IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Literature Review of Data Encryption Techniques

[1]Suyog Sunil Kotkar, [2]Sachin Arun Thanekar

[1]Master of Engineering, [2] Master of Engineering

[1]Computer Engineering,

[1]Amrutvahini College of Engineering, Sangamner, India

Abstract: In this IT world, databases contain lot of confidential and sensitive details of different organizations all over the world. But the data gets vulnerable due to the lack of default potent security tools in Hadoop. Many security issues which were not given preference earlier emerge due to its flexibility. These issues are dangerous for our data and could lead to an attack. The users are forced to install various external security tools to protect their data clusters. The security of Hadoop framework is getting better in the versions but it has a very little effect. Database security is the most important one. Encryption secures data within database. All the data will be changed as cipher text. So, no use of hack it. There are number of methods and techniques are available to encrypt a database. So in this paper, we will discuss about the various techniques for encryption and decryption data to secure data over cloud.

Index Terms **- Encryption, decryption, AES, OTP, RC4, cryptography, cipher, cloud, big data, bite, DES, HDFS, RSA, hybrid key, data, security**

I. INTRODUCTION

The high growth in the cloud computing technology leads a common culture for interchanging of the digital data very drastically. Hence it is more vulnerable of duplicating of digital information and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like companies confidential papers, miletry data, governoment secert information and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. Data encryption have applications in many fields including the internet communication, companies communications, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues. The performance of all those encryption techniques are studied and discussed in later chapters of the paper.

II. LITERATURE SURVEY

In DES algorithm there is used 64 bit of plain text and key with 56 bit is used. It also works on various shifting and XOR operation. DES has a main problem of key. Its key size is too much small so attacker can get the plain text.[1]

3DES is a new technique of the DES. It performs same operation as a DES but the difference is that it is encrypted three times so it is more secure than DES. The main problem is that it uses three time level of encryption which becomes very much slower than other method.[2]

AES is founded by Rijndael. AES has block size of 128 bits and key sizes of 128, 192, and 256 bits with 10 rounds, 12 rounds, and 14 rounds. In this algorithm XOR, mix columns, shift rows, add round key operations are performed. This algorithm suffers from brute force attack because if attacker has dictionary then he can easily break the word which is the key.[3]

Blowfish is the fastest and secure than above three algorithms. It has 32–448 bits of key length which is changeable, and its block size is 64 bits. Main advantage of the Blowfish is that it is openly available and not payable. These all have some weak points. Like long range of key provides high security than short. Very typical structure increases execution time.[2]

AES algorithm results using encryption into file size increased to double of the original file and hence file upload time also increases. The technique [4] used removes this drawback in this project. The technique has implemented the method in which OAuth is used for authentication and authorization of client in the conventional client-server model. The authorization token used for secure data on HDFS by a Key that generated by it. this project enhanced file uploaded time using OAuth does achieve the authentication.

Triple encryption scheme [5] integrated into Hadoop based cloud data storage by adding the hybrid encryption to encrypt HDFS files using RSA and DES based on IDEA to encrypt user's RSA private key to encrypt the files in HDFS when being stored in a buffer after uploading it to the HDFS. paper improved the performance of data encryption and decryption using MapReduce to make decryption parallel.

The aim of the cryptography is to transfer data in very secure manner between two parties over a network. Bhoomika Modi and Vinitkumar Gupta[6] have proposed "The novel security mechanism in symmetric cryptography using MRGA" used to overcome some disadvantages. It gives high throughput and is more secure. It has easy process for encryption and decryption. For security purpose they have used Magic Rectangle Generation Algorithm (MRGA) of size 16 × 24. Main benefit of MRGA algorithm is that it provides more security in starting Min, Max values because those values are transfer to the receiver in encrypted form. So attacker cannot know that values even he has table. But they haven't applied this algorithm on the large database and also comparison of this algorithm with others are missing.

Aaron Barrera, Chu-Wen Cheng and Dr. Sanjeev Kumar conducted study on the most popular encryption algorithm AES[7]. They targeted one mode of operation, Cipher Block Chaining (CBC), in terms of encryption time and delay on the Mix columns section. The results reveals that using parallelism in signal processing results in less time delay, logic elements and virtual memory. In the future work, they are going to focus on other sections for parallelization and try to implement AES on the FPGA. Finally, they will be able to obtain optimized area and speed hardware implementations of AES based on the sub-pipelined architecture.

