Improvisation of RSA Algorithm in Respect to Time and Security with the Proposed (AEA) Algorithm

A Taneja1 R K Shukla2 and R S Shukla3

1, 2 Department of Computer Science and Engineering, Invertis University.
3 Department of Computer Science, College of Computing and Informatics Saudi Electronic University, KSA
amit.t@invertis.org

Abstract The security of digital information has become increasingly vital in the digital world, which is currently evolving and changing at such a quick speed. With the rapid growth of hidden contact and communication around the world, the need for communication security is becoming increasingly important. The main motive of cloud service providers is to collect the information and details of the material uploaded on their cloud servers. One of the major concern is security of the contents uploaded on the cloud servers. Although, they challenge about the security provided by them to the individuals but they are the owner of servers and the information on it. The same has been observed when one of our server crashed and we consulted about the incident with the customer care department of our CSP. We use to back up our university servers backup on cloud for which we pay some amount as decided by our management as well as CSP. The aim of this research is that the cloud owners cannot have access to data of the users. I proposed a new robust encryption technique in this paper to improve the security of the key generating algorithm. To achieve this, an algorithm has been implemented which performs much better than renowned algorithm i.e. RSA algorithm. This algorithm achieves better response time than RSA algorithm which is described and proved in this paper. This paper uses ASCII and EBCDIC codes while encryption and decryption.

Keywords: Algorithm, Cloud, CSP, RSA, Server, ASCII, EBCDIC

1. Introduction

The access to secured system is controlled by some authentication system which points out that the user who is trying to authenticate him is a legitimate user or an imposer. This is established by the system in two ways – (i) Does user know something which is supposed to be known only by the genuine user? And (ii) Does the user own some unique characteristics of the legitimate user. In first case it is possible that an imposter can know that something which is required to enter in a secured system. We are therefore interested in second case. The characteristics of a person which can be used to authenticate a legitimate user are biometric characteristics. In 1995, the basic concept of ransomware was introduced as a crypto virus. Nevertheless, since then, it has been considered for more than a decade merely a philosophic topic. Throughout 2017, Ransomware came to life, with many popular ransomware incidents targeting critical computer systems around the world. Biometric characteristics are further classifies as physiological and behavioural characteristics. Physiological characteristics are those which are biologically owned by the user (face, finger prints, iris pattern etc.) and behavioural characteristics are those which includes user’s habits (handwriting, keystroke dynamics, mouse interaction, gait etc.).
The problems with the password based systems are that (i) User need to remember the password (ii) Shoulder surfing is possible (ii) Password can be guessed or (iii) Password can be stolen. To overcome these problems, behavioural biometric based authentication systems are very good option however some complexities are associated with behavioural biometric based authentication systems – It is difficult to capture descriptors for the construction of user patterns.

For security purpose, some modifications were made in RSA algorithm and compared the results with RSA through which an optimized RSA algorithm was generated. The description of the comparative study was analysed. This approach was preferred and continued the research work taking into consideration of removing the limitations of RSA.

Later on after searching for other approaches, the limitations of optimized RSA algorithm were also observed which are specified as follows:
1) Complexity involved in computation was less than RSA but computation power required for encryption and decryption was high.
2) The time of CPU was less than RSA but CPU process synchronization and time was somewhat similar to RSA.
3) The time consumption was also dependent on the file size.

This paper emphasis on a new approach to encrypt and decrypt any file that should overcome the above limitations.

2. Proposed architecture and its description

This proposed architecture will resolve the security issue in cloud by applying cryptography techniques. The security in cloud can be provided in three cases:

**Case 1.** Uploading file to cloud server.
- The user will sign in with his email id and password.
- The user will upload the file which will be encrypted by user’s private key and server’s predefined key.
- The encrypted file will be stored to the cloud server.

![Figure 1. Upload file using encryption to cloud server](image)

**Case 2.** Downloading file from cloud server.
- The user will sign in with his email id and password.
- The user will request to access the file which will be decompressed.
The file will be decrypted by server’s predefined key and user’s private key.

Case 3. Request to access other user’s file from cloud.

- The user will sign in with his email id and password.
- The user will request to access the file which will be forwarded to the owner of the file.
- The access will be granted or denied as per the response from the owner of the file.
- The file will be available only for an hour and afterwards request is to be reapproved.

