International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Innovative Synthesis Cryptic Technique for Distributed Cloud Computing

B. Lavanya, V.ThamizhThendral

Abstract: ***The initial time period of computer science development, technologies were only used for military and government information communication and cryptography were used only to protect the military's high official communications. Then the continuous evolution of computer technology changes the modern era to a computer dependent transmission and storage of confidential data. And today on demand technology is the cloud computing and it is providing the computing services including servers, storage, databases, networks, software and so on. But cloud main disadvantage is a security issue because the cloud provides the computing amenities by the third-party services so third parties also can easily access the user data and it deals with more confidentiality related problems. So to protect the cloud data we propose the Deep Substitution and Advanced Encryption (DSAE) technique. Encryption converts the plaintext into unintelligible text and the proposed system is a combination of AES (Advanced Encryption Standard) and DSEM (Deep Substitution Encryption Method) algorithms. The DSAE algorithm splits the user data into two parts and one half is send to AES and other half is send to DSEM algorithm for secure the data and store into cloud storage. This paper comprehensively explain the DSAE cryptic process.***

Index Terms: ***Encryption, cloud computing, cryptography, hybrid encipher, AES, cloud security***

I. INTRODUCTION

A Distributed system is composed of several nodes connected through network and intact as a single network. Distributed computing divides a single task into many numbers of tasks then distributed to different systems for performing its operations. The fame of internet among the people, IT industries, organizations, and governments leads to this technology continuous development.

From cloud computing the word "cloud" is referred to "the internet" and cloud computing provides the on-demand computing resources through the internet based on pay for using the services. Through the cloud, we can access the data anywhere anytime in the globe. Cloud provides the platform as a service, software as a service and infrastructure as a service. But the main barrier of the cloud is security issues such as data breaching, Malware Injection, Abuse of cloud service, Insecure API, Denial of Service attacks, Insufficient due diligence, shared vulnerabilities and Data loss.

Manuscript published on 30 September 2019
* Correspondence Author
Dr. B. Lavanya*, Department of Computer Science, University of Madras, Chennai (Guindy), Tamilnadu, India.
Email: lavanmu@gmail.com
V. ThamizhThendral, Department of Computer Science, University of Madras, Chennai (Guindy), Tamilnadu, India.
Email: tamilz2015@gmail.com

So to prevent from the security issues and protect cloud data we proposed the new hybrid encryption algorithm that is Deep Substitution and Advanced Encryption algorithm (DSAE). DSAE encrypts and decrypt the data using AES (Advanced Encryption Standard) and Deep Substitution Encryption Method (DSEM).

This paper elaborately explains about the DSAE encryption and decryption process.

II. RESEARCH PROBLEM AND SOLUTION

The research problem of the paper is distributed cloud computing security issues. Cloud computing security and privacy issue is an ever-evolving problem. The main attack is Malware and it causes the data theft, account compromise, and more unauthorized network access. And using malicious software to attack the user systems and steal their private data and so on. So Google provides Google's safe browsing technology to inspect the URLs to detect unsafe website and also there a lot of website scanners, antivirus engines to detect the malware contents [1]. But hackers or attackers break these blockages and break into the user account to steal the data, so we should give the best solution to the problem for cloud data storage protection. To overcome these difficulties, we proposed an algorithm called Deep Substitution and Advanced Encryption algorithm.

III. LITERATURE SURVEY

Ghada Farouk Elkabbany and Mohamed Rasslan, stated the security issues in distributed computing system models, explained about distributed system and computing then its types in detail manner. Some security issues are Confidentiality, Data integrity, Authentication, Authorization and Access control, Non-Repudiation and Accountability. And they mentioned security attacks of distributed system such as Distributed Denial of Service (DDoS) Attack, Identity Attack in Distributed System and etc., [2]. Mohamed Firdhous performed a comparison study about the security implementation in the distributed system. Explained the security implementations of the distributed systems and defined about the cluster computing, Grid computing, distributed storage system, and distributed database. Finally, existed proposed security solutions are compared together and summarized [3]. Manoj Kumar and Nikhil Agrawal analyzed the different security issues and attacks of the distributed system. Authors mainly focused on three securities issues in the distributed system and that security issues concerns about the Security of Information, Physical security in distributed system and Security of network and authentication policy.

And describe the few methodologies to solve the issue presents in the distributed system [4]. Bih-Hwang Lee, Ervin Kusuma Dewi and Muhammad Farid Wajdi are provided the data protection using AES-128 for HEROKU cloud. HEROKU is a cloud platform and offer the platform as a service and support a few programming languages [5].

