained within their own physical worlds. To enter this virtual environment requires them to transfer data on the cloud. Consequently, several data storage concerns can arise. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data confidentiality (prevention of unauthorized disclosure of information), integrity (change in data), availability (readiness of correct service at all times), reliability (continuity of correct service), and the service provider must offer capabilities that, at a minimum, include a tested encryption schema

2. SECURITY ISSUES
Cyber crime's effects are felt throughout the Internet, and cloud computing is an enticing target for many reasons. Providers such as Google, Microsoft, and Amazon have the existing infrastructure to deflect and survive cyber-attacks, but not every cloud has such capability. If a cyber-criminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cyber criminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous websites, and without proper security, hundreds of websites could be compromised through a single malicious activity. Cloud computing security includes a number of issues like multi tenancy, data loss and leakage, easy accessibility of cloud, identity management, unsafe API's, service level agreement inconsistencies, patch management, internal threats etc. [2]. It is not easy to enforce all the security measures that meet the security needs of all the users, because different users may have different security demands based upon their objective of using the cloud services.

2.1 Multi Tenancy
Cloud services work on multi-tenancy model where the same resources are shared by multiple independent cloud users. Many times this would lead to a situation where competitors co-exist on the same cloud. Such an environment opens up a whole lot of possibility of data stealth.

2.2 Data Loss and Leakage

Data can be compromised in multiple ways. Access of sensitive data to unauthorized entities can expose it. Removal or modification of data without having backup can lead to its loss. Storing data on unreliable media can make it susceptible to multiple attacks, thereby compromising its integrity

2.3 Easy Accessibility of Cloud

Cloud services can be used by one and all. A simple registration model where anybody with a valid credit card can register and become a cloud user. This opens a world of opportunity for the wily minds.

2.4 Identity Management

Cloud computing is uniting of multiple technologies coming together to satisfy the needs of diversified users through a labyrinth of services and software's. This requires Identity Management (IDM) for different technologies to inter-operate and function as a single entity in a shared landscape.

2.5 Unsafe API's

Application program interface is a set of routines and protocols describing how software components will communicate with each other. API is user manual. Every CSP publishes its API for reference of cloud users while they are deploying their data on cloud. The architectural and design specification details mentioned in the API are accessible by attackers also who can study them and then design targeted attacks.

2.6 Service Level Agreement

Service Level Agreement is the legal document signed by CSP and cloud user defining their business relationship. It enlists the services to be delivered by the CSP, their evaluation criteria, tracking and compliance of offered services and legal measures to be taken in case of unsatisfactory performance.

2.7 Patch Management

A patch is a piece of code written to fix bugs, or update/enhance an existing computer program. This includes fixing security vulnerabilities and other errors, and improving its usability and performance. Patch management is the process of planning which patches should be applied where and how.

2.8 Internal Threats

Internal security is as important as external security. A cloud user has placed his confidential data on the cloud, with little or no control over it. A malicious mind in disguise of an employee can lead to accessing of confidential data, stealing it and passing it on to user's competitors

3. RELATED WORK

Cloud computing is likely to suffer from a number of known vulnerabilities, enabling attackers to either obtain computing services for free or steal information from cloud users. In the world of computing, security and privacy issues are a major concern and cloud computing is no exception to these issues. A study ascertains that securing outsourced data and computation against mistrusted clouds is indeed costlier than the associated savings, with outsourcing mechanisms up to several orders of magnitudes costlier than their no outsourced locally run alternatives [3]. From the view of a broad class of potential users, using cloud is much like trusting the telephone company–or Gmail, or even the post office–to keep communications private. People frequently place confidential information into the hands of common carriers and other commercial enterprises. There is another class of users who would not use the telephone without taking security precautions beyond trusting the common carrier. For procuring storage from the cloud, same thing applies-never send anything but encrypted data to cloud storage [4]. Affirming this notion we provide a mechanism for achieving maximum security by leveraging the capabilities of cryptography. We provide architecture and guidelines to increase the security as well as the privacy of the data owner by transferring the process of encryption and decryption from the cloud to self. For maximizing the security of data, user segments and encrypts the data using a secured co-processor. It may be argued that such encryption on user's end raises issues as user controlled keys may be inconsistent with portions of CSP's business model. Also this architecture can limit a cloud provider's ability to data mine or otherwise exploit the users' data [5]. So, to fully exploit potential of cloud computing there should be limited restrictions on processing and computation. This is possible when CSP can enable search on encrypted data. A model for this exists where CSP's can partially access the data without having to decrypt it. Sharing, updating and querying a dataset without leaking any information to the cloud provider is possible [6].

