International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 20 (2019) pp. 3918-3923
 https://dx.doi.org/10.37622/IJAER/14.20.2019.3918-3923

Analysis and Implementation of AES and RSA for cloud

Manoj Tyagi
Research Scholar, Computer science, faculty of engineering
Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya, Chitrakoot, Madhya Pradesh, India.

Manish Manoria
Professor, Department of Computer Science and Engineering
Sagar Institute of Research and Technology, Bhopal, Madhya Pradesh, India.

Bharat Mishra
Associate Professor, Faculty of Science & Environment, Department of Physical Sciences
Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya, Chitrakoot, Madhya Pradesh, India.

Abstract
Cloud computing is recently a vogue in IT cooperate world. The cloud server provides various services to customers like software, storage, and infrastructure. Every Start-Up, small company or big company needs a space where they can store their data and use it whenever it is required. Cloud provides you one of the most important services that are storage, where security is necessary aspect. This paper analyze the most popular symmetric algorithm AES and asymmetric algorithm RSA, It also suggested a hybrid model for achieving data confidentiality and key privacy by combining these famous algorithm. Additionally it implements the various modes of AES and also implements RSA on various key sizes in java. Finally generate the graph on the basis of implementation which shows the performance of AES and RSA.

Keywords: Cloud computing, Symmetric algorithm, Asymmetric algorithm, AES, RSA, Hybrid model

INTRODUCTION

Cloud computing is the most recent growing technology; it enables unlimited capacity for storage by incorporating shared memory management over the network. Cloud server gives a new model for service in which stored data are preserved, organized and backed up remotely and cloud users get facility of particular service over the internet at irrespective time and place. The advantages of cloud computing technology are that services are available all time at low cost. Cloud computing is based on the architecture of an advanced information system. The cloud computing model rotates around three functional units such as Cloud Service Provider (CSP), client and user. CSP is an entity, which oversees Cloud Storage Server (CSS), has huge storage space to safeguard the data and high computation power [1].

In cloud computing two models are used they are deployment models and service models. Deployment model will define the access type to the device in the network based on cloud computing. In cloud computing access type is classified into four models they are public, private, hybrid and community. In public access type, cloud allows all the devices connected in cloud based network to get the facility of particular service. The nature of this type is openness, and then it requires more security concern as compared to others. In private access type, services are available only within the organization, it provides high security. In community based access type, services are utilized by organizations which belong to the same group. In hybrid based access type, private and public clouds are combined so this type is highly vulnerable to attack [2].

Service models are the orientation model. In cloud computing three types of service models are available. They are infrastructure as a service, platform as a service and software as a service. Infrastructure as a service model permits access to basic resources including virtual machines, virtual storage and physical machine. Platform as a service model enables the environment in runtime for applications also for development. Software as a service model provides application software to the users. Moving data into the cloud provides incredible comfort to users since they don't need to think about the complexities of direct hardware management. An online services as web based applications, do offer large amount of space for storage and sharing computing resources. This type of computing is eliminating the requirement of built-in devices for resource preservation. Therefore, cloud based users are at the clemency of their service providers for the availability and integrity of their information [3]. Cloud can confirm the user’s data security through the concept of firewalls, virtual private networks and by executing other security policies with in its own boundaries. Security is key component for distributed computing framework, where users access the cloud only when CSP approved its access by verifying it. From the perspective of information security, which has dependably been noteworthy part of nature of administration, Cloud computing faces new difficult security dangers for number of reasons [4].

Initially, traditional cryptographic primitives for the reason of data security shield cannot be directly espoused due to the lack of control on data under cloud computing. Hence,

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 20 (2019) pp. 3918-3923
 https://dx.doi.org/10.37622/IJAER/14.20.2019.3918-3923

verification of exact data storage in the cloud must be directed without explicit knowledge of the entire data. Considering numerous issue of data protection for every client, those put their data from distant location in the cloud and believe on cloud which guarantee of their data security.

The data stored in the cloud may be regularly updated by the users. To ensure storage accuracy under dynamic data update is principal prominence of cloud. However, this dynamic feature also makes traditional integrity insurance strategies worthless and involves new solutions. Last yet not the slightest; the game plan of cloud computing is controlled by server running in a simultaneous, conjoined and dispersed way. Generally, effective security methods for storage is utilized for achieving strong and secure data storage on cloud based system in the real scenario [5].