Eng. Hashem H. Ramadan and Moussa Adamou Djamilou are using AES and RSA algorithms for file encryption and store into clouds storage. First, using AES to encrypt the data and then encode by the RSA algorithm. Decryption also performing same as the encryption technique [6]. Babitha.M.P and K.R. Remesh Babu authors have proposed the mechanism for encoded the data using AES128 and store into the cloud. Using SMS (Short Message Service) to alert the users when unauthorized person tried to access the data [7]. ManreetSohal and Sandeep Sharma are proposed the BDNA- A DNA symmetric key cryptography technique to defend the cloud computing. To encipher the user files using BDNA. The BDNA ideas were created from DNA cryptography. The proposed framework first ask the user for secret key and use that key for cipher then store into cloud storage [8]. K.Arul Jothy, K.Sivakumar and M J Delsey are using AES to encode the text after sending to PGP (Pretty Good Privacy) algorithm and finally, the encrypted text is stored into multicloud [9]. Abha Sachdev and Mohit Bhansali authors ensure the data protection using Advanced Encryption Standard for encrypting the data after that load into the cloud [10]. Rajput Snehal and Prof. J S Dhobi are provided the data security in cloud computing using AES method. Two enterprises having their own private cloud and they securely share a file by using AES. [11]

IV. SECURITY ALGORITHMS USED IN DSAE

A. AES algorithm

AES expansion is the Advanced Encryption Standard. AES is developed by Vincent Rijmen and John Daemen [12]. AES is a symmetric block cipher and its process the data blocks of 128 bits and using cipher key lengths are 128, 192, and 256 bits [13]. AES ciphering number of rounds are 10, 12 or 14 and the number of rounds is decided based on the key length of AES algorithm [12]. Encoding and decoding procedure as follows:

Sub-bytes operation and inverse operation:

- In Sub-byte step, each byte in the state array was replaced by another byte using 8-bit S-box. S-box contains values are derived from the multiplicative inverse over $GF(2^8)$. Inverse sub-byte is performed in the reverse order of sub-byte operation. [14]
- *Shift row and* inverse *shift row step:* In shift row transformation, cyclically shifted the bytes in the state rows right to left except the first row and in the inverse operation, cyclically shifted left to right. [14]
- *Mix Columns and* inverse *Mix column transformation:* Combined the four bytes of each column in the state using linear transformation and in the inverse operation processed in the inverse order. [14]
- *Add round key:* Using bitwise XOR operation to add a round key with State. [14]

In the Decipher function, decrypt order is inverse shift row, inverse sub byte, add round key and inverse mix column.

B. Reason of AES choice

AES is strongly recommended by NIST for using to protect the data and it is still using by many organizations and IT industries among that some top companies are Google, IBM, and Microsoft Azure and so forth. AES is the very strongest algorithm compared to others. So, we use the AES encryption technique in our proposed algorithm.

C. DSEM algorithms

DSEM abbreviation is the Deep Substitution Encryption Method. In this method, we encipher the text using repeated substitution process, so we named it as "Deep Substitution Encryption Method". It is a bit–by-bit stream algorithm. DSEM perform the five substitution phases like the first phase is ASCII code substitution phase, second is Periodic element substitution phase, third is Flower name substitution phase, fourth is HTML color name substitution phase and the fifth phase is color hexcode substitution phase. The DSEM uses the same key for encryption and decryption.[15]

DSEM key generation: Initially, the key value is fixed as the ASCII value of given user plaint text. Then we add that key value with increment variable so each and every time we get different key value and there is no repetition will occur for the same letter. To get the inverse key value we subtract the increment variable from the key value.[15]

Deep* Substitution *Encryption Method:

- ASCII code substitution *phase:* Initially we get the given user plaintext and convert it as ASCII value.[15]
- Periodic *element substitution phase:* Using key value to get the periodic element from the substitution table then we substitute the element in the place of corresponding its ASCII values.[15]
- Flower *name* substitution *phase:* Based on key value we retrieve the flower name then we replace periodic element as flower name.[15]
- *HTML color* name *substitution phase:* In this phase, use the key to get the HTML color name from the substitution table then we swap the flower name as HTML color name.[15]
- *Color* hexcode substitution *phase:* This substitution phase is to replace the color name to its corresponding hexcode value using key value.[15]

Finally, the text is encrypted as Hexcode. Each and every letter in the plain text is cryptic into six letters. So to break the encryption is difficult for hackers. The same way as encryption we perform the decryption in the reverse order using key value.[15]

Deep Substitution Encryption Method using different substitution process these substitutions are not used in the encoding process and periodic elements are used very rarely in the cipher algorithms. So to break this algorithm is very difficult for the attackers. And it maintains the strong protection for the user data.[15]

V. PROPOSED METHOD

The Proposed work is Deep Substitution and Advanced Encryption algorithm and simply referred to as "DSAE".

