Efficiency of Modern Encryption Algorithms in Cloud Computing

Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem

1Ma’arif University College, Computer Science Department, Anabr, Iraq
2, 3, 4 Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

Abstract: Cloud computing bears everything as a service over the web supports user demand. The benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. So each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. There is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments and storage “databases hosted by the Cloud provider”. This paper discussed the various encryption algorithms (symmetric, asymmetric) and issues involved in using cloud services such as the performance of encryption algorithms on a cloud environment for different input block data size, how the change in the size of the files after encryption is complete.

Keywords: Cloud computing, encryption/decryption process, cloud security.

1. INTRODUCTION

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It bears everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider [1], [2], and [3].

The concept of cloud computing is associated closely with Infrastructure as a Services (IaaS), Platform as a Services (PaaS), Software as a Services (SaaS) all of which means a service oriented architecture [7]. These provides the first benefit of the cloud computing (i.e.) it reduce cost of hardware that cloud have been used at end user. As there is no need to store data at end user’s because it is already at some other location. So instead of buying the whole infrastructure required to run the process and save bulk of data you are just renting the assets according to your requirement. The similar idea is behind all cloud networks [2], [5].

Generally, several cloud data storage concerns can arise. Typically, users will know neither the exact location of their data nor other sources of the data collectively stored with theirs.

To secure the Cloud means secure the treatments and storage “databases hosted by the Cloud provider”. Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA). Confidentiality of data in the cloud is accomplished by encryption/Decryption process [8], [9], and [10].

Encryption/Decryption process, in modern days is considered combination of three types of algorithms. They are (i) Symmetric-key algorithms cryptography such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron’s Code (RCn), and Triple DES, (ii) Asymmetric-key algorithms such as Rivest, Shamir, & Adleman (RSA), Elliptic Curve(EC), Diffi-Hillman(DH), and (iii) Hashing. Integrity of data is ensured by hashing algorithms.

To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm’s performance is slower when compared to symmetric-key algorithms [11], [12].

Both approaches have a major problem related to encryption key management (i.e.) how to securely generate, store, access and exchange secret key. The most common classification of encryption algorithms can be shown in Figure 1.

Figure 1: Classification of Encryption Algorithms

This paper examines a method for evaluating performance of selected encryption algorithms with different mechanisms (symmetric or asymmetric, classical or modern), this evaluation is done cloud networking environment. Usually, encryption algorithms consume a significant amount of computing resources such as CPU time, memory, etc. This study evaluates seven different encryption algorithms namely: AES, DES, 3DES, RC4, Blowfish, RSA, and DH, the performance measure of...
encryption schemes will be conducted in terms of data types (text or documents), size of the input data and changing the key size for the selected cryptographic algorithm.

TABLE 1. Shows the comparison between Asymmetric Algorithms such as RSA, and Symmetric Algorithms such as DES, 3DES and AES [18].

<table>
<thead>
<tr>
<th>Factors</th>
<th>RSA</th>
<th>DES</th>
<th>3DES</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contributor</td>
<td>Rivest, Shamir’78</td>
<td>IBM 75</td>
<td>IBM 78</td>
<td>Rijman, Joan</td>
</tr>
<tr>
<td>Key Length</td>
<td>Based on No. of bit in N=p×q</td>
<td>56- bits</td>
<td>168, 112 bits</td>
<td>128, 192, and 256</td>
</tr>
<tr>
<td>Rounds</td>
<td>1</td>
<td>16</td>
<td>48</td>
<td>10 or 12 or 14</td>
</tr>
<tr>
<td>Block size</td>
<td>Variance</td>
<td>64-bits</td>
<td>64 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Security rate</td>
<td>Good</td>
<td>Not enough</td>
<td>Adequate</td>
<td>Excellent</td>
</tr>
<tr>
<td>Execution time</td>
<td>Slowest</td>
<td>Slow</td>
<td>Very slow</td>
<td>More fast</td>
</tr>
</tbody>
</table>

The rest of the paper is organized as follows: Section 2 surveys the related works for encryption algorithms in cloud computing, cloud environment setup and analysis results are given in section 3. In section 4 explains the inferences obtained from the results. Section 5 presents the conclusion and future works.

2. Related Works

Encryption phase is a well-known technology for protecting sensitive data during transmission process in cloud environment. Recently, many researches have focused on the encryption phase using many techniques in order to perfectly hide the sensitive transmitted data and files [4], [5], and [6].

A. Padmapriya et al. [7], [8], and [9] propose a new level of data security using ASCII code to develop an encryption system in cloud based Reverse Caesar Cipher. Their main target was to solve the security issue in both cloud providers and cloud consumers. This contribution considered as the first proposed model in cloud security that depends on text file format for the transmitted data. However, the usage of the classical Caesar Cipher algorithm, suffers from the brute-force and authentication attacks that can easily hack the transmitted data.

In [3], [5], [13], and [17] authors described data security system in cloud computing based DES algorithm to secure client and server. The security architecture of the system is design by using DES-Cipher Block Chaining (CBC), which eliminates the concerns that occurs today with data stolen. Unfortunately, DES algorithm hacked by many attackers such as man-in-the-middle attack and side channel attack, in which the key expansion phase is exploited in the DES structure.

