Security Algorithms for Cloud Computing Environment

Akashdeep Bhardwaj, Dr. GVB Subrahmanyam, Dr. Vinay Avasthi, Dr. Hanumat Sastry

1 Fiserv Global Services
Noida, Uttar Pradesh, India
Bhrdwh@yahoo.com

2 Tech Mahindra
Hyderabad, Andhra Pradesh India
Subrahmanyam.gvb@techmahindra.com

3 University of Petroleum and Energy Studies, Computer Science
Dehradun, Uttarakhand, India
VAVASTHI@DDN.UES.AC.IN

4 University of Petroleum and Energy Studies, Computer Science
Dehradun, Uttarakhand, India
HSASTRY@DDN.UES.AC.IN

Abstract
With growing awareness and concerns regards to Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms into data systems and processes. This paper presents a brief overview and comparison of Cryptographic algorithms, with an emphasis on Symmetric algorithms which should be used for Cloud based applications and services that require data and link encryption. In this paper we review Symmetric and Asymmetric algorithms with emphasis on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption.

Keywords: Cryptography, Security Algorithm, Symmetric, Asymmetric, RSA, RC6, AES, 3DES, MD5

1. Introduction

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of an eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents.

In simple terms, Cryptography can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text and then performing decryption which is reverting back to the original plain text.

With this ability, Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
- Authentication for determining whether someone or something is, in fact, who or what it is declared to be.
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
- Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

Figure 1: Encryption and Decryption process

In pure science terms, Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and converting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text.

This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key}

Defining some terms used in Cryptography:
- Plaintext is the original intelligible source information or data that is input to algorithms
- Cipher text is the scrambled message output as random stream of unintelligible data
• Encryption Algorithm substitutes and performs permutations on plain text to cipher text
• Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text
• Keys are used as input for encryption or decryption and determines the transformation
• Sender and Recipients are persons who are communication and sharing the plaintext

With respect to Cloud computing, the security concerns are end user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud:

• Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
• Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
• Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
• Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
• User Access Control: for Web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

Security Algorithms are classified broadly as:

• Private Key / Symmetric Algorithms:
  Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.

• Public Key / Asymmetric Algorithms:
  Use a key pair for cryptographic process, with public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public key algorithms.

• Signature Algorithms:
  Used to sign and authenticate use data are single key based. Examples include: RSA and DH

• Hash Algorithms:
  Compress data for signing to standard fixed size. Examples include: MD5, SHA

• Some other ways of classifying Algorithms based on their processing features as below

  Figure 2: Classification of Algorithms

With several Cloud services, Servers and hosted applications under IT management, most Cloud providers have no defined process to ensure security of data from threats and attacks. Cyberattack these target the end user data for which the Cloud Service providers seek to try and secure by using Cryptographic algorithms whose primary goal is to make it as difficult as possible to ensure decrypting the generated cipher text from the plain text. When the key length is long, that makes it harder to decrypt the cipher texts, which in turn make the algorithms efficient and effective.

2. Asymmetric Algorithms

Asymmetric Algorithms a pair of related key, one key for encryption called the Public key and a different but inter related key for Decryption called the Private keys when performing transformation of plain text into cipher text. The main asymmetric algorithms are ECC, Diffie-Hellman and RSA.

  Figure 3: Asymmetric Algorithm process

RSA and Diffie Hellman are checked as the most widely used Block Cipher Algorithms.

RSA:

• RSA Algorithm named after its inventors (Rivest, Shamir, and Adelman) is best suited for data traveling to/from Web and Cloud based environments. In working with Cloud Computing, the end user data is first encrypted and then stored on the Cloud.
• When the data is required, the end user simply needs to place a request to the Cloud Service provider for accessing the data. For this the Cloud service provider first authenticates the user to be the authentic owner and then delivers the data to the requester using RSA Asymmetric Algorithm. This algorithm has support from .NET Security Framework as well.
  
  When the data is required, the end user simply needs to place a request to the Cloud Service provider for accessing the data. For this the Cloud service provider first authenticates the user to be the authentic owner and then delivers the data to the requester using RSA Asymmetric Algorithm. This algorithm has support from .NET Security Framework as well.