Deep Substitution and Advanced Encryption algorithm is synthesis encryption technique that means mixed up of two algorithms called AES (Advanced Encryption Standard) and our algorithm called Deep Substitution Encryption Method. From DSAE the word "Deep Substitution" derived from the Deep Substitution Encryption Method and "Advanced Encryption" originated from the AES algorithm. The proposed method is divides the user text into two parts and encode the data by AES and DSEM algorithms after store into cloud and the same way it will decode by the DSAE algorithm.

DSAE cryptic steps are:1) Split plain data step 2)Right half encryption/DSEM step, 3)left half encryption/AES step, and 4) Merge encrypted data step.

The deciphering process includes: 1) Split encoded data step, 2) Right half/DSEM decryption data step, 3) Left half/AES decryption and 4) Merge decrypted data step.

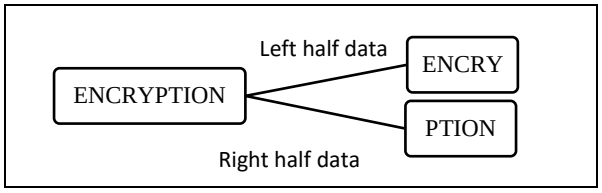
Fig. 1. Explain about the overall process of DSAE algorithms. The DSAE algorithms is explained step by step in this section.

A. DSAE encryption procedure

Initially, DSAE gets cloud user data.

- *Split original text:* Equally *divide* the given user text as Right half and Left half.

  Example: User text is ENCRYPTION. From *ENCRYPTION*, ENCRY as left half data and PTION as right half data split by first step. If cannot be divided equally like e.g. TAMIL, DSEM split the "TA" as left half and MIL as right half or "TAM" as left and "IL" as right half.



- *Right half/ DSEM encryption step:* To encode the right half data send to the Deep Substitution Encryption Method. Right half data is encoding as mentioned in section IV.

For an *example*:

For "PTION" DSEM cipher is:
['D9381E', 'EEE600', '6A0DAD', 'B768A2', 'B768A2']

The below Fig. 2 Explain the Right half encryption data flow [15].

- *Left half/AES encryption step:* To cipher, the left half text is direct to the AES algorithm. Left half data is ciphering as described in section IV.

For an example:

Left half : ENCRY
AES cipher:
[31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254].

- *Merge* cipher *data step:* In this step, we merge the split encrypted text and upload into the Cloud.

For an example:

DSAE output: [31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254, 'D9381E', 'EEE600', '6A0DAD', 'B768A2', 'B768A2']

Fig. 3 describes the encryption process of the_DSAE algorithm.