MOTIVATION

Organizations store their customer's data on cloud. This allows customers to access their data from anywhere and anytime. But most of the times organizations fail to prevent unauthorized access to the data. Cloud computing is the most efficient and affordable solution for businesses but comes with severe issues which can leave the data vulnerable. To secure the data, the organizations must implement some policies to define data access rules and roles clearly. The authentication, confidentiality and integrity are main issues considered in security issues. Encryption is one of the most trusted ways to ensure the security of data. In encryption, convert the data in to elusive format at sender side and in decryption, convert back in to original form at receiver side. This approach is widely used for storing, and communication of data. Security issues invite the researcher to study and analysis this area.

PROBLEM FORMULATION

Mostly persons and enterprises utilize the cloud for keeping their data. For avail this service there is need to register with cloud. Cloud only enable their services for registered clients after verify them by effective authentication scheme. For maintaining privacy, authentication is compulsory steps. Single level authentication is generally used but in case of financial services or sensitive data protection, multifactor authentication is recommended [6]. Files encrypted using asymmetric encryption techniques take a large amount of time in encrypt/decrypt process while when symmetric techniques are used it takes very less time as compare to asymmetric techniques. But the trust regarding the key security is major issue in symmetric approach, because key is shared between sender and receiver. To keep the data safe from the third parties, ultimately increase the standard of security by the combination of asymmetric and symmetric encryption techniques which is called hybrid model [7]. In symmetric encryption, AES is widely accepted and popular for encrypting small to large data. In asymmetric encryption RSA is famous and used by many organizations for encrypting only small data like keys, password, and metadata. For these reasons, first analysis AES and RSA separately to verify their performance, then design a hybrid model by combining AES with RSA which reduce the time complexity and enhance the security. Elliptic curve is also most popular and replacement of RSA. It is efficient and offered less key size as compared to RSA for attaining same security level [8].

ADVANCE ENCRYPTION STANDARD (AES)

AES utilizing substitution and permutation process which is the basic principle behind this idea. It has fixed block size of 16 bytes (128 bit) and variant key sizes 16 byte, 24 byte (192 bit) , and 32 byte (256 bit). Transformation rounds on a block are specified using key size which is fixed in numbers. 10 rounds for 16 byte size key, 12 rounds for 24 byte size key and 14 rounds for 32 byte size key [9]. For encryption, the first step is Add round key and then apply n rounds , namely usual rounds and final round by applying round key where final round is different. In usual round four steps are executed: sub bytes, shift rows, mix columns and add round key in a sequence. Then comes final round, under which three steps are executed: sub bytes, shift rows and add round key. Here, the usual round is repeated n-1 times where n depends on the key size as mentioned already. Ciphering and deciphering algorithms are different, then for decryption, inverse shift rows, and inverse sub bytes, add round key, inverse mix column are sequentially executed in usual round and inverse shift rows, inverse sub bytes and add round key are executed in final round [10].

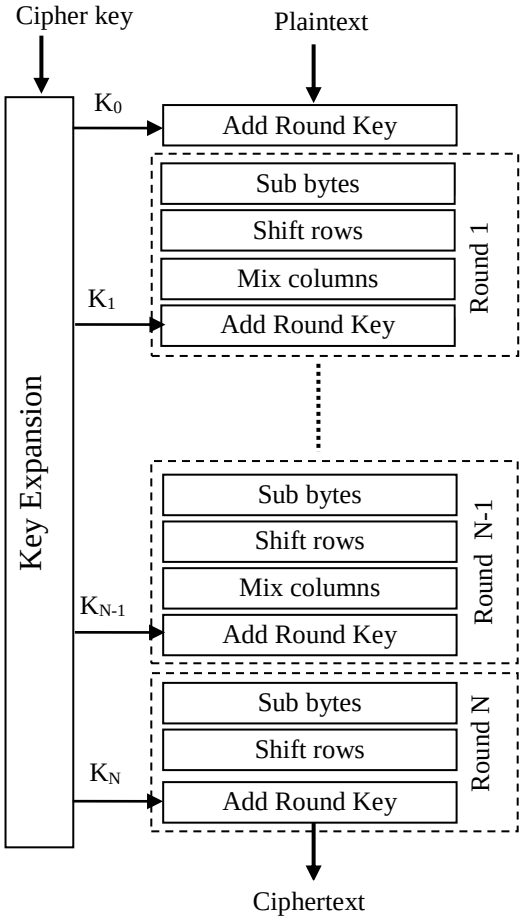

Figure 1: Encryption Process of AES

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 20 (2019) pp. 3918-3923
 https://dx.doi.org/10.37622/IJAER/14.20.2019.3918-3923