• Here two keys involved – first the Public Key which known to all and the other Private Key which is known only to the end user. Data conversion from plain text to cipher text is done using Public Key by the Cloud service provider and the cipher text to plain text decryption is done by the end user using Private Key as the Cloud service consumer. Once the user data is encrypted with the Public Key, that cipher data
can only be decrypted with the corresponding Private Key only. In this Algorithm, prime numbers are used to generate the public and private keys based on mathematical formulas and by multiplying the numbers together.

- This uses the block size data in which plain text or the cipher texts are integers between 0 and 1 for some n values. Here the processed plaintext is also encrypted in blocks and the binary value of each block needs to be less than the number (n). RSA being multiplicative homomorphic which essentially means that to find the product of the plain text, multiply the cipher texts so that the outcome of the result is the cipher text of the product.

3. Symmetric Algorithms

Symmetric algorithms involve a single shared secret key to encrypt as well as decrypt data and are capable of processing large amount of data and from computing standpoint are not very power intensive, so has lower overhead on the systems and have high speed for performing encryption and decryption. Symmetric algorithms encrypt plaintexts as Stream ciphers bit by bit at a time or as Block ciphers on fixed number of 64-bit units.
4. Related Work

With DDoS and Malware attacks on the rise, Cloud Providers are giving more focus on having end user data as secure as possible and having low priority for cloud performance due to inconsistent selection of algorithms for encryption and encoding. By selecting the right cryptographic scheme end user data security can be achieved without losing out on cloud performance.

Since Algorithm analysis is an essential in gathering the knowledge against any accidental or unintentional use algorithm that may prove to be inefficient or significantly impact application system performance due to encryption or decryption. For those cloud based web applications or portals needing real time or time sensitive data, an algorithm that might be taking a long time to long to run would prove a hindrance for the real time application as it may render the results to be useless. Such in efficient algorithm might end up needing lots of computing power or storage to execute over the cloud, making the algorithm useless in that environment.

Authors compared Symmetric encryption algorithms and encoding algorithms using size and time to decide on selection of the right algorithms based on the parameters as

- File Size: indicates file of different size to be taken
- Encryption Computation Time: time an algorithm takes to produces a cipher text from a plain text
- Encoding Computation Time: time taken by encoding algorithm to produce a hash code

The authors then used the below infrastructure for our data gathering research work:

- Connectivity: 1Mbps WAN circuit link connected to a public Cloud server provider
- Cloud Simulation: Hosted Web application server on the IaaS systems for cloud environment
- Working environment:
  - Used Java as the programming language environment
  - Setup one 64 bit Windows Server 2008 Operating system
  - Running on VMware based a Virtual machine
  - Over hardware as Intel Core i5-3230M CPU @ 2.66GHz, 8GB memory.

Performance metrics were collected based on the following:

- Encryption & Decryption Time: This is calculated as the time required for encryption which involves converting the plain text payload file into cipher text. The authors used the encryption time to find the throughput which indicated the computation cost i.e. the encryption speed. The decryption time is calculated for the amount of time required for converting the cipher text back into the plain text.
- CPU Processing Time: This is determined as the time CPU is committed for the process and reflects the CPU load during the encryption process. The CPU

Clock Cycle and Battery power are the energy consumed during encryption and decryption process.
- Size of payload to be tested: This is actual size of the test file that is being used for the experimental work.

The below mentioned actions were performed as input using different algorithms to encrypt the data (text file) to determine the time required for reading the file, encrypting it, creating the encrypted data, then sending the data to a cloud location and receiving a confirmation. The input variables are

- File upload: D:\SACC\Data\Encrypt.txt (input)
- Choosing algorithm:
- Encoding Hash
- Key size:
- Mode: Encrypt or Decrypt

![Figure 7: Encrypting text file to send to the cloud](image)

5. Results Obtained

The data from experimental work on Symmetric algorithms is depicted below by using varied file sizes as input and recording the computation cost for those algorithms. Encoding algorithms checks for data integrity for end user data on the cloud and computation cost data obtained for different algorithms by varying the size of payload.

![Figure 8: Computational Cost for Encryption](image)

![Figure 9: Computational Cost for Decryption](image)
6. Conclusions

With Cloud computing emerging as a new in thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. This makes Cloud security a must to break the acceptance hindrance of the cloud environment. Use of security algorithms and ensuring these are implemented for cloud and needs to be properly utilized in order to ensure end user security.

