Enhancing Cloud Computing Security using AES Algorithm

Abha Sachdev
Assistant Professor
Department of Computer Science & Engineering
ASET, Amity University, Noida, India

Mohit Bhansali
Student
Department of Computer Science & Engineering
ASET, Amity University, Noida, India

ABSTRACT
With the tremendous growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services reside in massively scalable data centers and can be accessed everywhere. The growth of the cloud users has unfortunately been accompanied with a growth in malicious activity in the cloud. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published. 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 Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

General Terms
Cloud Service Provider (CSP)

Keywords
Cloud Computing, Cloud Security, Cryptography, AES

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 provide independence of accessing them from any place through a network. There are three major cloud service categories: software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS).

Cloud computing is the broader concept of infrastructure convergence. This type of data centre 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. PROPOSED 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 non-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. 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 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.

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.

4.2 Implementing AES Algorithm

AES 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.

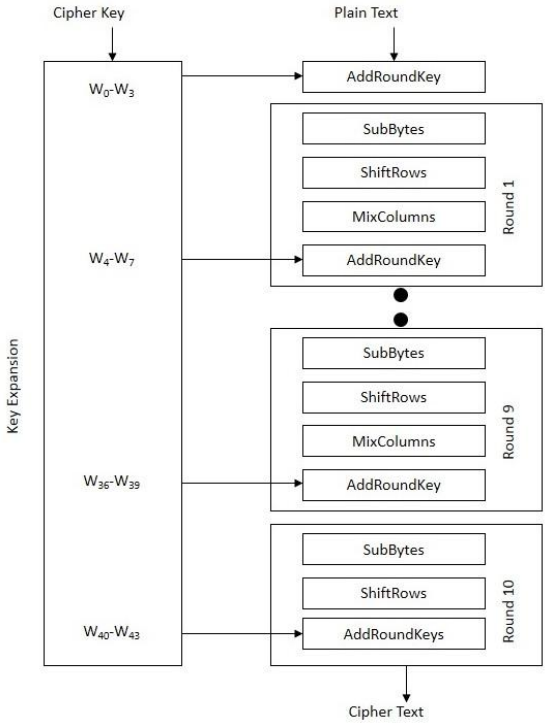

Fig 1: AES Encryption

For the final round only three steps are performed: SubBytes, ShiftRow and AddRoundKey.

4.2.1 SubBytes

The purpose of this step is to give ample resistance from differential and linear cryptanalysis attacks.

This is byte-by-byte substitution where each byte is substituted independently using Substitution table (S-box). Each input byte is divided into 24-bit patterns, representing an integer value between 0 and 15 which can then be interpreted as hexadecimal values. Left digit defines the row index and right digit defines the column index of S-box. At the intersection of row and column, value given is substituted. There are sixteen distinct byte-by-byte substitutions. S-box is constructed by a combination of GF (28) arithmetic and bit mangling.

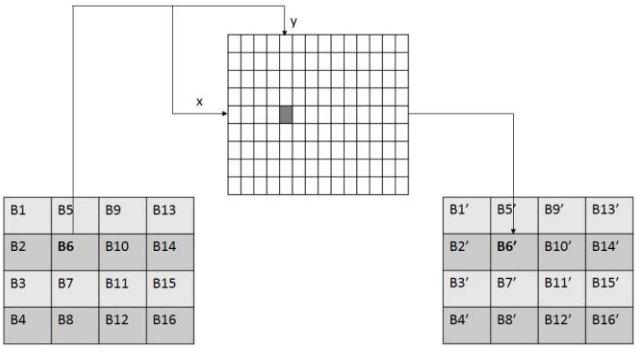

Fig 2: SubBytes Transformation Step

4.2.2 ShiftRows

The purpose of this step is to provide diffusion of the bits over multiple rounds. The row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, row 2 is circular left shifted by two bytes, and row 3 is circular left shifted by three bytes.

