IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Hybrid and Advanced Data Encryption Mechanism

[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: Big Data is a term used to describe a collection of huge data that none of the traditional data management tools are able to store or process it efficiently. Big Data has been speeded rapidly in many domains such as, social networks and other information systems. There are many promising platforms to reliably process and store big data. It provides flexible and low cost services to huge data through cloud storage. One of the main challenges of big data is how to keep sensitive information private and secure. Absence of any inherent security mechanism in cloud storage increases the possibility of malicious attacks on the data processed or stored. So, data protection is considered the major problem of big data. So in this project we are introducing the Hybrid and Advanced Data Encryption Mechanism (HADEM) which will provide more security to sensitive data.

Index Terms **- Encryption, decryption, AES, OTP, RC4, cryptography, cipher, cloud, big data, bite, DES, HDFS, RSA, hybrid key, data, security, Hybrid and Advanced Data Encryption Mechanism (HADEM)**

I. INTRODUCTION

Big Data is a term used to describe a collection of huge data that none of the traditional data management tools are able to store or process it efficiently. Big Data has been speeded rapidly in many domains such as, social networks and other information systems. There are many promising platform to reliably process and store big data. It provides flexible and low cost services to huge data through cloud storage. One of the main challange of big data is how to keep sensitive information private and secure. Absence of any inherent security mechanism in cloud storage increases the possibility of malicious attacks on the data processed or stored. So, data protection is considered the major problem of big data.

Cloud computing is a technology to relocate data and applications on infrastructures dematerialized accessible virtually through the Internet. Cloud computing is just a buzzword used to repackage grid-computing and utility computing, both of which have existed for decades. Privacy and security are often cited as major obstacles to adopt cloud services, where access to data hosted in the cloud typically has a high level of security due to the authentication mechanisms. On the other hand, the virtualization of the infrastructure helps to protect the access of the data. Big data indicates that the data are become huge, so it is difficult to process and analysis the data using traditional basic data management tools or information management. Cryptographic mechanism is considered a proper solution and a basic tool to guarantee data security (i.e., confidentiality, integrity, and authentication) [8]. It concerns about using symmetrical numbers with private key and asymmetrical numbers with public key. There are some Cryptography algorithms have been existed such as block ciphers (e.g., AES, DES, 3DES, and Blowfish algorithms), and stream ciphers (e.g. Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), Rivest Cipher 6 (RC6) and One Time Pad (OTP) algorithms).

II. RELATED WORK

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. Instead of relay on any single encryption technique, they have used two best techniques i.e. 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. The encrypted data file is completed secure until the private key is unexposed. But now we are considering worst case scenario, what if private key will get exposed accidently. Anyone can be able to easily decrypt the data. Because the encrypted file is completed depend on the private key. In todays' internet world, hackers are so smart and intelligent to hack anything.

III. THE PROPOSED HYBRID AND ADVANCED DATA ENCRYPTION MECHANISM (HADEM)

We are proposing the encryption mechanism which will provide the more security to encrypted data. It is the extension to the existing system. We are creating this system by considering the worst case scenario like what if private key will get exposed? Here we are introducing "Binary complement algorithm" to encrypt OTP key. In the proposed system, we are focusing on key. The main data will encrypt by OTP only. But here we are slightly changing the encryption process of keys. In the existing, OTP key is encrypted by AES algorithm. Encrypted OTP stored in cloud storage with the encrypted main data and AES key used as a private key. In proposed system, we will encrypt OTP key using binary complement algorithm. Output cipher data will encrypt by AES and stored with main data in cloud storage. Same here also AES key will be private key.

3.1 ARCHITECTURE

System will read the file data in the chunk of 128 bit. Using generated 128 bit OTP key, every chunk will get encrypt. By following same process, whole data file will get encrypt using OTP key. This is a first part of the architecture in which we are just encrypting complete data using the OTP key. Now in second part of architecture we are going to focus on encryption of generated OTP key to provide more security. The generated 128 bit OTP key will get encrypt using the binary complement algorithm. In the upcoming topics we will see that how binary complement algorithm will get worked. After completion of OTP key encryption using binary complement algorithm, we will get a new encrypted cipher key. Then AES encryption comes in the picture. System will apply AES encryption on generated new encrypted cipher key using 128 bit AES key. As output we will get one more encrypted cipher key. Here we have applied 2 level of encryption on original OTP key. At the first we applied binary complement algorithm and then AES encryption algorithm. Please check the architecture diagram for more details.