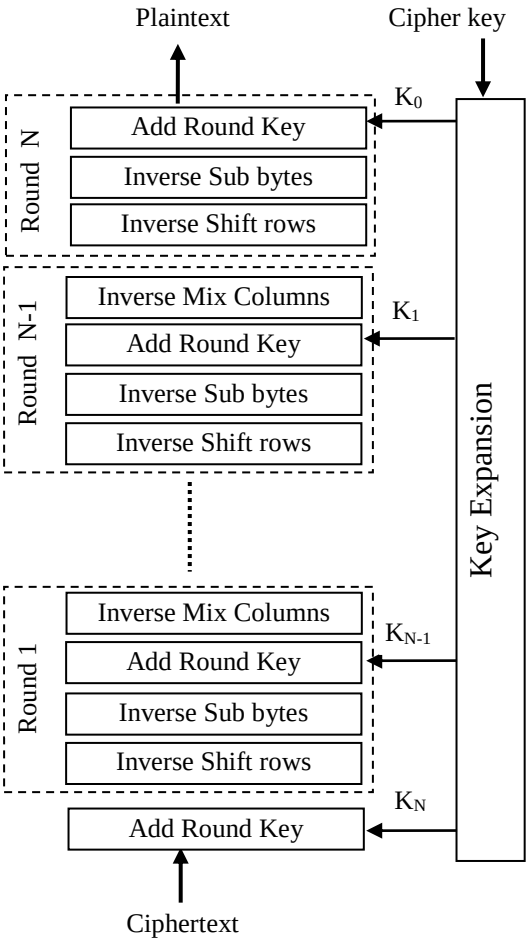

Figure 2: Decryption Process of AES

The security provided by the AES algorithm is higher as compared to other symmetric techniques. The technique is vulnerable to brute force attacks when the key size is kept small. Recommended key size is 16 byte (128 bit) or more for preventing such attacks. AES is available in various modes and widely used according applications [11].

Electronic codebook (ECB) Mode
Data is partitioned into block; where encryption is performed on each block separately. So it is not recommended to hide the sensitive information. Lack of diffusion is the main disadvantage of this mode. It faces the replay attacks.

Cipher Block Chaining (CBC) Mode
First each block is Ex-ored with previous cipher block after that apply encryption on it. CBC is mostly used mode of AES.

Cipher Feedback (CFB) Mode
Operation is extremely similar; specifically, CFB decryption is almost indistinguishable to CFB encryption which is done in reverse order.

Output Feedback (OFB) Mode
It creates a block cipher to a synchronous flow cipher. It creates key-stream locks, which subsequently XORed with a block of plain text to find the ciphertext.

Counter (CTR) Mode
CTR style has related characteristics to OFB; however, it also supports a random-access throughout decryption. CTR mode is ideal for working on a multiprocessor machine wherever blocks can be encoded in parallel. Moreover, it does not experience the short-cycle problem.

Galois/Counter (GCM) Mode
It is Widely adopted due to its performance. GCM may take complete benefit of concurrent processing, and executing GCM could create efficient usage of hardware pipeline.

Security Analysis of AES

While considering the analysis of the AES, treating security as a point since the AES is the successor of the DES (Data Encryption Standard) all the known attacks on DES are tested and AES beats them all, like brute-force, statistical, differential and linear attacks. And since the AES is having very less requirement of processor usage, it is quite fast and widely used.

RSA ALGORITHM

It is public key approach for enciphering and deciphering the data. It is the most popular asymmetric or public key cryptography that works on the concept of dual keys. The sender's public key is utilized to encrypt the message whereas the secret key is utilized for decryption. Public key cryptography is popularly applying for authentication, key exchange and digital signature. It is most adaptable and universally used algorithm which depends upon prime factorization. For obtaining the security, this algorithm considers the large prime number. It is utilized in ecommerce security, virtual private networks, emails, and handles the authenticity of e- documents. For secure transmission of the data over the open network, asymmetric encryption is a very important technique [12]. It has three processes namely key generation, encryption and decryption.

