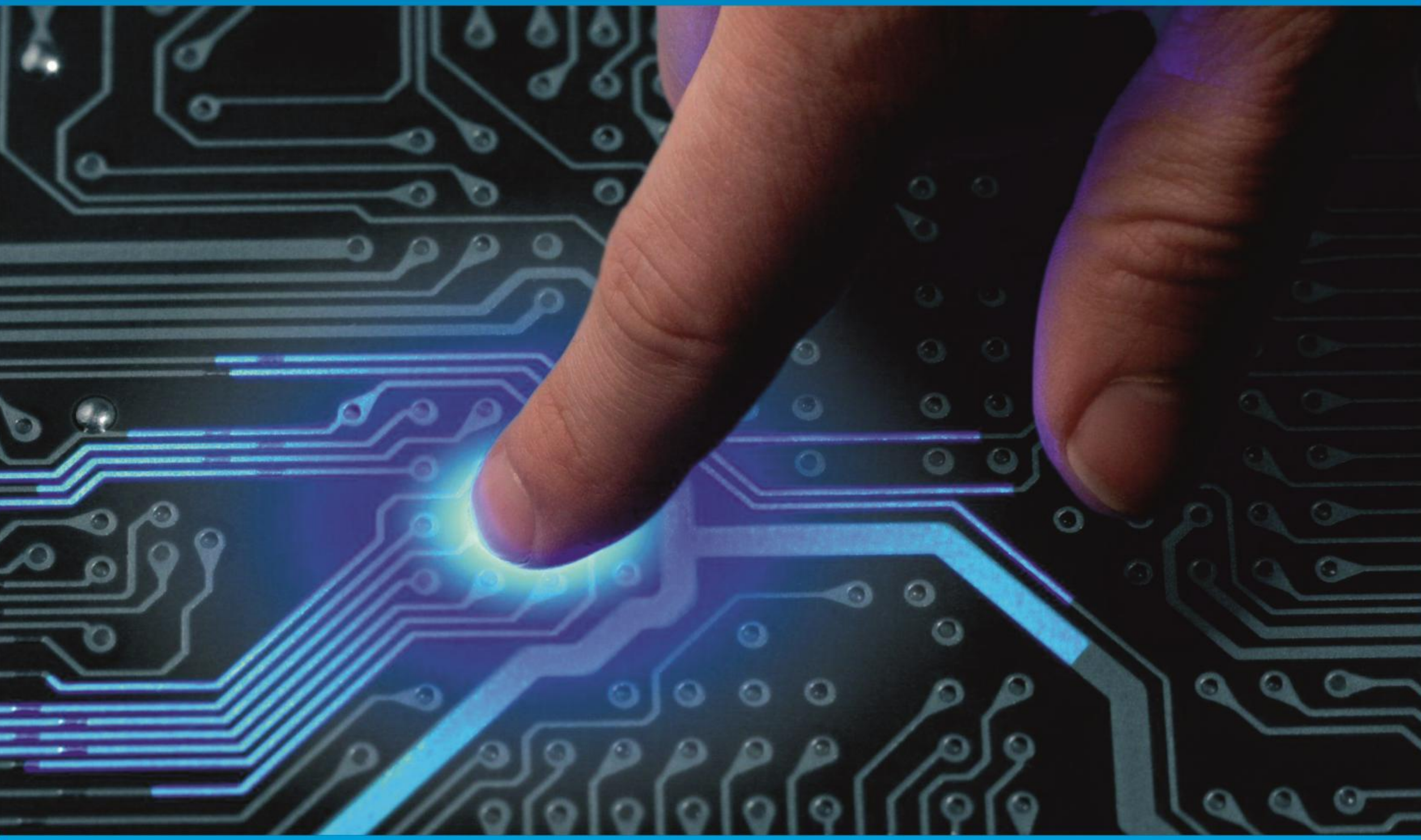
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Cloud Data Security Using Advanced Encryption Standard

Akash B. Bhawar

Research Student Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India

ABSTRACT: In the field of information technology, cloud computing does a very important role because it provides services, storage, network, and many other things. Cloud computing uses in many fields like education, business, etc. SaaS, PaaS, and IaaS such model provided by cloud computing, and an organization can make their businesses with less effort compared to any traditional computing. So, security became a big problem in such a sector to protect their data. Safe communication and transfer of data over the internet So, the major issue is security in cloud computing, and attackers always trying access that data and always ready to enter into the system. Symmetric and asymmetric algorithm of cryptography has used to secure the data. In this paper, we discussed how AES that is Symmetric algorithm works to secure the data before it reaches to the cloud. It encrypts the data into ciphertext and decrypts the data into its original form using AES 128, 192, and 256 bits of keys.

KEYWORDS: cloud computing, data security, cryptography, AES.