2.1 Algorithm Description

1. Register a User and username must be of at least 10 characters.
2. Select 5 alternate character from username.
3. Store that characters as a private key for the user.
4. Convert all odd index of private key into EBCDIC 8-bit.
5. Convert all even index into ASCII 8-bit.
6. Merge both EBCDIC & ASCII code and form 40-bit encryption key.

Encryption Technique: -

1. First read the file and store into string.
2. Convert each character of string into ASCII 8-bit.
3. Read encryption key and append first and next bit of key on 8-bit code of characters.
4. Continue step 3 until the end of file.
5. Merge all bits of characters into a single string.
6. And Complement each bit of that string.
7. Finally, we get encrypted text.
8. The encrypted file will be stored on the cloud server.
9. If same user wants to decrypt that file then use decryption technique so that the file appears in Decryption area.
10. If any third user want to access the file then that user has to request for that file to the file owner.
11. If request of third user is approved then file can be downloaded. 
12. Else third user doesn’t have right to access that file.

NOTE: - The approval request is valid up to 60 minutes only. Afterwards the request must be sent again for approval.

**Decryption Technique:**

1. Read the encrypted file and store into a string.
2. Complement each bits of string.
3. Read 10 characters of string and removes its first and last bit.
4. Convert remaining 8 characters into integer.
5. And then convert that integer into ASCII characters.
6. Continue step 3, 4 & 5 until we get end of string.
7. Merge all characters and store into a file and that file is decrypted file.

**3. Implementation**

The above approach is implemented using .NET platform and SQL server as backend. The approach includes six different types of files such as portable document format, PowerPoint, word, text, excel and image file. The input output screens are attached as follows:

**3.1 Encryption data set and pictorial representation**

The data of different types of files along with their size has been tested. The encryption time for each type of file is depicted in a table which differentiates between the two approaches.

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 797            | 667            | 100      |
| 832            | 672            | 125      |
| 322            | 309            | 150      |
| 456            | 315            | 175      |
| 963            | 755            | 200      |
| 1035           | 998            | 225      |
| 1537           | 1095           | 250      |
| 1286           | 1107           | 275      |
| 202            | 111            | 300      |
| 393            | 158            | 325      |

*Table 1 Data set of PDF file*
The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:

![Comparative Analysis of Encryption Delay for PDF file](image)

Table 2 Data set of PowerPoint file

| File Size (in Kb) | RSA Encryption | AEA Encryption | Size(KB) |
|------------------|----------------|----------------|----------|
| 100              | 206            | 174            | 100      |
| 200              | 215            | 193            | 400      |
| 300              | 247            | 240            | 800      |
| 400              | 480            | 437            | 600      |
| 500              | 504            | 409            | 700      |
| 600              | 198            | 175            | 900      |
| 700              | 282            | 192            |          |
| 800              | 461            | 431            |          |
| 900              | 568            | 448            |          |

The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:

![Comparative Analysis of Encryption Delay for PowerPoint file](image)
The data set of WORD file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 419            | 402            | 100      |
| 457            | 444            | 120      |
| 1222           | 1007           | 140      |
| 393            | 312            | 160      |
| 335            | 331            | 180      |
| 774            | 688            | 200      |
| 803            | 786            | 220      |
| 654            | 598            | 240      |
| 372            | 353            | 260      |
| 1409           | 1006           | 280      |
| 653            | 511            | 300      |

Table 3 Data set of Word file

The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:

![Figure 6 Comparative analysis of Encryption delay for Word file](image)

The data set of Text file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 1043           | 32             | 5        |
| 87             | 50             | 10       |
| 383            | 50             | 15       |
| 186            | 72             | 20       |
| 666            | 240            | 25       |
| 257            | 131            | 30       |

Table 4 Data set of Text file
The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:

![Comparative Analysis of Encryption Delay between RSA and Proposed Technique](image)

**Figure 7 Comparative analysis of Encryption delay for Text file**

The data set of EXCEL file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|-----------------|----------------|----------|
| 816             | 178            | 10       |
| 899             | 257            | 20       |
| 395             | 166            | 30       |
| 1057            | 761            | 40       |
| 757             | 545            | 50       |
| 635             | 560            | 60       |
| 177             | 52             | 70       |
| 1416            | 568            | 80       |
| 564             | 532            | 90       |
| 1028            | 735            | 100      |