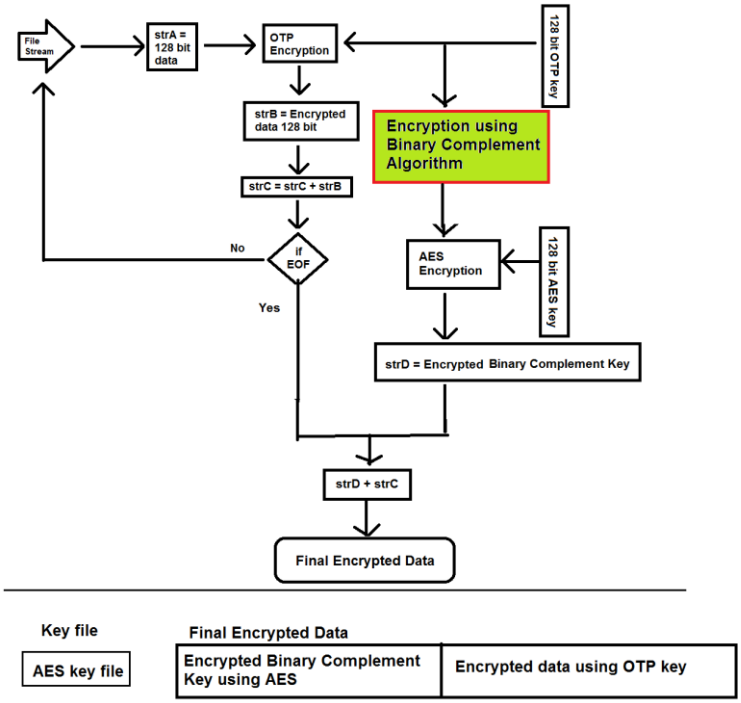


Fig 1. Architecture of Hybrid And Advanced Data Encryption Mechanism

After completion of proposed encryption mechanism, user will get two files as output. The one file will contain the final encrypted data which user can store on cloud or share with the other person. The second file will be the key file which will need to decrypt the encrypted data.

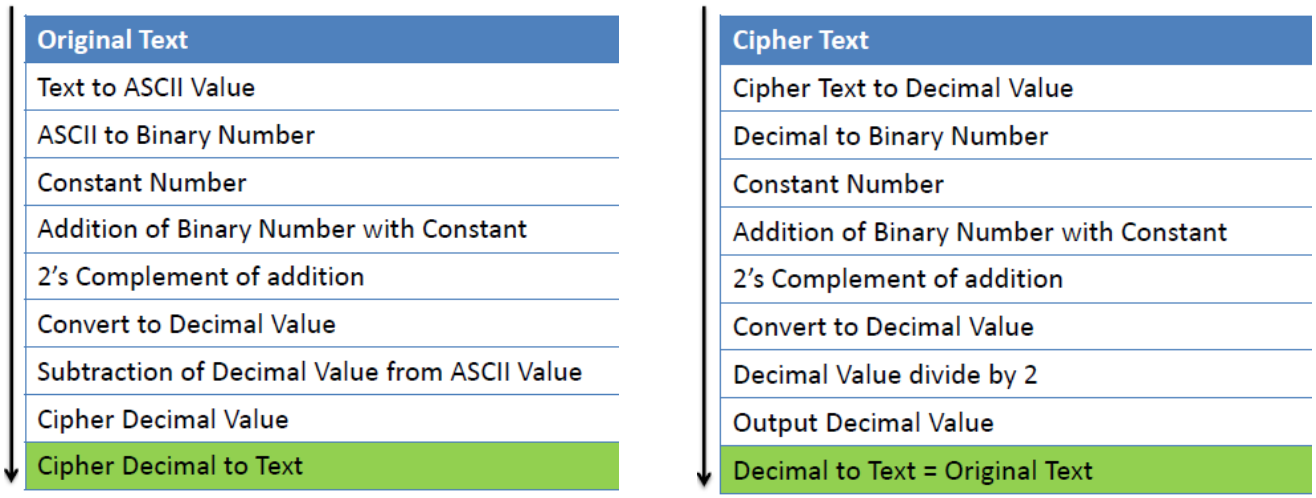
The decryption process is completely reverse of encryption. Now after encryption user have two files i.e. private key file and encrypted data file. System will read first 192 bits (CipherText1) from encrypted data file. AES description will get apply on ciphertext1 using private key file. As output user will get new key and binary complement decryption algorithm will get apply on new key. As output system will return a new key again. This key wills nothing but the original OTP key. Then system will perform OTP decryption on remaining cipher text from encrypted data file. After the completion of the whole operations, system will return the original text.