Hadeer Mahmoud et al. [8] have introduced an enhancement algorithm to protect the data in HDFS. According to this algorithm, AES algorithm is used to encrypt two thirty of the data in the file, while the OTP algorithm is used to encrypt the rest of data. On the other hand, the OTP is a stream cipher algorithm which grantees the data confidentiality. The concept of OTP algorithm is that a password is used for one and only one session. In addition, the password is generated automatically using a recalculated method instead of choosing by the user Dictionary. This removes the constraints of the Longevity of the password. In addition, by using the OTP algorithm, the encrypted file size has been reduced relative to the encrypted file using the Block cipher. In spite of the simplicity of the OTP algorithm, and the size of data file is not increased, the used a OTP key size (192bit) after encryption using the AES will be added to every block. So, the encrypted file will be increased. By using the OTP and AES algorithms to encrypt the data, the performance of data encryption/decryption has been enhanced. Unfortunately, using the AES to encrypt a part of data (i.e., 2/3 of data size), the size of the original data file has been increased by 20%.

Venkat Krishna Pavan Kalubandi and Yamuna M, proposed Byte Encryption of a string using periodic table. The periodic table has 118 elements and the characters are randomly assigned in the table. So unless this is known it is tough to decrypt the message. Also each cell of the periodic table is assigned a 8 – bit code. So unless this is known, decryption is not possible. The periodic elements are randomly assigned to each character in the original text. Decrypt the encoded text as same way as encoded using key value but in the reverse order. Also, periodic table is not in wide use for encryption, decryption. Periodic table not using generally other than it is used in drug encryptions, encode chemical composition of drugs. The proposed method is also user friendly and can be implemented in any programming language. So the proposed method is safe for encryption of any text message[10].

Research conducted by Ketan and Vijayarajan [12] proposed hybrid RC4 and AES methods with modifications. The number of rounds at AES is reduced from 10 to 6 to increase encryption speed. Based on the results of the test, this method can indeed work faster than the AES method but is longer than the RC4 method only. This research also claims that this method has good security, but the security tests performed are incomplete and only analysis.

Hybrid-Key Stream Cipher Mechanism introduced by Omar Helmy Khafagy, Mohamed Hasan Ibrahim and Fatma A. Omara is one of the best hybrid encryption mechanism[9]. Instead of relay on a any single encryption technique, they have used two best techniques ie. AES and OTP (one time pad). OTP used for encryption of main data and then OTP key encrypted using AES algorithm. System returns AES key in a file as a secret/private key file. Same file owner can use to decrypt the encrypted data. According to the work in this paper, a hybrid-Key stream cipher (HKSCM) encryption mechanism is introduced, where HDFS files are encrypted by using AES and OTP algorithms. According to the implementation results it is found that the performance of Encryption/Decryption file using our HKSCM mechanism has been improved by 50% from the Hybrid encryption mechanism.