**Table 5 Data set of Excel file**

The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:
The data set of IMAGE file is as follows:

| File Size (in Kb) | RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|------------------|----------------|----------------|----------|
| 20               | 813            | 651            |          |
| 30               | 539            | 454            |          |
| 40               | 586            | 456            |          |
| 50               | 166            | 151            |          |
| 60               | 266            | 168            |          |
| 70               | 599            | 486            |          |
| 80               | 390            | 364            |          |
| 90               | 859            | 815            |          |
| 100              | 530            | 467            |          |
| 110              | 484            | 408            |          |

Table 6 Data set of Image file

The following graph shows the comparative analysis of Encryption delay between RSA algorithm and proposed algorithm:

**Figure 8 Comparative analysis of Encryption delay for Excel file**

**Figure 9 Comparative analysis of Encryption delay for Image file**

3.2 Decryption data set & pictorial representation

The data set of PDF file is as follows:

The data set of PDF file is as follows:
Table 7 Data set of PDF file

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 455            | 421            | 100      |
| 723            | 703            | 125      |
| 981            | 951            | 150      |
| 1299           | 1153           | 175      |
| 377            | 370            | 200      |
| 823            | 783            | 225      |
| 434            | 423            | 250      |
| 911            | 863            | 275      |
| 1329           | 1311           | 300      |
| 1632           | 1599           | 325      |

Table 8 Data set of Power point file

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 519            | 471            | 100      |
| 599            | 566            | 200      |
| 943            | 980            | 300      |
| 345            | 340            | 400      |
| 821            | 782            | 500      |
| 211            | 199            | 600      |
| 165            | 110            | 700      |
| 498            | 425            | 800      |
| 1123           | 1009           | 900      |

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:

Figure 10 Comparative analysis of Decryption delay for PDF file

The data set of PPT file is as follows:

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:
Figure 11 Comparative analysis of Decryption delay for Powerpoint file

The data set of WORD file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 359            | 304            | 100      |
| 556            | 521            | 120      |
| 995            | 941            | 140      |
| 256            | 211            | 160      |
| 567            | 539            | 180      |
| 321            | 311            | 200      |
| 664            | 611            | 220      |
| 341            | 336            | 240      |
| 954            | 871            | 260      |
| 1024           | 999            | 280      |
| 561            | 544            | 300      |

Table 9 Data set of word file

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:

Figure 12 Comparative analysis of Decryption delay for Word file

The data set of TEXT file is as follows:

| RSA | AEA | SIZE(KB) |
|-----|-----|----------|
|     |     |          |
The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:

![Comparative analysis of Decryption delay for Text file](image)

**Table 10 Data set of Text file**

| ENCRYPTION | ENCRYPTION |
|-------------|-------------|
| 45          | 32          |
| 533         | 521         |
| 345         | 301         |
| 122         | 115         |
| 245         | 222         |
| 862         | 799         |

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:

![Comparative analysis of Decryption delay for Text file](image)

**Figure 13 Comparative analysis of Decryption delay for Text file**

The data set of EXCEL file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 178            | 155            | 10       |
| 257            | 245            | 20       |
| 166            | 122            | 30       |
| 761            | 760            | 40       |
| 545            | 484            | 50       |
| 284            | 205            | 60       |
| 52             | 43             | 70       |
| 568            | 532            | 80       |
| 542            | 459            | 90       |
| 735            | 653            | 100      |

**Table 11 Data set of Excel file**

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:
The data set of IMAGE file is as follows:

| RSA ENCRYPTION | AEA ENCRYPTION | SIZE(KB) |
|----------------|----------------|----------|
| 641            | 633            | 20       |
| 564            | 502            | 30       |
| 432            | 388            | 40       |
| 677            | 555            | 50       |
| 468            | 438            | 60       |
| 355            | 344            | 70       |
| 321            | 290            | 80       |
| 615            | 598            | 90       |
| 367            | 309            | 100      |
| 608            | 536            | 110      |
| 179            | 170            | 120      |
| 323            | 278            | 130      |

Table 12 Data set of Image file

The following graph shows the comparative analysis of Decryption delay between RSA algorithm and proposed algorithm:
4. Conclusion:
The approach depicts the difference in the performance of RSA and proposed algorithm. The major reason for the improvement is only the reduction in computation time. Although, it has been noticed that time required to encrypt and decrypt with RSA is more than the time elapsed with the proposed algorithm yet it is not tested with any of the tools. This paper describes new method to encrypt and decrypt with the above mentioned scope and depicts that it is much better than renowned RSA algorithm.