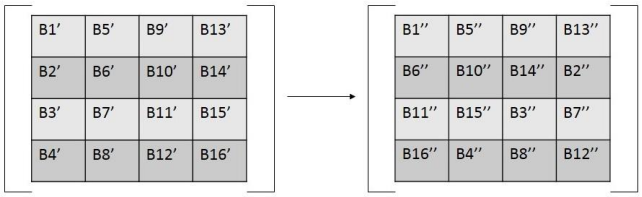

Fig. 3: ShiftRows Transformation Step

4.2.3 MixColumns

Like previous step, the purpose of this step is to provide diffusion of the bits over multiple rounds. This is achieved by performing multiplication one column at a time. Each value in the column is multiplied against every row value of a standard matrix. The results of these multiplication are XORed together. For e.g. value of first byte B1′′ is multiplied with 02, 03, 01 and 01 and XORed to produce new B1′′′ of resulting matrix. The multiplication continues against one matrix row at a time against each value of a state column.

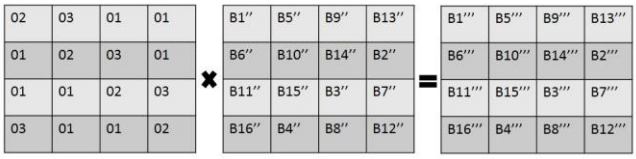

Fig. 4 MixColumns Transformation Step

4.2.4 AddRoundKey

In this step, the matrix is XORed with the round key. The original key consists of 128 bits/16 bytes which are represented as a 4x4 matrix. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3] The rest of expanded key i.e. W[4] to W[43] is generated as follows:-

```
for (i=4; i<44; i++)
        {
                T = W[i-1];
                if (i mod 4 = = 0)
                        T = Substitute (Rotate (T)) XOR RConstant [i/4];
                W[i] = W[i-4] XOR T;
        }
```

Here

Rotate means - perform a one byte left circular rotation on the 4-byte word.

Substitute means - perform a byte substitution for each byte of the word, using S-box, also used in the SubBytes step.

RConstant means – Round Constant (size of 4 bytes) which is XORed with the bytes. The rightmost three bytes of the round constant are zero.

In this way, W [4]… W [43] of the key schedule are generated from the initial four words. Although, overall, the same steps are used in decryption, as in encryption, the order in which the steps are carried out is different.

5. Why AES?

- AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.
- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- This algorithm has speedy key setup time and good key agility.
- It requires less memory for implementation, making it suitable for restricted-space environments.
- The structure has good potential for benefiting from instruction-level parallelism.
- There are no serious weak keys in AES.
- It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
- Statistical analysis of the cipher text has not been possible even after using huge number of test cases.
- No differential and linear cryptanalysis attacks have been yet proved on AES.

6. COMPARING AES WITH OTHER ALGORITHMS

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES. A performance comparison amongst AES, DES and Triple DES for different microcontrollers shows that AES has a computer cost of the same order as required for Triple DES [9]. Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of time consumption [8].

7. CONCLUSIONS

Worldwide spending on cloud services is set to take off. According to a report, "Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast" released by IDC, cloud services will see as much as 41% growth from 2013 to 2016. Spending on IT cloud services worldwide will edge toward $100 billion by 2016 [10, 11]. And in all this cloud growth, security will play a key role. Users will be ready to avail cloud services, and cloud providers have to justify security issues and satisfy users. Each of the cloud providers has their own set of rules, pricing, flexibility, support and other important parameters. The key consideration dealt in this proposal is the encryption schema to secure data by making it unintelligible for all. Implementing AES for security over data provides benefits of less memory consumption and less computation time as compared to other algorithms. Though each cloud infrastructure has its own security strengths; the user can choose infrastructure according to his security

requirements. AES provides security to cloud users as encrypted data in the cloud is safe from many attacks.

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] Sachdev Abha Thakral, and Mohit Bhansali. "Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.

[3] Chen, Yao, and Radu Sion. "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/op-ed-encryption-not-restriction-key-safe-cloud-computing/58608/

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

[8] Elminaam, Diaa Salama 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] Sanchez-Avila, C., and R. Sanchez-Reillol. "The Rijndael block cipher (AES proposal): a comparison with DES." Security Technology, 2001 IEEE 35th International Carnahan Conference on. IEEE, 2001.

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

[11] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit.com/news/technology/1112692915/cloud-computing-growth-paas-saas-091212/

[12] Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=236552

[13] John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―, 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[14] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.