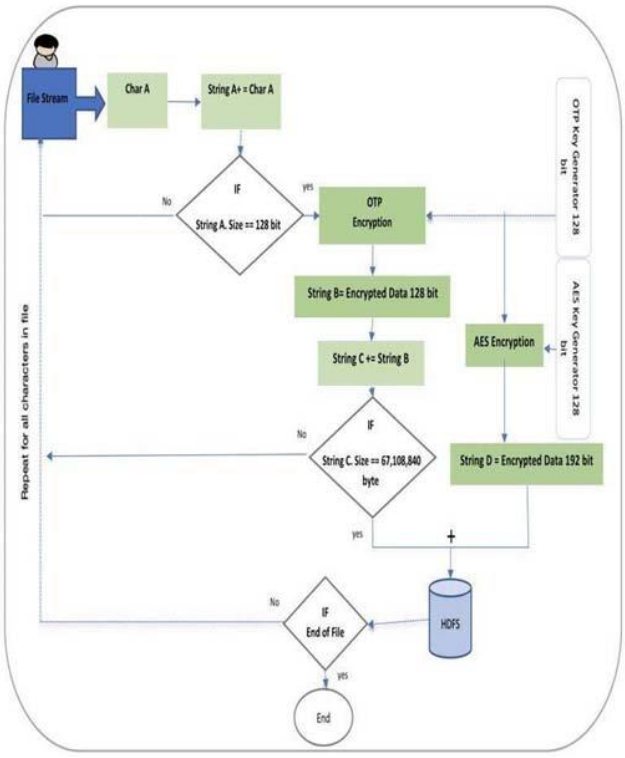

Fig. HKSCM Encryption Process

Lavanya B and ThamizhThendral V introduced A novel data ciphering method, uses different combination of substitutions. In this technique every single character is encode into 6 characters. To breach DSEM algorithm attackers should have the knowledge about the periodic elements and also applies to other substitutions. Attacker should know the flowers names, colors names and hexcodes used in this method. There is thousands of colors, flowers is available in the world so they will not be able to collect all those information and it will take more time.

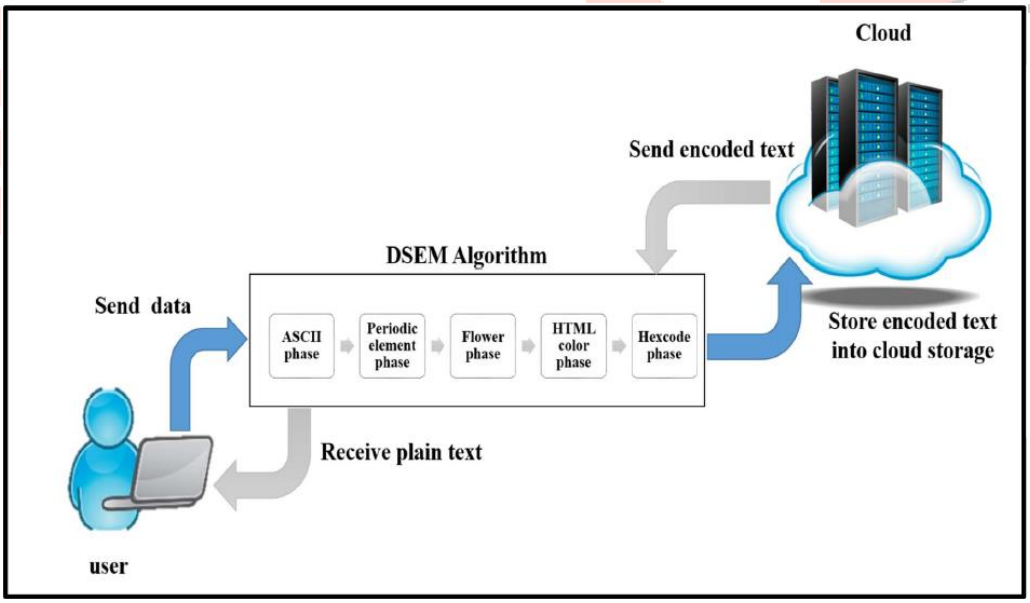

Fig. DSEM process

So hackers not easily identify which of them we have used in our encryption model then they have to find the hexcode. Hence, cracking this algorithm is impossible. The proposed method is simple to understand and easy to implement considering the above all reasons and this method provides best protection for confidential data especially for cloud data storage[11].

In the research proposed by Bhoge and Chatur [13] test the AES algorithm based on the avalanche effect. It was concluded that the ciphertext results from AES encryption were very strong. And it is difficult to decrypt to the initial plaintext. This is evidenced by testing the avalanche effect which changes 1-bit on key characters generated by encryption ciphers very different.

Nur Atikah and their team members proposed one structure, combines AES and RC4 cryptographic algorithms to get better security[14]. In this they are applying AES encryption on plaintext using AES key and creating cipher text. Again encrypting output cipher text using RC4 encryption with RC4 key and again getting secon level of cipher text. That cipher text is nothing but the final encrypted data. The combination of AES and RC4 works well. In the file size, the results of AES and RC4 encryption are relatively small. In the avalanche test, the effect of AES and RC4 managed to get a high score of 58.41% compared to other

algorithms. That means the change in the bit value on the modified key works well. And that means the combination of the AES and RC4 algorithms can improve the security of file encryption[14].