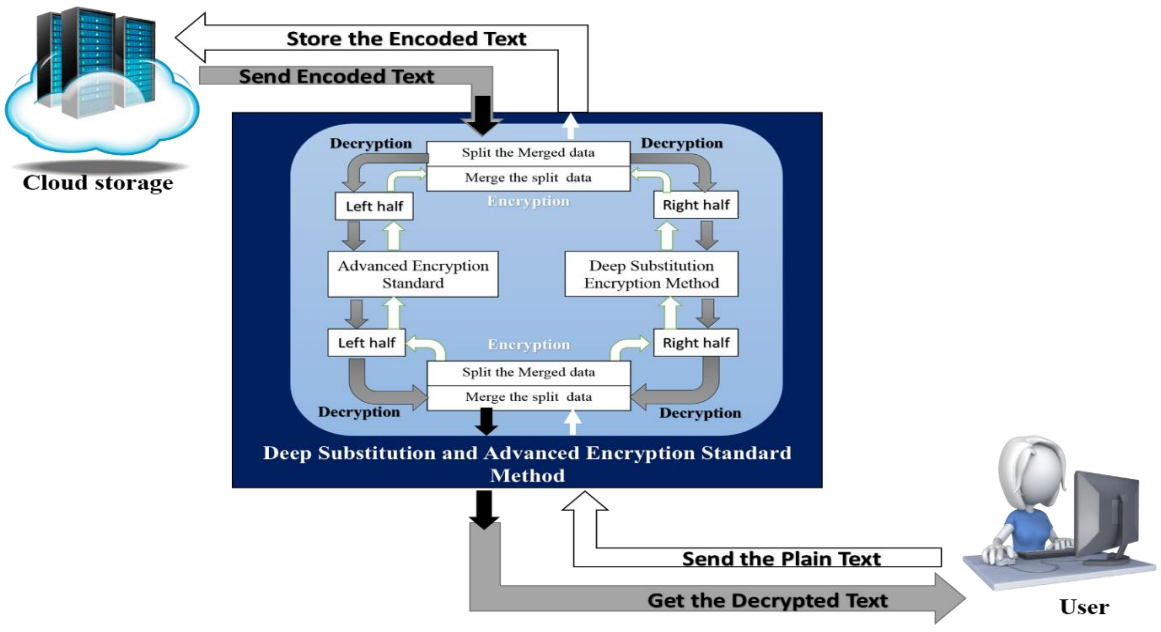


Fig. 1. Architecture of Deep Substitution and Advanced Encryption

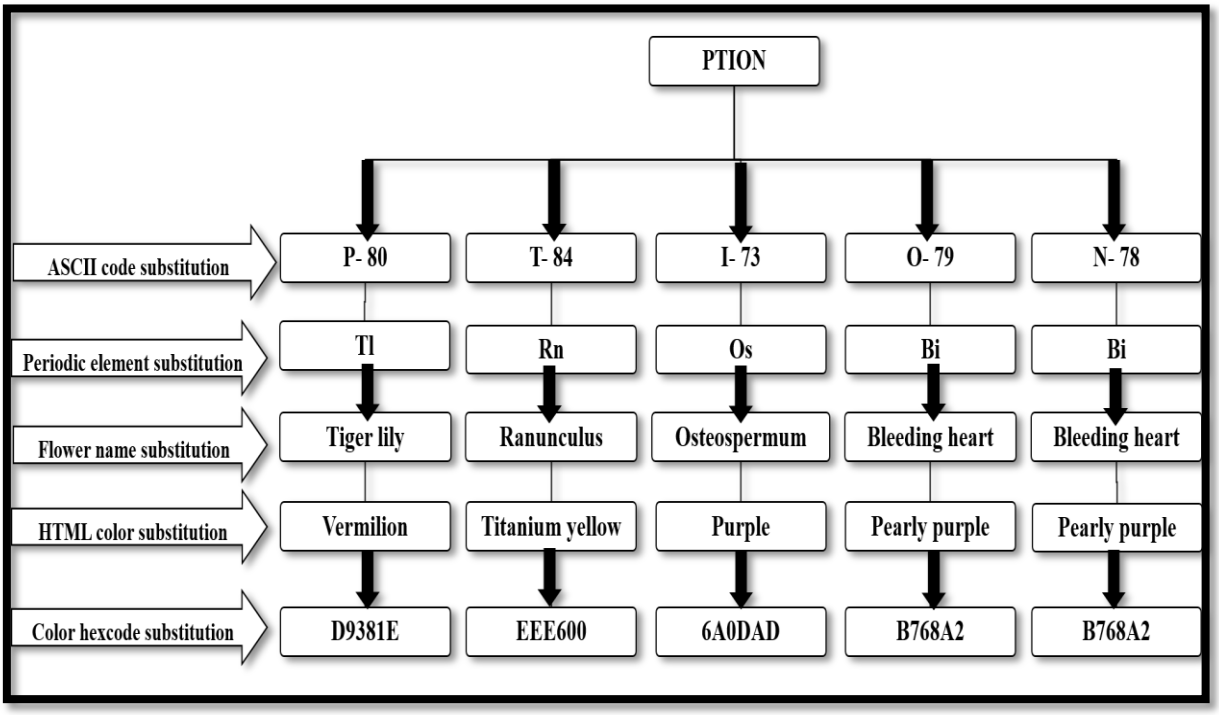


Fig. 2. Encryption process of DSEM

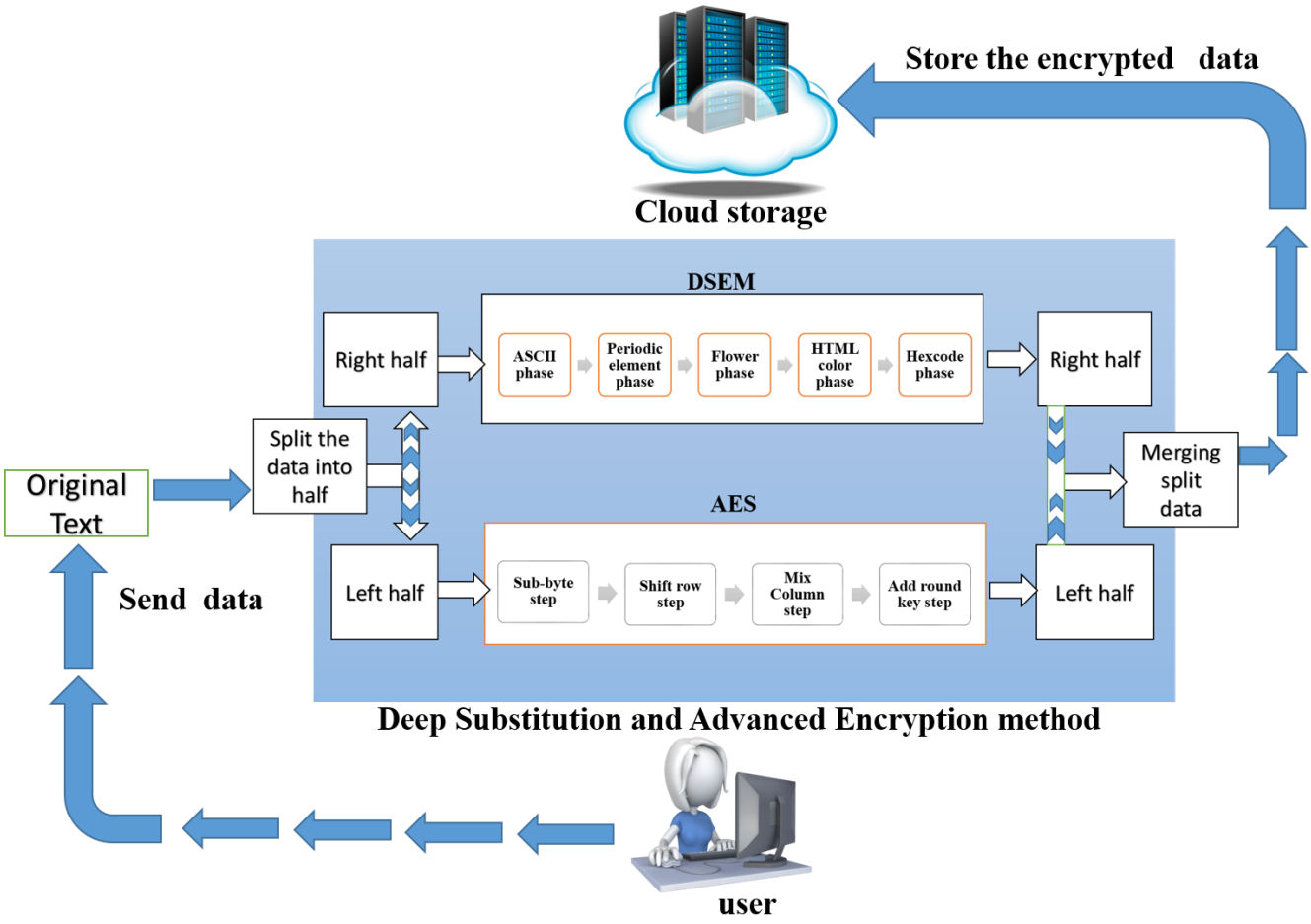


Fig. 3. DSAE encryption

B. DSAE decryption procedure

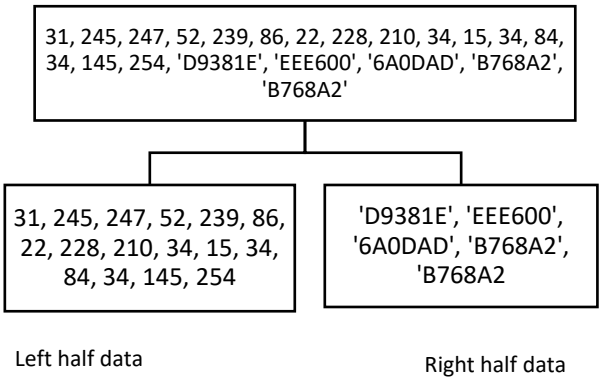
To decode the unreadable text, we follow the same procedure as the encryption process of DSAE.

- *Split decrypted Text step:* First, the encrypted text is split up as right half and left half. And the below example define the splitting process.

For an example:

DSAE encryption is: [31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254, 'D9381E', 'EEE600', '6A0DAD', 'B768A2', 'B768A2'] .

Splitting data flow:



- *Right* half/ *DSEM* decryption *step:* The right half data is sent to DSEM for decipher and decryption perform as defined in section IV.

For an example:

DSEM encoding is: ['D9381E', 'EEE600', '6A0DAD', 'B768A2','B768A2']

DSEM decoding is: *PTION*

- *Left* half/ *AES decryption step:* The left half data is sent_to AES for deciphering the text and decode as defined in section IV.

For an example:

AES encryption: [31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254].

AES decryption: ENCRY.

- *Merge deciphered data* step*:* Finally, merge the decrypted right half and left half text together and sent to the cloud user.

For an example:

Merged decoded data is ENCRYP T I O N

The below Fig. 4 illustrates the deciphering process of DSAE.