I. INTRODUCTION

Cloud computing resources provide many facilities to the user as well organization like data storage, network services through internet technology. Cloud computing also provides scalability, flexibility, cost-saving which are mainly done by virtualization. There are different kinds of models in cloud computing i.e. deployment and delivery. In cloud computing deployment models are the public, private, community, hybrid models and delivery models are Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS) [16]. the delivery models in the cloud represent the IT resource combination that is provided by the cloud provider. Cloud computing provides the demands of hardware, as well as software resources with very little effort in management and cloud infrastructure, provides functionality by using some components such processors, database, networks services, and operating system [17]. In data storage of cloud where the user and organization store their data files, that's why this part became very sensitive in the case of security. By using cryptography, we can secure the data. Cryptography is the most useful and powerful technique to protect the data from unauthorized parson or attacker by using Encryption and Decryption processes [14]. There are two key-Algorithms in cryptography are Symmetric and Asymmetric key algorithm. The Symmetric key algorithm is much secure than the Asymmetric algorithm. It consists of various symmetric algorithms like Advanced Encryption Standard, Data Encryption Standard, and blowfish, Triple AES, Triple DES, and Ron's code [17]. Now a day AES Encryption algorithm is the most powerful and rarely used to protect the data. Still, no attacker could crack AES encrypted data.

II. LITERATURE REVIEW

[1] The most important priority that security is a crucial issue, the author explained the system proposed concentrates on providing security to transferring data using encryption techniques.[2] the author Rajput, S et al, Dhobi, J. S. et al &Gadhavi, L. J et al talked about the AES algorithm (RIJNDAEL) that secures data in cloud storage and it was more efficient than DES where it is based on a Symmetry algorithm. [3] author Kumar, N. M proposed that this scheme could achieve fine-grained access control and any group of members access the use of a source in the cloud and revoked users cannot access the cloud again after they are revoked. [4] The author proposed a systematic way and opportunities in the case of cloud storage with the AES algorithm and also expressed the importance of encryption in data security.[5] The author said data security is the main problem in a case to secure the data in cloud computing, can't be completely trusted with the cloud provider. Verification of integrity and time consumption can be managed by using AES and RC6 algorithm. [6] An introduced novel method to protect personal as well as organizational data and cloud storage. Also proposed strength of authentication about security with help of AES and time-stamping algorithm while sharing data integrity.[7] Millions of people use the cloud for various purposes so they need security and safety services, the author proposed very simple data protection that is to be encrypted using the AES algorithm.[8] Proposed that the cloud provide data storage that's came with various advantages but it also came with risk and vulnerabilities so it was a good idea about encryption to secure data and

its transformation in the cloud.[9] the author introduced a new security mechanism the usage of symmetric key cryptography set of rules and steganography .in this proposed gadget AES set of rules are used to offer block sensible safety to records, Kakade, V et al,[10]Author M. Bhansali et al proposed a simple data protection model where data is encrypted using the Advanced Encryption Standard (AES) before it was launched in the cloud, thus ensuring data confidentiality and security.[11] Kumar, P et al proposed that security compression to the data with AES and they also examined encryption and decryption of AES that result more security to the data.[12] The author Sachdev, A et. al proposed the model where the data protected using Advanced Encryption Standard while it launched in the cloud to became secure and protected from malicious activities. [15] The article is related to the level of models that is SaaS, IaaS, and PaaS. Also explained about security in data using various encryption algorithms, said by Albugmi, A et al.

III. **IMPLEMENTATION OF ALGORITHM**:

Advanced Encryption Standard:

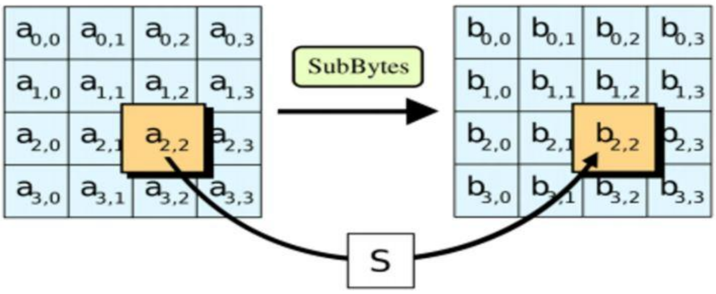
AES algorithm(RIJNDAEL) is a Symmetric cryptographic algorithm that processes 128 bits of a block of data. It is the most recent algorithm to encrypt the data. It is a Symmetric algorithm as it has the same keys for encryption as well as decryption. It has various keys to encrypt and decrypt the data. 128 bits keys have 10 blocks of a round, 192 bits kyes has 12 blocks of round and 256 bits key has 14 blocks of round and these keys are used to convert the data into cipher form and inverse cipher form using its different rounds. These keys indicate the length of the key. There are various steps to encrypt and decrypt the data in two processes as follows:

I. Encryption process.

I. Byte substitution(S-box).
II. Shifting rows.
III. Mixing the data within each column.
IV. Adding Round Key.

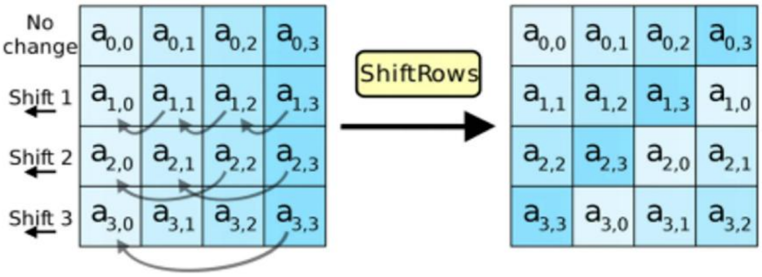
I. Byte Substitution:

In this step, the substitution of block text of 16 input bytes depends on the substitution of the box(s-box) is represented in a matrix that is four rows and four columns.


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

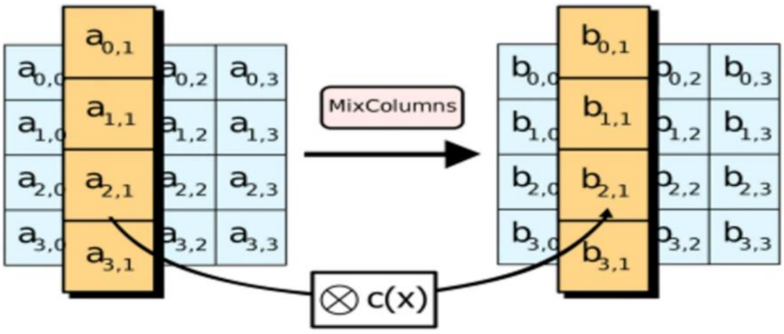
II. Shifting Rows:

This is a permutation step. In this step, all rows are shifted one by one to the left in which only the 1st row is not shifted. This form a new 16 bytes of a matrix, only the difference is rows are shifted to each other.


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

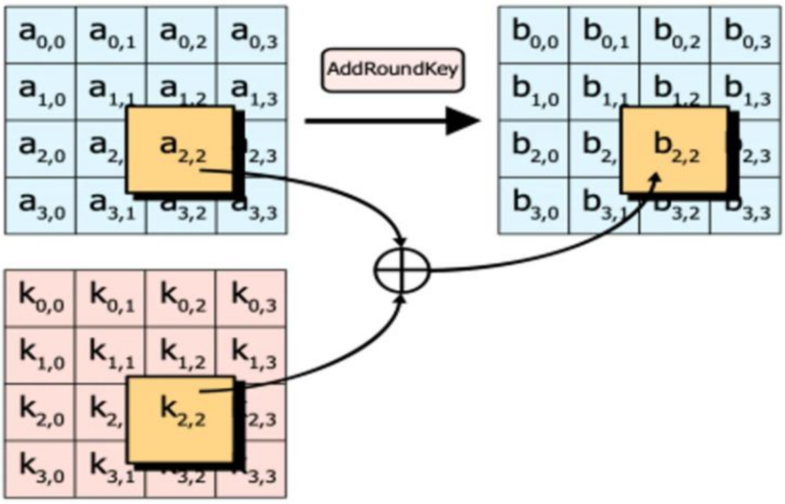
III. Mix columns:

In this step the operation is works on columns and combines 4 bytes in each column states.



IV. Add round key:

In this step, 128 bits of the round are bitwise XORed with 128 bits of the state. This operation is performed on column-wise operation between 4 bytes of a state column and one word of the round key. [15]. this step is also affected on each bit of state. [15].



II. Decryption process:

In the decryption process, it uses the same key as the encryption but it converts the ciphertext into plain text. It is the reverse of the Encryption process.

I. Adding Round Key.
II. Inverse Mixing the data within each column.
III. Inverse Shifting rows.
IV. Inverse Byte substitution(S-box)

AES in cloud computing:

User uploads their data or transfer the data to the cloud and then submit their services requirement that is provided by the cloud provider. While transferring data, the application uploads data to the cloud, it is encrypted into ciphertext and then sent to the cloud, and this is done by using AES encryption. To read or get that data is only after decrypting it, so the ciphertext converts into the plain text. Encrypted data doesn't store any related key. Users have to stored keys in their physical server. So, this is the best encryption algorithm to protect the data in cloud computing.