Emraida Marie M. Manucom and team introduced AES-RC4 encryption technique to improve file security[15]. Work is focused on encryption keyt for OTP algorithm. Instead of creating random key by using some existing algorithms, they tried to monitor mouse movement from user. Algorithm takes x and y coordinates from mouse movement and performs X|Y and X&Y. Then appends X&Y to X|Y and implements Fisher-Yates. This operation continues until number of random keys are equal to plain text size. And then finally performs the OPT encryption. True random number generator produces numbers which are truly random. Implementing the refining phase in TRNG with integration of Fisher-Yates shuffling algorithm increases the randomness of numbers[15].

III. CONCLUSION

In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

IV. REFERENCES

1] Nadeem, A.; Javed, M.Y. “A Performance Comparison of Data Encryption Algorithms” Information and Communication Technologies, 2005. ICICT 2005. First International Conference Publication Year: 2005, Page(s): 84–89.

2] J Thakur, N kumar. “DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”. International Journal of Emerging Technology and Advanced Engineering Website: http://www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 2, December 2011).

3] Thomas Fuhr, Eliane Jaulmes, “Fault Attacks on AES with Faulty Ciphertexts Only”, (978-0-7695-5059-6/13, DOI 10.1109/FDTC.2013.18, 2013, IEEE).

4] M. M. Shetty and D. H. Manjaiah, “Data security in Hadoop distributed file system,” Proc. IEEE Int. Conf. Emerg. Technol. Trends Comput. Commun. Electr. Eng. ICETT 2016, pp. 939–944, 2017.

5] C. Yang, W. Lin, and M. Liu, “A novel triple encryption scheme for hadoop-based cloud data security,” Proc. - 4th Int. Conf. Emerg. Intell. Data Web Technol. EIDWT 2013, pp. 437–442, 2013.

6] Bhoomika Modi and Vinitkumar Gupta, "A Novel Security Mechanism in Symmetric Cryptography Using MRGA", Springer Nature Singapore Pte Ltd. 2018, Practice, and Applications, Advances in Intelligent Systems and Computing 519, DOI 10.1007/978-981-10-3376-6_22

7] "Improved Mix Column Computation of Cryptographic AES", by Aaron Barrera, Chu-Wen Cheng, Dr. Sanjeev Kumar, ©2019 IEEE DOI 10.1109/ICDIS.2019.00042

8] H. Mahmoud, A. Hegazy, and M. H. Khafagy, “An approach for big data security based on Hadoop distributed file system,” Proc. 2018 Int. Conf. Innov. Trends Comput. Eng. ITCE 2018, vol. 2018–March, no. Itce, pp. 109–114, 2018.

9] Hybrid-Key Stream Cipher Mechanism for Hadoop Distributed File System Security, by Omar Helmy Khafagy, Mohamed Hasan Ibrahim, Fatma A. Omara. 2020 International Conference on Innovative Trends in Communication and Computer Engineering(ITCE 2020) 978-1-7281-4801-4/20 ©2020 IEEE

10] Venkat Krishna Pavan Kalubandi1, Yamuna M2 , Byte Encryption of a String using Periodic Table, International Journal of Computer Science and InnovationVol. 2016, no. 1, pp. 98-106 ISSN: 2458- 6528Copyright © Infinity Sciences.

11] A novel data ciphering method for secure cloud storage, by Lavanya B and ThamizhThendral V, Department of Computer science University of madras, 2019 IEEE

12] P. K. Ketan and V. Vijayarajan, “An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption,” Int. J. Comput. Appl., vol. 54, no. 12, pp. 29–36, Sep. 2012.

13] J. P. Bhoge and P. N. Chatur, “Avalanche Effect of AES Algorithm,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 3, pp. 3101–3103, 2014.

14] Nur Atikah, Mutia Rizky Ashila, Christy Atika Sari, Eko Hari Rachmawanto, "AES-RC4 Encryption Technique to Improve File Security", [IEEE 2019 Fourth International Conference on Informatics and Computing (ICIC) - Semarang, Indonesia, 2019 Fourth International Conference on Informatics and Computing (ICIC) doi:10.1109/ICIC47613.2019.8985825

15] Emraida Marie M. Manucom, Bobby D. Gerardo, Ruji P. Medina, "Analysis of Key Randomness in Improved One-Time Pad Cryptography", 978-1-7281-2458-2/19©2019 IEEE