4. PROPOSED SECURITY IMPLEMENTION ON CLOUD

4.1 Data Security Model

User's data can be made secure in the cloud using encryption. But the question arises that is user's data actually encrypted when it is stored in the cloud? For example, EMC's MozyEnterprise does encrypt user's data whereas AWS S3 does not encrypt user's data [7]. If CSP does provide encryption, what encryption algorithm is being used? What is the key length? Not all encryption algorithms are created equal. Cryptographically, many algorithms provide insufficient security; especially proprietary algorithms should not be trusted.

Most secure data encryption solutions must support all of the major business use cases: full disk encryption, database encryption, file system encryption, distributed storage encryption and even row or column encryption. CSP cannot provide such encryption granularity to each user at each level. So we need encryption solution between user applications and database servers in the cloud initiated by the user himself. We choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data. In symmetric cryptosystems, the longer the key length, the stronger the encryption. Also, although long key lengths provide more protection, they are more computationally intensive, and may strain the capabilities of computer processors. A performance evaluation reveals that going from 128 bits key to 192 bits key causes increase in power and time consumption by 8% and 256 bits key causes an increase of 16% [8]. So we propose use of industry standard high grade Advanced Encryption Standard (AES) symmetric encryption algorithm with key length of 128-bits and Diffie Hellman Algorithm for this purpose.

- The user decides to use cloud services and migrate his data on the cloud.
- User submits his service requirements with CSP's and chooses provider offering best specified services.

- When migration of data to the chosen CSP happens and in future whenever an application uploads any data on the cloud, the data is encrypted and then sent.
- The encryption process is done using AES algorithm.
- Once encrypted, data is uploaded on the cloud
- Any requests to read the data will happen after it is decrypted on the users end and then plain text data can be read by the requesting application.

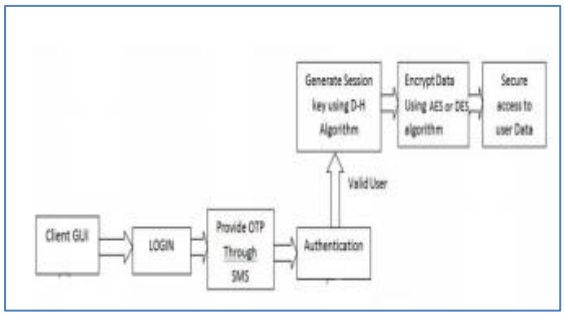

Fig2: Proposed System

The plain text data is never written anywhere on cloud. This includes all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily without any application changes at all. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption solution protects data and encryption keys and guarantees they remain under user's control, and are never exposed in storage or in transit. For authentication we use Diffie Hellman algorithm

4.2AES Algorithm for Encryption

AES[9] is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule. For encryption, each round consists of the following four steps:

- ***SubBytes*** – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

- ***ShiftRows*** – a transposition step where each row of the state is shifted cyclically a certain number of times

- ***MixColumns*** – a mixing operation which operates on the columns of the state, combining the four bytes in each column.

- ***AddRoundKey*** – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule

4.3 DIFFIE HELLMAN for Authentication

It is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange [11] method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The scheme was first published by Whitfield Diffie and Martin Hellman in 1976, although it had been separately invented a few years earlier within GCHQ, the British signals intelligence agency, by James H. Ellis, Clifford Cocks and Malcolm J. Williamson but was kept classified.[citation needed] In 2002, Hellman suggested the algorithm be called Diffie–Hellman–Merkle key exchange in recognition of Markel's contribution to the invention of public-key cryptography .Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).The method was followed shortly afterwards by

Function of Diffie Hellman Algorithm Authentication Module:

1. Make New Registration for Cloud Service :
At first the company or a user who needs the various cloud services are required to register. During registration various details of user such as there user id and mobile no. is taken . The mobile no.is later used for validating a user whether it is a genuine user or not by sending immediately a small text message which will include a key that the user will require to enter for creating a account over the cloud and then the registration will be successful. Figure shows how the authentications process occurs which depicts that when a user enters its user id and a password, a key is being send to his device which is being generated using a D-H Key Exchange and also this key is valid a specific time instance and will get destroyed after that specific time instance.

2. Using Cloud Service:
Whenever a user is required to use the services provided by the cloud service provided ,the user enters his user id and password ,if the user id and password is correct a new key is generated using the Diffie-Hellman Key Exchange Algorithm and is sent to the users mobile device using the number which was provided by the user during registration. The user then enter the key which he/she has received on his
device .If the key matches with the one generated using the Diffie-Hellman Algorithm, data access is provided to the user and all the cloud services are provided to the user after authentication is made successful.

5. ANALYSIS OF OUR PROPOSED SCHEME

Security Analysis: In this section, we analyze the security properties and the performance of our Proposed Scheme. The analysis consist of analyzing various security properties such as Data Confidentiality, Authentication and Integrity of the data.