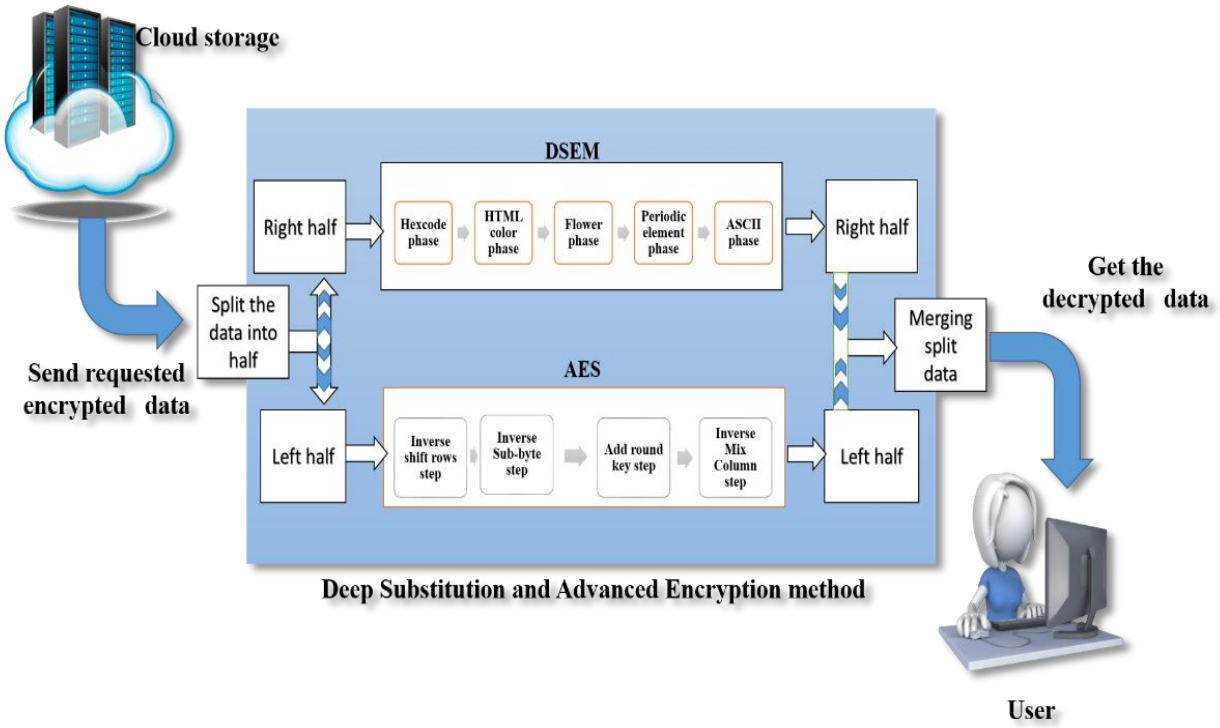


Fig. 4. DSAE decryption

VI. IMPLEMENTATION AND RESULTS

For the implementation of DSAE, we_used the python 3.7 programming language and spyder as developing environment.

A. Performance analysis

Compared to existed encryptions a minimal amount of time only is needed to deploy the DSAE algorithm. Here, for an example we take 118 data size for minimum and maximum 468 data size to analyze the execution time of algorithms.

Table- I: Execution time of algorithms

Algorithm names	Data size 118 (seconds)	Data size 468 (seconds)
RSA	3.868	4.053
AES	2.344	2.698
DSAE	0.048	0.137
DSEM	0.008	0.020

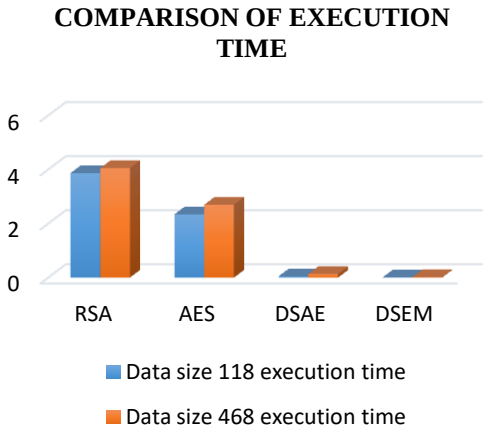


Fig. 5. Comparison of execution time

According to Table-I, Comparison analysis of execution time of encryption algorithms, our both of the algorithms consumed minimum execution time compared to existing algorithms. So, based on the performance evaluation DSAE is faster than already existing encoding algorithms. Figure 5 shows the variance of performance evaluation time.

B. DSAE encryption pseudo code

DSAE encryption Algorithm

Input: A, A is plain text $A=a_{1,}a_{2,\ldots,}a_{n-1}$,

K K is key value

Output: Z, Z is encoded text.