3.2 BINARY COMPLEMENT ALGORITHM

Binary complement algorithm is playing the main role in this proposed system. This algorithm is same as the other encryption algorithms. User can encrypt and decrypt own data using this algorithm. So we are using this algorithm to encrypt OTP key. The detail flow of encryption and decryption is mentioned in the given figures.

At encryption side, the original text will get convert into ASCII value. Generated ASCII value will get convert into to binary number. In the next step we will require one constant binary number. User can create or generate or consider any random binary value as a constant number. Same binary constant number will require in the decryption phase. Then algorithm will add the binary number with constant number and it will perform 2's complement on the output of addition. Then output will get converted to decimal value. Then system will perform subtraction of decimal value and the ASCII value of original text. Finally we will get the

cipher decimal value and that cipher decimal value will get convert to text. The final output text is nothing but the encrypted cipher data. Decryption process also has same kind of operations. Please check figures for more details.



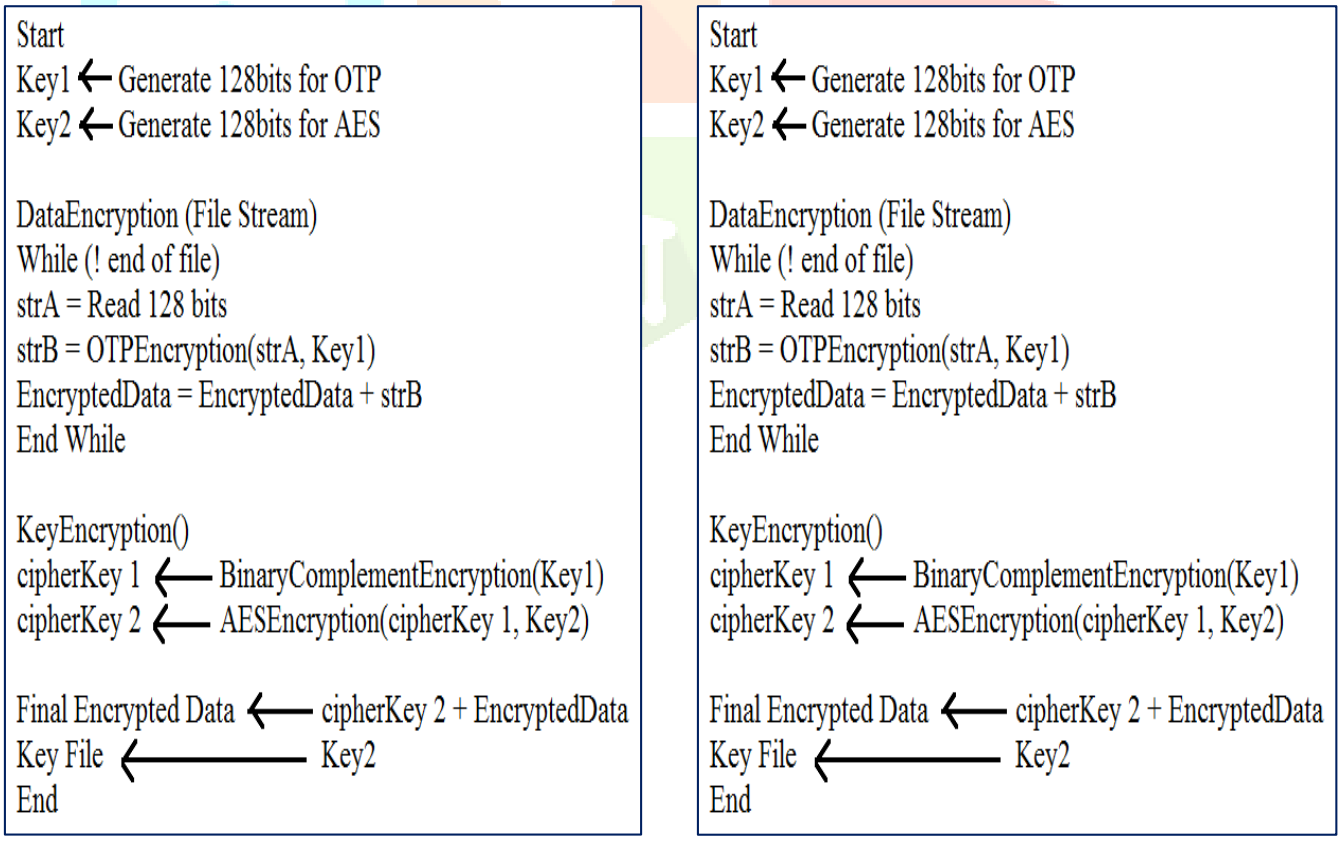
Encryption Decryption

Fig 2. Binary Complement Algorithm

The best part of binary complement algorithm is the binary constant number. This is a hidden part of this algorithm. User can consider any prime number as a constant. The same constant number will get used for encryption and decryption. Constant number creates the uniqueness in the mechanism. This uniqueness confirms that, it is very hard to decode encryption and decryption mechanism by an authorized user.