The authors analyzed Symmetric algorithms for different encryption and encoding techniques, found AES to be a good candidate for key encryption and MD5 being faster when encoding.

References

[1] Leena Khanna, Anant Jaiswal, “Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them”, IJARCSE 2013
[2] G Devi, Pramod Kumar “Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm” IJCTT 2012
[3] Simarjeet Kaur “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of CS and IT, 2012
[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi “A quantitative analysis of current security concerns and solutions for cloud computing”, Springer 2012.
[5] Ronald Krutz, Russell Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing” Wiley Publishing 2010
[6] Behrouz Forouzan, “Cryptography and Network Security”, McGraw-Hill Special Indian Edition 2007
[7] Wayne Jansen, Timothy Grance “Guidelines on Security and Privacy in Public Cloud Computing”, National Institute of Standards and Technology 2011
[8] Akhil Behl “Emerging Security Challenges in Cloud Computing”, IEEE 2011
[9] Maha Tebba, Said Haji Abdellatif Ghazi, “Homomorphic Encryption Applied to the Cloud Computing Security”, World Congress on Engineering 2012
[10] Cloud Security Alliance (CSA), “Security Guidance for critical Areas of Focus in cloud computing V3.0” CSA 2015
[11] Ayan Mahalanobis, “Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups.” 2005
[12] Neha Jain, Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security”, VSRD International Journal of CS and IT, 2012
[13] Mandeep Kaur, Manish Mahajan, “Implementing Various Encryption Algorithms to Enhance The Data Security Of Cloud In Cloud Computing” VSRD International Journal of Computer Science & Information Technology 2012
[14] Jeeva, Dr. Palanisamy, Kanagaram, “Comparative Analysis of Performance Efficiency and Security Measures of some Encryption Algorithms”, IJERA ISSN: 2248-9622 Vol. 2, Issue 3, 2012
[15] Dr. Sarbari Gupta,”Securely management cryptographic keys used within acloud environment”, NIST Cryptographic Key management workshop, 2012
[16] Dr. R. Chandramouli “Key Management Issues in the Cloud Infrastructure”, Workshop on Cloud Computing, 2013
[17] Sandro Rafaeli, “Survey of key management for secure communication”, ACM Computing Surveys, 2013
[18] S. Anahita Mortazavi, Alineza Nemaney Pour, Toshihiko Kato,"An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSHA", CNDS Feb 2011
[19] ENISA,”Algorithms, Key Sizes and Parameters Report,2013”, recommendations version 1.0 – October 2013
[20] Y. Fan, L. Xiao-ping, D. Qing-kuan and L. Yan-ming, “A Dynamic Layering Scheme of Multicast Key Management,” IEEE 5th International Conference on Information Assurance and Security, Xian 2009
Akashdeep Bhardwaj, PhD research scholar from UPES, PGDM, B.E (Computer Science) is an Enterprise Risk and Resilience Technology Manager working on Information Security and Infrastructure Operations domain having worked for over 20 year with various US based MNCs and trained and certified in Internal Information Security, Ethical Hacking, Microsoft, Cisco and VMware technologies.

Dr. GVB Subrahmanyam, PhD is an enterprise Architect and focuses on Development, Delivery and Sustenance of IT Applications in Supply Chain/Insurance/Banking/Finance. He is a TOGAF certified Enterprise Architect and IBM certified Rational Software Architect.

Dr. Hanumat G Sastry, received his M.Tech (CSE) from Acharya Nagarjuna University and PhD in Computer Science from Dravidian University. He has 11 research papers in referred international journals. He has 8+ years of teaching experience at University level. His active research interests include Optimization algorithms, Data mining, Evolutionary Computing and Semantic Web.

Dr. Vinay Avasthi, received PhD in Computer Science from University of Petroleum & Energy Studies. He has published many Papers at both National and International levels. He has rich experience in Academic & Research includes Data mining, Networking algorithm, distributed computing, cloud computing and IOT. He is the member of ACM, CSI and ISTE. He is also the recipient of CSI Significant Contribution Award 2012-13.

[21] Rajesh Ingle, G. Sivakumar, "EGSI: TGKA based Security Architecture for Group Communication in Grid", 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, pp. 34-42, 17-20 May, 2010.

[22] NIST, “Cloud Computing Synopsis and Recommendations”, Special publication 800-146, May 2012