Algorithm: DSAE enc ()

Begin

A=get input()

Split() //first step

Split the A into two half

Rtext= right half of A

Ltext=left half of A

DSEMenc() // second step

AESenc() // third step

Mergetext() //final step

End

Function: DSEMenc()

R= get the Rtext

ASC= convert the Rtext into ASCII code // First step

Keygen() //

Key= ASC

Initially I is 0 // increment variable

K= add I with Key

Return K

Pbox()// substitute the periodic elements using key

Fbox() // substitute the flower names using key

HTMLcolor() // substitute the HTML color name using key

Hexcode() // use the key to apply the Hexcode values

R= cipher R

Return R

Function: AESenc()

L=get the Ltext

Key gen() // to generate the key

Expand key() // expand the key if it is not in key size

Sub-byte() // performing byte by byte substitution

Shif row() // performing cyclic shift row

Mixcolumn() // process the mix column

Addround() // add the round key with L

L= AES enciphered L

Return L

Function: Mergetext()

Z=merge the R and L

Return Z

Plain text: ENCRYPTION

DSAE Encrypted text:

[31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254, 'D9381E', 'EEE600', '6A0DAD', 'B768A2', 'B768A2']

C. DSAE decryption pseudo code

DSAE decryption Algorithm

Input: Z, Z is encoded text.
K, K is key value
Output: A, A is plaintext.
Algorithm: DSAEdec()
Begin
Z=get input()
Splitdectext() // split the encipher text into 2 half
Split the Z into two half
Rtext= right half of A
Ltext=left half of A
DSEMdec()
AESdec()
Mergedectext()
End
Function: DSEMenc()
R= get the encrypted Rtext
InverseKeygen() //process the inverse key generation
Key= get the index of R
Initially I is 0 // increment variable
K= subtract I with Key
Return K
invHTMLcolor() //decipher hexcode as HTML color name
invFbox() // decrypt the HTML color name as Flower name using key
Pe= invPbox() // retrieve the periodic element
Asc=get the ASCII value (for I in Pe)
A = get character of (for j in Asc)
Print ("DSEM Decrypted text:" A)

R= decipher A

Return R

Function: AESdec()

L=get the encrypted Ltext
inverseKey gen() // process the inverse key generation
Expand key() // expand the inverse key if it is not equal to key sizes
invShif row()// inverse shift row operation is perform
invSub-byte()// inverse sub-byte is process
invAddround() //inverse add round key perform by bitwise XOR operation
invMixcolumn() //inverse mix column operation process
L= AES deciphered L
Return L
Function: Mergetext()
A=merge the R and L
Return A

DSAE Encrypted text: [31, 245, 247, 52, 239, 86, 22, 228, 210, 34, 15, 34, 84, 34, 145, 254, 'D9381E', 'EEE600', '6A0DAD', 'B768A2', 'B768A2']

DSAE Decrypted text: ENCRYPTION

Deep substitution and Advanced Encryption algorithm result snapshot is shown in Fig. 6.