3.3 HADEM ALGORITHM

Below is the algorithm of Hybrid and Advanced Data Encryption mechanism.



Encryption Decryption

Fig 3. HADEM Algorithm

IV. THE PERFORMANCE EVALUATION

To evaluate the performance of our proposed HADEM, it has been implemented using text file with 1 Gigabyte size. We used windows 7 operating system with Intel core i5 processor, 4 GB RAM and 1 TB hard disk. We implemented the proposed solution in .Net framework. The performance of our proposed HADEM has been evaluated with respect to the execution time and file size. This has been done by a comparative study among the AES algorithm, RC4 stream cipher algorithm and our proposed HADEM algorithm.

The encryption execution times are presented in Table1.

File Size (MB)	AES algorithm (seconds)	RC4 Algorithm (seconds)	HADEM (seconds)
64	1.2077	0.8920	0.8793
128	2.0843	1.4982	1.3376
256	2.7878	2.2099	2.0049
512	8.8221	5.3652	4.9702
1024	13.8540	12.2805	11.999

Table1: Encryption Performance Comparison

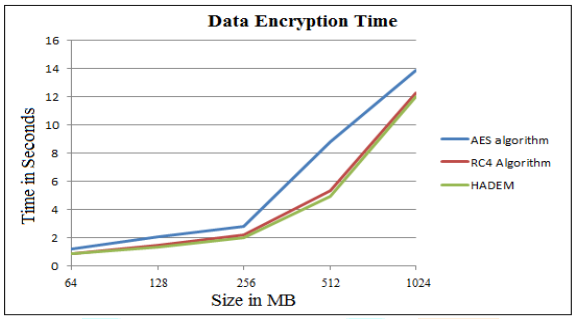


Fig 4. Encryption Performance Comparison

The execution time to encrypt the file using AES algorithm, RC4 stream cipher algorithm are 13.8540 minutes, 12.2805 minutes respectively, while our proposed HADEM algorithm execution time is only 11.999 minutes. So, our proposed Hybrid and Advanced Data Encryption Mechanism outperforms the AES algorithm and RC4 stream cipher algorithm by 14% and 3% in average respectively.

The decryption execution times are presented in Table2.