1) Data Confidentiality: Data Confidentiality of our proposed scheme is analyzed by comparing it with various data Encryption algorithms such Advanced Encryption Standard or Data Encryption Standard which uses the symmetric key for encrypting the data. In our proposed scheme as the data is encrypted, hence the cloud service provider do not have any access to the data as he do not know

the key, and is only known to the data owner which ensures the Data Confidentiality.

2) Authentication: In our proposed scheme, whenever a new user is added or it tries to access the data over a cloud , a Two Factor Authentication is performed with the help of the password set by the user during registration and the key which is generated with the help of Diffie-Hellman algorithm which is sent to the user mobile device. If the password and the key matches or is correct then access is granted to the user over the cloud services. In this way the Authentication occurs in our proposed scheme.

3) Integrity: Integrity of data is maintained with the help of encryption module of our proposed scheme. It ensures that the data integrity is maintained and the data over the cloud is secured.

4) Computational Complexity: Fig shows the computational complexity of a public key encryption technique and the Diffie-Hellman Key Exchange. As the size of the Key increases, the computation complexity also increases in the Public key encryption technique when compared to Diffie Hellman Key Exchange.

6. RESULT

As per our analysis we show our result in graph that the our proposed algorithm is faster than AES and Diffie Hellman,. As the processing time of AES and Diffie Hellman is more than proposed algorithm, hence the transmission time, Confidentiality, Computation time, Authentication process is faster than AES and Diffie Hellman algorithms .In terms of security proposed algorithm is more secure for cloud because it has quality features of both algorithm .

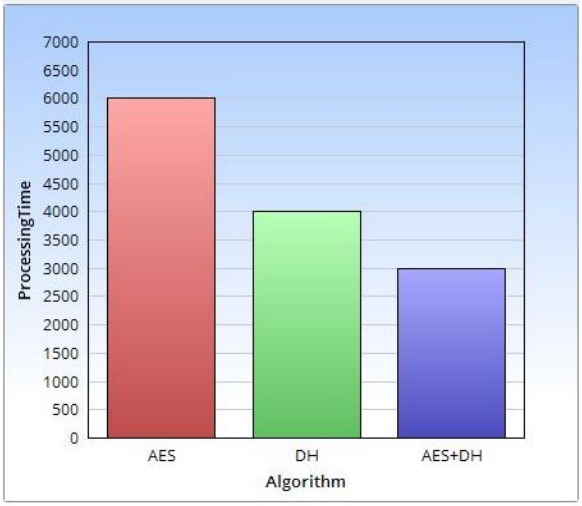

Fig3: Comparison of algorithms

7. CONCLUSION

This paper represents the security methods, which secure the data of malicious usersat the cloud is completely avoided by DiffieHellman key exchange algorithm. This paper also addresses the problems of the access control using proper authentication mechanism by two factors. D-H protocol fits better in this scenario as number of users on cloud is very large and key management is very difficult. Our proposed scheme eliminates the overheads of key computation and their management. Implementation of the AEScryptographic algorithms in a cloud computing environment also covered in this paper. Provision of security to the users data on the cloud will defiantly empowers the Data owner to outsource the data to cloud

8. REFERENCES

[1] Ellen Messmer (2012). Gartner : Growth in Cloud Computing to shape 2013 security trends, Network World [Online]. Available: http://www.networkworld.com/news/2012/120612-gartner-cloud-security-264873.html

[2] SachdevAbhaThakral, and MohitBhansali."Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.

[3] Chen, Yao, and RaduSion . "On securing untrusted clouds with cryptography. "Proceedings of the 9th annual ACM workshop on Privacy in the electronic society.ACM, 2010.

[4] Talbot, David (2009). " How Secure Is Cloud Computing?" Technology Review [Online].Available: http://www.technologyreview.com/computing/23951/

[5] Agudo , Isaac and Nuez , David and Giammatteo , Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing, Data Management, and Applications, pages 190–197, Springer Berlin Heidelberg, 2011.

[6] Op – ed : Encryption, not restriction, is the key to safe cloud computing. Available Online: http : / / www. nextgov.com/cloud-computing/2012/10/oped-encryp-tion-not-restriction-key-safe-cloudcomputing/58608/

[7] " Cloud Security and Privacy " , Tim Mather, Subra Kumaraswamy, and ShahedLatif – O'Reilly Book.

[8] Elminaam, DiaaSalama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance Evaluation of Symmetric Encryption Algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.

[9] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[10] MudiliSoujanya, Sarun Kumar "The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.,Personalized IVR system in Contact Center, Department of Computer Science Engineering International Institute of Information Technology Bhubaneswar, India.

[11] ANSI press, 1999. Specified X9.42: key management using Diffie-Hellman, this standard specifies several variations of unauthenticated Diffie-Hellman key agreement, providing shared symmetric keys