IV. CONCLUSION

Now a day cloud computing is a newer technology that provides various services and benefits to the user and also comes under security challenges. In this paper, we discussed encryption methods to evoked from risk in a case of security which is involved in the cloud. AES encryption is a powerful and fattest technique that has flexibility and scalability [16]. AES has high security because it has 128, 192, and 256 bits of keys used in the algorithm. It protects the data against malicious attacks and, it also secures the data from square attacks, keys attacks, and such various attacks that are always trying to get the user data in the cloud. AES is a very secure algorithm that secures data from phishing. It is most powerful and has high storage capacity and high performance with no drawbacks compared to other Symmetric algorithms which have some weaknesses.

ACKNOWLEDGEMENT

I would like to acknowledge Prof. Swapna Augustine Nikale, Department of Information Technology, B. K. Birla College (Autonomous) Kalyan for guidance and support to this Research work.

REFERENCES

[1] Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017). Enhanced cloud data security using AES algorithm. *2017 International Conference on Intelligent Computing and Control (I2C2)*, 109–115. https://doi.org/10.1109/i2c2.2017.8321820

[2] Rajput, S., Dhobi, J. S., &Gadhavi, L. J. (2016). Enhancing Data Security Using AES Encryption Algorithm in Cloud Computing. *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*, 135–143. https://doi.org/10.1007/978-3-319-30927-9_14

[3] Kumar, N. M. (2017). Encrypted Bigdata Using AES Deduplication in Cloud Storage. *International Journal of Engineering and Computer Science*, *6*(7). Retrieved from http://103.53.42.157/index.php/ijecs/article/view/2715

[4] Hidayat, T., &Mahardiko, R. (2020). A Systematic Literature Review Method on AES Algorithm for Data Sharing Encryption On Cloud Computing. *International Journal of Artificial Intelligence Research*, *4*(1), 2579–7298. https://doi.org/10.29099/ijair.v4i1.154

[5] Krishnan, M., priya, H., devi, A., &pthi, D. (2019). Security Enhancement and Time Delay Consumption for Cloud Computing Using AES and RC6 Algorithm. *Bonfring International Journal of Software Engineering and Soft Computing*, *9*(1), 01–06. https://doi.org/10.9756/bijsesc.9003

[6] Sheeja, R., Bibin, C., Krishnan, P. R., Nishanth, R., Gopinath, S., & Ashok, K. G. (2020). Secure File Sharing System in Cloud Using AES and Time Stamping Algorithms. *IOP Conference Series: Materials Science and Engineering*, *906*, 012023. https://doi.org/10.1088/1757-899x/906/1/012023

[7] Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., &Ditta, A. (2020). Secure Framework Enhancing AES Algorithm in Cloud Computing. *Security and Communication Networks*, *2020*, 1–16. https://doi.org/10.1155/2020/8863345

[8] Sachdev, A., & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. *International Journal of Computer Applications*, *67*(9), 19–23. https://doi.org/10.5120/11422-6766

[9] Wani, A. R., Rana, Q. P., & Pandey, N. (2020). Cloud Data Security Using Modified AES Algorithm with Advanced User Authentication System. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(9), 13–19. https://doi.org/10.5373/jardcs/v12i9/20202615

[10] Kakade, V. S., Kirve, A., Bhoir, A., & Kadam, S. (2017). Enhancing Distributed Data Storage Security for Cloud Computing using AES algorithm. *IJARCCE*, *6*(3), 752–755. https://doi.org/10.17148/ijarcce.2017.63178

[11] Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. *Optik*, *127*(4), 2341–2345. https://doi.org/10.1016/j.ijleo.2015.11.188

[12] Sachdev, A., & Bhansali, M. (2013b). Enhancing Cloud Computing Security using AES Algorithm. *International Journal of Computer Applications*, *67*(9), 19–23. https://doi.org/10.5120/11422-6766

[13] Salman, S. A. (2018). New Method For Encryption Using Mixing Advanced Encryption Standard And Blowfish Algorithms. *المجلة العراقية لتكنولوجيا المعلومات*, 33. https://doi.org/10.34279/0923-008-002-007

[14] https://www.researchgate.net/profile/Ako_Abdullah/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf

[15] Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016). Data security in cloud computing. *2016 Fifth International Conference on Future Communication Technologies (FGCT)*, 2377–2638. https://doi.org/10.1109/fgct.2016.7605062

[16] Smitha Nisha Mendonca. (2018). Data Security in Cloud using AES. *International Journal of Engineering Research And*, *V7*(01), 205–208. https://doi.org/10.17577/ijertv7is010104

[17] Jothy, K., Sivakumar, K., & M J, D. (2018). ENHANCING THE SECURITY OF THE CLOUD COMPUTING WITH TRIPLE AES, PGP OVER SSL ALGORITHMS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *2*(7), 75–82. https://doi.org/10.5281/zenodo.1165634

[18] Pitchaiah, M., Philemon, D., & P. (2012). Implementation of Advanced Encryption Standard Algorithm. *International Journal of Scientific & Engineering Research*, *3*(3), 1–6. http://www.ijser.org

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details