File Size (MB)	AES algorithm (seconds)	RC4 Algorithm (seconds)	HADEM (seconds)
64	0.7604	0.5347	0.5189
128	1.7214	0.9914	0.8679
256	2.6378	2.0234	1.8889
512	6.4622	3.9850	3.6981
1024	12.7654	10.4457	8.3907

Table2: Decryption Performance Comparison

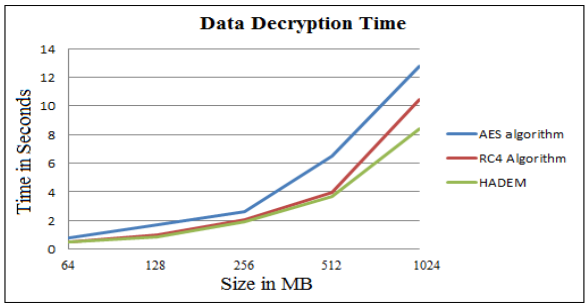


Fig 5. Decryption Performance Comparison

The execution time to decrypt the file using AES algorithm, RC4 stream cipher algorithm are 12.7654 minutes, 10.4457 minutes respectively. While our proposed HADEM algorithm execution time is only 8.3907 minutes. So, our proposed Hybrid and Advanced Data Encryption Mechanism performs better than AES algorithm and RC4 stream cipher algorithm.

V. CONCLUSION

There are many promising platforms to reliably process and store big data. It provides flexible and low cost services to huge data through cloud storage. One of the main challenges of big data is how to keep sensitive information private and secure. Absence of any inherent security mechanism in cloud storage increases the possibility of malicious attacks on the data processed or stored. So, data protection is considered the major problem of big data.

The main challenge is the security problem of the data in cloud storage is that, how to protect data from unauthorized user even if they got encrypted file with secret key. The proposed hybrid and advanced data encryption mechanism will help to achieve required security. According to the work in this paper, Advanced and Hybrid encryption mechanism introduced, where data files are encrypted by using OTP algorithms. Then OTP key encrypted using binary complement algorithm and its output encrypted using AES algorithm. So we are performing three stages encryption on private key.

REFERENCES

[1] "A New Technique for One Time Pad Security Scheme with Complement Method", Devipriya.M, Sasikala.G
[2] Omar Helmy Khafagy, Mohamed Hasan Ibrahim, Fatma A. Omara, Hybrid-Key Stream Cipher Mechanism for Hadoop Distributed File System Security, 2020 International Conference on Innovative Trends Communication and Computer Engineering.
[3] Aaron Barrera, Chu-Wen Cheng, Dr. Sanjeev Kumar, Improved Mix Column Computation of Cryptographic AES, 2019 2nd International Conference on Data Intelligence and Security
[4] Bhoomika Modi and Vinitkumar Gupta, A Novel Security Mechanism in Symmetric Cryptography Using MRGA, Springer Nature Singapore Pte Ltd. 2018
[5] Song, Youngho, Young-Sung Shin, Miyoung Jang, and Jae-Woo Chang, Design and Implementation of HDFS Data Encryption Scheme using ARIA Algorithm on Hadoop
[6] Mike Rosulek. Creative Commons BY-NC-SA 4.0, One-Time Pad Kerckhoffs' Principle
[7] Prabhudesai Keval Ketan, Vijayarajan V., An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption
[8] Avdonin Ivan, Budko Marina, Budko Mikhail, Grozov Vladimir, Guirik Alexei, A Method of Creating Perfectly Secure Data Transmission Channel between Unmanned Aerial Vehicle and Ground Control Station Based on One- Time Pads, ©2017 IEEE
[9] Otto Kugler, One Time Pad Encryption The unbreakable encryption method
[10] SHUBHAM SINHA, SAHIL GUPTA, AMIT KUMAR, Emerging Data Security Solutions in HADOOP based Systems: Vulnerabilities and Their Countermeasures, 2019 International Conference on Computing
[11] Nur Hayati, Muhammad Suryanegara, Kalamullah Ramli, Yohan Suryanto, Potential Development of AES 128-bit Key Generation for LoRaWAN Security, 2019 2nd International Conference on Communication Engineering and Technology
[12] Felix B¨usching and Lars Wolf, The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink, FEBRUARY 2015
[13] Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun, Chittaranjan Pradhan, Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain
[14] Chandra Prakash Oewanganl,Shashikant Agrawal, Akash Kumar Mandae, Mrs. Archana Tiwari, Study of Avalanche Effect in AES Using Binary Codes,2012 IEEE International Conference