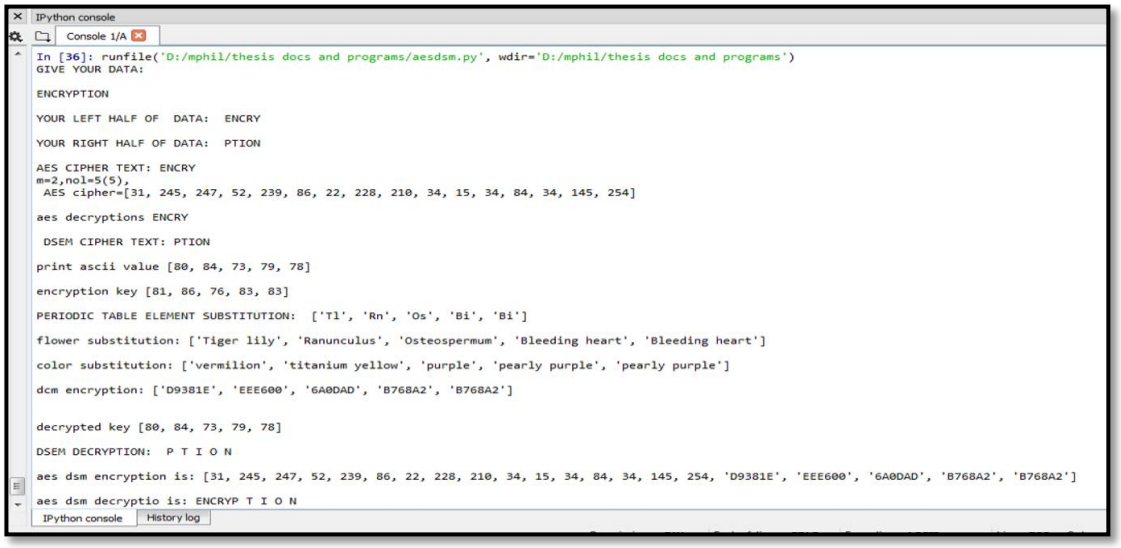


Fig. 6. Output snapshot

VII. CONCLUSION AND DISCUSSION

In DSAE, uses the AES because, as I mentioned in the section IV, AES is robust compared to other_cryptography algorithms. All AES attacks were proven theoretically only not practically. So, we have used the AES to propose the very strongest algorithm called DSAE. Based on the performance analysis section, compared to existed algorithms DSAE is fastest algorithm and the results are verified. In this concept, we split the user text then divided the data and encrypted by two different algorithms so attackers cannot break the DSAE algorithm. Although if they hack the one side of enciphered data and the other half would be near to impossible to decipher. Because the two encryptions are not related to one another and both encoding techniques uses different key. To break DSAE algorithm it takes more time to hack the user data. So practically it is not possible to crack the algorithm. And DSEM method use the unique kind of substitution techniques so attacker first they have to get the knowledge about that substitution techniques otherwise they cannot_break the DSAE method. So considering the above all reasons DSAE is the best encryption algorithm and it is also can be used to protect the confidential data likes military secrets, government top official information, and also for medical information.

VIII. FUTURE SCOPE

To improve the DSAE algorithm for the future purpose we can add more substitution and permutation process. Provide the best key generating function for DSEM. And add more rounds in AES to get stronger than now. And also we can expect this algorithm practically implement to protect the data stored in cloud.

REFERENCE

1. URL:https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf
2. El-Kabbany, Ghada & Rasslan, Mohamed. (2016). Security Issues in Distributed Computing System Models. Security Solutions for Hyper connectivity and the Internet of Things, Advances in Information Security, Privacy, and Ethics (AISPE). 36. 211-259. 10.4018/978-1-5225-0741-3.ch009.
3. Firdhous, Mohamed. (2012). Implementation of Security in Distributed Systems - A Comparative Study.
4. Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018, April). Data security in cloud computing using AES under HEROKU cloud. In 2018 27th Wireless and Optical Communication Conference (WOCC) (pp. 1-5). IEEE.
5. Kumar, Manoj, and Nikhil Agrawal. "Analysis of Different Security Issues and Attacks in Distributed System A-Review." International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013).
6. Eng. Hashem H. Ramadan. "Using Cryptography Algorithms to Secure Cloud Computing Data and Services." American Journal of Engineering Research (AJER), vol. 6, no. 10, 2017, pp. 334–337.
7. Babitha, M. P., & Babu, K. R. (2016, September). Secure cloud storage using AES encryption. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 859-864). IEEE..
8. Sohal, M., & Sharma, S. (2018). BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. Journal of King Saud University-Computer and Information Sciences.
9. Jadhav, M. S. P., & Nandwalkar, B. R. (2015). Efficient Cloud Computing with Secure Data Storage Using AES. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 377-381.
10. Sachdev, A., & Bhansali, M. (2013). Enhancing cloud computing security using AES algorithm. International Journal of Computer Applications, 67(9).
11. Rajput Snehal, and Prof. J S Dhobi. "Enhancing Data Security in Cloud Computing using AES encryption Algorithm" International Journal of Advance Research and Innovative Ideas in Education Volume 2 Issue 3 2016 Page 2894-2899.
12. Dr. B. Lavanya * V.ThamizhThendral, A Survey on Different Varied Data Communication Cryptography Methods, American International Journal of Research in Science, Technology, Engineering & Mathematic 2019, Page.63-67
13. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
14. URL: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
15. B. Lavanya, V.ThamizhThendral. "A novel data ciphering method for secure cloud storage", Accepted for publication in "The IEEE sponsored International Carnahan Conference on Security Technology", 2019 accepted

AUTHORS PROFILE

Dr. B. Lavanya working as an Assistant professor in University of Madras. Her specializations are Data mining, Big data Analytics, and Bioinformatics. She received many awards and some few awards are "B*est Researcher*" awarded on 2018, "Best Teacher" awarded on 9th month 2018, and so on. She had successfully completed 5 projects, published 2 books, and 30 research papers. She is a faculty trainer for college teachers for technical document writing and delivered numerous Invited talks. She is member of "Computer Society of India" and IEEE and served as Technical Program Committee member in conduct of many International conferences.

Ms. V. ThamizhThendral, Research Scholar in Department of Computer Science at University of Madras. Her interests include data mining and data security. She has published research papers in International Conference and journal.