Key Generation Process

It generates the two different keys, one for encryption and other for decryption. Following are the procedure to create the keys.

1. Take two large prime numbers m and n randomly.
2. Calculate $p = mn$
3. Compute $\varphi(p) = (m-1)(n-1)$
4. Choose integer e such that $\gcd(\phi(p), e) = 1$ and $1 < e < \phi(n)$
5. Compute $d \equiv e^{-1} (\mathrm{mod}\, \phi(n))$
6. Public Key: (e, p)
7. Private Key: (d, p)

Encryption process

It creates cipher text by applying public key on plaintext P at sender side.

$$C = P^e \bmod p$$

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 20 (2019) pp. 3918-3923
 https://dx.doi.org/10.37622/IJAER/14.20.2019.3918-3923

Decryption process

It finds the plaintext by applying private key on cipher text at receiver side.

$$P = \left(C^d \bmod p\right)$$

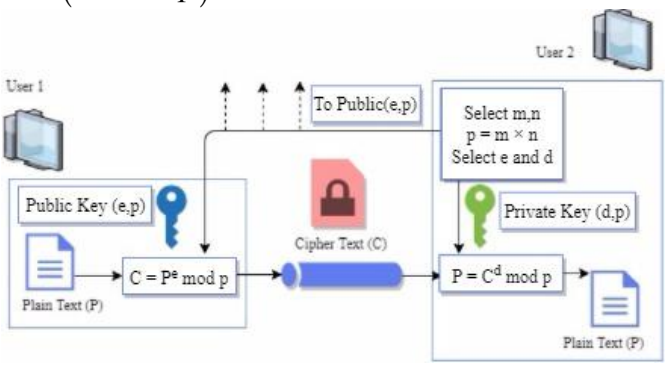

Figure 3: Process of RSA Algorithm

Analysis of Attacks on RSA

- One of the possible attacks on RSA can be by factoring the value of p. After knowing the factors of p one can easily find totient and d. But factoring large number is hard and time consuming.
- RSA can be break if one can find totient without computing p and hence can find d but this method is more difficult and impractical.
- One can break this algorithm by determine the value of d without factoring p or computing totient but this method is also impractical.
- It also face common modulus attack. If everyone is given same modulus p but different (e, d) then it is possible to decrypt message without d.
- It also faces the forward search attack. If message space is predictable, attacker can decrypt ciphertext by encrypting all possible messages until a match with ciphertext is obtained.

Advantages of RSA

It is easier to understand and have **s**imple encryption and decryption process. It is widely deployed and has better industrial support.

Disadvantages of RSA

Key generation is very slow in RSA. Decryption process is also slow hence it is not suitable for large message. Key is vulnerable to various attacks if algorithm is poorly implemented.

HYBRID MODEL

Registered client want to keep their data on cloud. First, clients login on cloud by giving its credential. After successful client verification, CSP authorize the client to keep their data on cloud over internet. For authentication, two factors are used, where first factor is username-password , and second factor is OTP. There are following steps to keep the data on cloud through Hybrid model.

- Encryption is performed at data owner side for maintaining the trust of client. Client enciphers the data by applying AES using key k. Then AES key is encoded by RSA public key e.
- Data and key both are secure in communication channel, and through internet data owner keeps their data on cloud.
- At the time of accessing the data, any authorized client first pass the authentication phase then get the data. By applying the RSA secret key d, find the AES key k and then using this key, decrypt the data successfully.
- Combine RSA and AES to enhance the security strength and reduce the time complexity.
- RSA encipher the information by applying various key sizes such as RSA-1024, RSA-2048, RSA-3072, RSA-4096. Selection of key size is depending on required security level. For more security prefer large key size.
- AES encipher the data by applying various key sizes such as AES-128, AES-192, and AES-256. Selection of key size is depending on needed security strength. Larger key provides more security.