5. Future Scope:
The paper can be enhanced with taking other types of files such as zip files, rar files as well as large files. I wish that somebody should apply new technique to reduce time for the algorithm designed as well as the technique applied for the above mentioned encryption and decryption.

References:
[1] Ahmed M, Litchfield A T 2016 Taxonomy for identification of security issues in cloud computing environments Journal of Computer Information Systems 58:1 pp 79-88.
[2] Anisetti M, Ardagna C, Damiani E, and Gaudenzi F 2017 A semi-automatic and trustworthy scheme for continuous cloud service certification IEEE Transactions on Services Computing 10:1 pp: pp 30 -43
[3] Annette JR, Banu WA and Chandran PS 2015 Rendering-as-a-service: taxonomy and comparison Procedia Computer Science 50 pp 276–281
[4] Bajaj A (2000) A study of senior information systems managers decision models in adopting new computing architectures Journal of the Association for Information Systems 1
[5] Baldwin LP, Irani Z and Love PED 2001 Outsourcing information systems drawing lessons from a banking case study European Journal of Information Systems 10:1 pp 15–24
[6] Bayramusta M, Nasir VA 2016 A fad or future of IT?: a comprehensive literature review on the cloud computing research International Journal of Information Management 36:4 pp 635–644
[7] Benlian A, Hess T 2011 Opportunities and risks of software-as-a-service findings from a survey of IT executives Decision Support Systems 52:1 pp 232–246
[8] Benlian A, Kettinger WJ, Sunyaev A and Winkler TJ 2018 The transformative value of cloud computing a decoupling, platformization, and recombination theoretical framework Journal of Management Information System 35:3 pp719–739
[9] Bharadwaj A, El Sawy O A, Pavlou P A and Venkatraman N 2013 Digital business strategy: toward a next generation of insights MIS Quarterly 37:2 pp 471–482
[10] Bhattacherjee A, Park SC (2014) Why end-users move to the cloud: a migration-theoretic analysis European Journal of Management Information System 23:3 pp 357–372
[11] Burda D and Teuteberg F 2014 The role of trust and risk perceptions in cloud archiving — results from an empirical study J. High Technology Management Research 25:2 pp 172–187
[12] Cafaro M and Aloisio G 2011 Grids, clouds, and virtualization Computer communications and networks pp 1–21
[13] Cloudscene 2018 Top ten data center operators in North America, EMEA, Oceania and Asia for the January to March 2018 period. Accessed 11 Dec 2018.
[14] Dašić P, Dašić J and Crvenković B 2016 Service models for cloud computing: search as a service (SaaS). Int J EngTechnol 8:5 pp 2366–2373
[15] Doelitzscher F, Fischer C, Moskal D, Reich C, Knahl M and Clarke N 2012 Validating cloud infrastructure changes by cloud audits. In: IEEE Eighth World Congress on Services Honolulu, HI pp: 24–29.
[16] Rastogi R, Agarwal G and Shukla R K 2021 Interactive Security of Ransomware with Heuristic Random Bit Generator. In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer, Singapore.
[17] Taneja A, Shukla R K 2021 Comparative Study of RSA with Optimized RSA to Enhance Security. In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer.
[18] Sisodiya A K, Yadao K N and Dhawale V R 2019 An analytical study on cloud computing International Journal of Engineering Technologies and Management Research 6:12, 73-77.
[19] Semsar H R, Daneshjoo P and Rezvani M H 2017 Cloud computing security solution based on grc method and fully homomorphic encryption algorithm in a private cloud International Journal of Science and Engineering Investigations 6:69.
[20] Kilari N 2018 Cloud Computing - An Overview & Evolution 3:1 pp149-152.
[21] Kumar R and Goyal R 2019 On cloud security requirements, threats, vulnerabilities and countermeasures: A survey Computer Science Review 33 pp 1-48.
[22] Anshika Negi, Mayank Singh and Sanjeev Kumar 2015. An Efficient Security Framework Design for Cloud Computing using Artificial Neural Networks. International Journal of Computer Application (IJCA), USA, vol. 129, no. 5, pp. 17-21.
[23] Bindu P, Bhaskar T and Reddy An exploration of security issues for cloud computing Journal of Engineering Sciences 11(1) Jan /2020 ISSN NO:0377-9254.