3. Cloud Environment

Many encryption algorithms have been developed and implemented in order to provide more secured data transmission process in cloud computing environment, such as, DES, AES, RC4, Blowfish, and 3DES for symmetric category and RSA, DH for asymmetric category. The study implemented the mentioned symmetric and asymmetric algorithms in order to ensure the data security in cloud environment, and examine the performance of such algorithms, considering the time of the encryption/ decryption process and the size of the output encrypted files.

The experimental environment consists of the cloud network, the cloud network entails the Xen (5.6 XCP) server and the client that uses Citrix [18] as V-mware system with N-Para-virtual machine. The cloud server utilizes the Core i5 (4.8GHZ) with 8GB of RAM with 500GB-HDD as the main hardware, however the client machine makes use of Core i3 (2.4GHZ) with 2GB of RAM with 300–HDD.

The cloud simulator environment is simulated based the Xen Server 5.6 platform (XCP) and Citrix Xen System for the client machine with Para-virtualization enabler.

Figure2. Screenshot of encryption algorithms simulation.
The encryption algorithms are different in many fields such as block input size, key size, and speed-up of the encryption transformation.

4. Experimental Results

This subsection will distinguish between the two different types of encryption categories by implementing symmetric and asymmetric algorithms on the cloud network.

In the following analysis both the symmetric and asymmetric techniques have been implemented using several input file sizes: 500kb, 1000kb, 1500kb, 2000kb, 2500kb, and 3500kb.

Figure (3) represents the running time of the implemented symmetric techniques using the cloud network, the running time is calculated in seconds and the Input size is taken in kilobytes.

![Figure 3: Running time for symmetric algorithm on XCP](image)

Based on the above analysis figures, the following can be concluded:

i. The running time of the data transformation on the cloud network is faster.

ii. There is an inverse proportion relation between the running time and the size of the input file. Such that, the increase of the input file size led to the decrease of the running time.

The AES is the fastest symmetric technique since it enjoys the scalability based on different hardware, as well as it can be implemented simply. After then, the symmetric techniques can be ordered as DES, 3-DES, RC4, and finally the Blowfish.

![Figure 4: Running time for asymmetric algorithm on and XCP](image)

5. Conclusion and Future Works

Cloud computing allows consumers to use applications without installation and access their personal files at any computer with internet access. In cloud computing technology there are a set of important policy issue, which includes issue of privacy, security, anonymity, telecommunications capacity, and reliability among others. But the most important between them is security and how cloud provider assures it.

In this paper analyses the importance of security to cloud. We compared seven algorithms, five algorithms for symmetric algorithm and two for asymmetric algorithm for data security in cloud. Moreover, we concluded that the algorithms implemented are more efficient on cloud environment.

In future plane, we have many more algorithms to be evaluated and their results can be analyzed with one another to produce the best implemented security algorithm in cloud environment for future use.

References


Authors Biography

Omer K. Jasim: He received his M.Sc. (2009) in Computer Science from Al-Anbar University, Iraq, and get B.Sc. (2007) in Information System from Al-Anbar University, Iraq. He got the first ranking in two above studies. His work experience includes 3 years as an academic in Iraq (Alma‘arif University College). He Worked as Head of computer science department, Alma‘arif University College (2010-2012). Now he a Ph.D. student in Ain Shams University, Omer is current areas of research are cloud computing, quantum cryptography, cryptography and network security, and artificial intelligent. Until now he published four papers in English language and one in Arabic language.

Dr. Safia Abbas: She received his Ph.D. (2010) in Computer science from Tokyo University, Japan, her M.Sc. (2003) and B.Sc.(1998) in computer science from Ain Shams University, Egypt. Her research interests include data mining argumentation, intelligent computing, and artificial intelligent. He has published around 15 papers in refereed journals and conference proceedings in these areas which DBLP and springer indexing. Moreover, she has been involved in more than 10 conferences as an International Program Committee member. She holds the first place in the international publication from the Ain Shams University president.

Professor El-Sayed M. El-Horbaty: He received his Ph.D. (1985) in Computer science from London University, U.K., his M.Sc. (1978) and B.Sc.(1974) in Mathematics from Ain Shams University, Egypt. His work experience includes 25 years as an academic in Egypt (Ain Shams University), Qatar (Qatar University), and Emirates (Emirates University, Ajman University, and ADU University). He Worked as Deputy Dean of the faculty of IT, Ajman University (2002-2008). He is working as a Vice Dean of the faculty of Computer & Information Sciences, Ain Shams University (2010-Now). Prof. El-Horbaty is current areas of research are parallel algorithms, combinatorial optimization, image processing. His work appeared in journals such as Parallel Computing, International Journal of Computers and Applications (IJCA), Applied Mathematics and Computation, and International Review on Computers and Software. Also he has been involved in more than 26 conferences.

Prof. Dr. Abdel-Badeeh M Salem: he is a Professor of Computer Science in the Faculty of Computer and Information Sciences, Ain
Shams University, Cairo, Egypt. He has been Professor Emeritus since 2007. Previously he was Director of the Scientific Computing Center at Ain Shams University (1984-1990). His research interests include intelligent computing, expert systems, biomedical informatics, and intelligent e-learning technologies. He has published around 250 papers in refereed journals and conference proceedings in these areas. He has been involved in more than 300 conferences and workshops as an International Program Committee member, organizer and Session Chair. He is author and co-author of 15 Books in English and Arabic Languages. His work appeared in more than 100 journals.