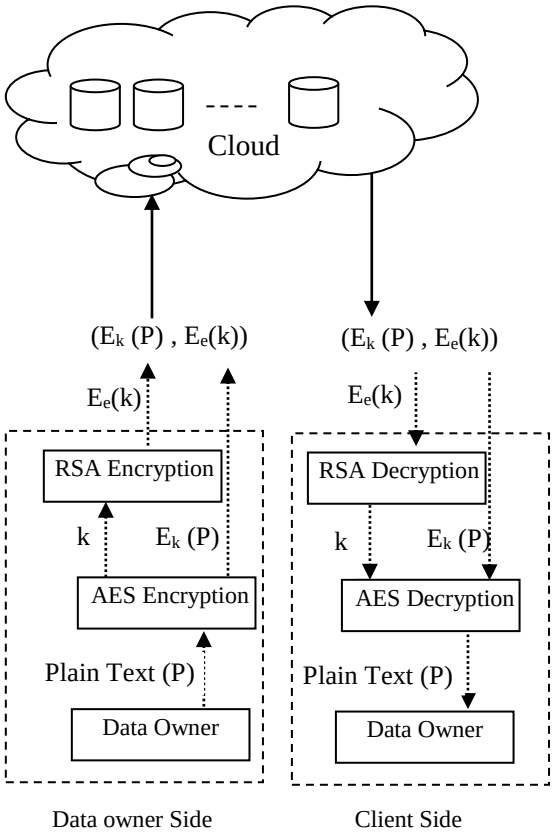

Figure 4: Hybrid Model

PERFORMANCE AND RESULT

AES and RSA are implemented on Intel X-64 based Processor i5-8250 U with speed 1.60 to 1.80 Ghz with 8 GB in environment of 64-bit operating System. Implement and analyze the time complexity of various modes of AES algorithm on 5 Notepad text file of size 1 MB, 2 MB, 3 MB, 4 MB, and 5 MB respectively , over average of 100 iteration .

The resulting time is pure execution time because reading writing time of file is not added in this time. This implementation result shows that AES is taking very less time to encrypt/decrypt the file, so it is feasible to encrypt the large file also. It is also observed that encryption and decryption time is identical. AES-ECB is very fast, and remaining modes are also fast except GCM. CBC is more secure than ECB which recommend CBC for data storage. GSM is also effective in security point of view and its time is more as compared to other modes of AES but it is efficient with respect to other symmetric approaches.

Here Execute the RSA algorithm on 1 KB file for various key sizes over 10 iterations on same machine. It is observed that encryption time is little bit increases but decryption time is rapidly increasing when increasing key sizes. It also proves that RSA is very slow as compared to AES, that's why it is not feasible for large file encryption. So it is used for small data. Now-a-days quantum concept improves the speed of system which calculates prime factorization in less time, so RSA key size face trouble because of computer
speed. To achieve security in RSA, solution is to increase the key size but we cannot increase key sizes more due to time complexity.

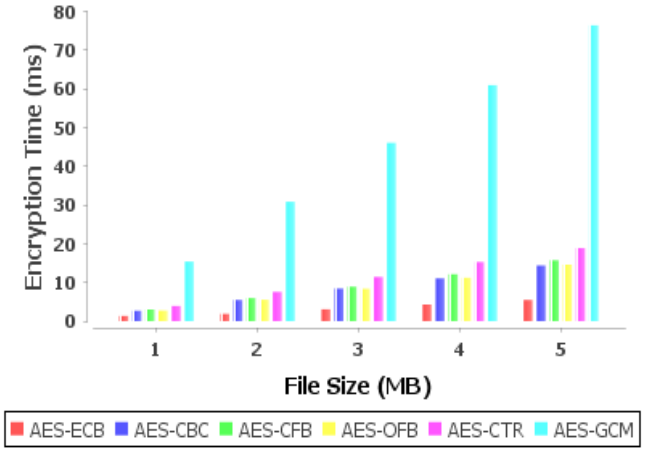

Figure 5: Encryption Time of Various AES Modes excluding read/write time

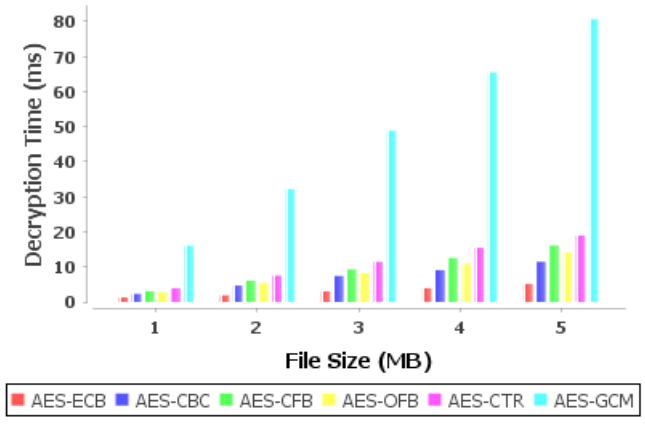

Figure 6: Decryption Time of Various AES Modes excluding read/write time

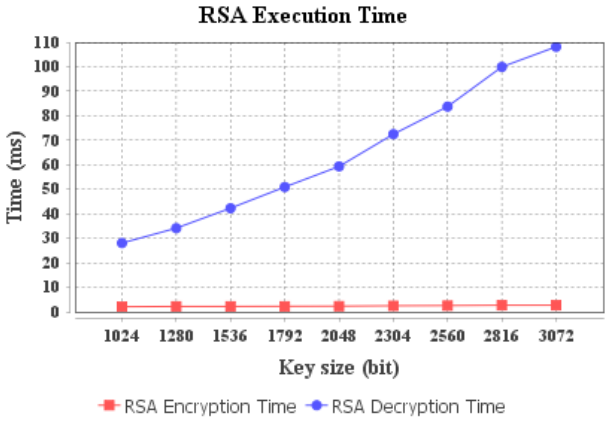

Figure 7: RSA Execution Time including read/write time

CONCLUSION

Now days in this fast running IT world, everything is trending towards the technology. Most people keep information on cloud and they can access their information from any location, any time from any devices. In this paper, implemented AES and RSA on various parameters in Java and on the basis of result analyze, it is observed that AES is efficient and suitable for large data, but because of single key, key security is major issue in AES. It is also find that RSA is very slow as compared to AES and time complexity of RSA is increases rapidly as increase in key size, that's why large key size is not suitable for RSA due to its slow execution time specially very slow decryption time. RSA is only feasible for encrypting small data. AES-128 and RSA 3072 are recommended for securing the data. This paper suggested Hybrid model by combining RSA and AES to attain the key privacy and data confidentiality both.

REFERENCES

[1] Bartolini C, Santos C, Ullrich C, "Property and the cloud". J Computer Law & Security Review 34(2) : pp. 358-390, 2017

[2] Buyyaa, R., Yeoa, C.S, Venugopala, S., Broberg, J., Brandic, I.: 2009 Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. J. Future Generation Computer Systems, Vol. 25, pp. 599-616, Elsevier

[3] Hsu C L, Lin J C C , "Factors affecting the adoption of cloud services in enterprises". J Information Systems and e-Business Management 14(4): pp. 791:822, 2016

[4] Ashish Singh, Kakali Chatterjee "Cloud security issues and challenges: a survey", Journal of Network and Computer Applications, Elsevier , 2017, vol. 79, Pages 88-115

[5] Ali, M ,Khan, S and, Vasilakos, A (2015) "Security in cloud computing: Opportunities and challenges", Information Sciences, Vol.305, pp.357-383

[6] Rohitash Kumar Banyal, Pragya Jain , Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing" Fifth International Conference on Computational Intelligence, Modeling and Simulation , IEEE , 2013, Pages 105 – 110

[7] Moghaddam, F., Alrashdan, M., Karimi, O.: A Hybrid Encription Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments. J. of Advances in Computer Network, Vol. 1, No. 3, (2013)

[8] Li X, Chen J, Qin D, Wan W, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC", ICALIP, IEEE 2010

[9] Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, Foti J, Roback E, " Report on the Development of the Advanced Encryption Standard (AES)", National Institute of Standards and Technology (2000)

[10] Almuhammadi S., Al-Hejri I., "A Comparative Analysis of AES Common Modes of Operation" In. 30th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE 2017

[11] Yuwen, Z., Hongqi, Z., Yibao, B.: Study of the AES Realization Method on the Reconfigurable Hardware. In: International conference on Computer Sciences and Applications, pp. 72 – 76. IEEE, Wuhan (2013)

[12] Karakra A, Alsadeh A, "A-RSA: Augmented RSA", SAI Computing Conference 2016, IEEE