Multimedia Data Security Enhancing DES & UTF8 ParameterizingTime Constraint

Ashish Sharma[1],Vikas Gupta[2]
[1]Research Scholar,[2]Associate Professor
[1,2]Department of Computer Science and Engineering, Rayat Institute of Engineering and Information Technology, Railmajra, SBS Nagar (Punjab), India
[1]ashish.sharma588@gmail.com,[2]Vikas718@yahoo.com,

***ABSTRACT*:-Internet and networking growing quickly. So it's very necessary to secure the data transmitted over different networks and servers. We mainly work through multimedia content over the internet. Multimedia content involves text, audio, video and other formats. As for now, the cloud computing is one of the most secure emerging platform which store the data in a much secure manner. But still the user must be aware about the security of the data they have been using, This paper focus on the security of the multimedia data using two enhanced algorithms namely U TF8 encoding and DES. Paper also focus on keeping the data on multiple servers rather than keeping the entire structure at one server. The evaluation of decryption is based on time to decrypt the data.**

***KEYWORDS*: Encryption scheme, UTF8, DES, multimedia security.**

1. INTRODUCTION

Cloud computing is degreerising computingparadigm where computing resources like severs, network, storage and services measurement delivered as a service over a network. In cloud computing there are a unit central remote servers that maintain different data and applications. CloudComputing depends on five attributes as multitenancy, giant quality, elasticity, pay as you go, self-provisioning of resources. Cloud Computing is providing various edgesto its users but there is a problem of security. The user information is keep inside the cloud server and thus the user desires that the knowledge keep got to be safe from unauthorized access. Third party auditor is on the brink of handle the data to and from the cloud server to the user. Any alterations inside the functioning of the third party auditor would relate to some attack by the intruder and will hurt the confidentiality of the data keep. Over this information causing and receiving from the cloud server jointly need some security measures. Many securitymeasures are developed to resist the securityproblems in cloud computing. but still many cyber-attacks had occurred on the data storage unit and on the data communicated between the user and there the cloud server. Though there is a unit many security issues in cloud computing the usage of cloud computing is increasing at a fast rate. There are different methods and algorithms are used for safely of data over the cloud and encryption is one of these. Encryption is a process changing the data in hidden form.So it's intelligible solely to someone who is aware of the way to decrypt it. . For encryption and decryption there are a unit 2 aspects: algorithmic rule and key used. Secret's like just once pad employed in vernam cipher. If same secret'sused for encryption and decryption then this can be referred to as secret key cryptography. And if completely different keys area unit used and encryption we tend to decision this public key cryptography. Secretly key cryptography single secret's used. Therefore as before distributing the information between entities the key should be transferred. Private key cryptography includes DES, AES, 3DES,Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest and UTF8 algorithms.

2. EXISTING MECHANISMS FOR SECURING CLOUD

There are several important mechanisms used to tackle with the various types of attacks over servers. Even all those mechanisms are helpful for cloud computing. The cloud computing state of affairs is principally like client-server design. John Harauz, Lori M. George Simon Kaufman and Bruce Potter describe three basic mechanisms to safeguard the information security as follows:

- A tested encryption/decryption
- Strict access control mechanisms.
- A schedule information backup theme.

B. Information security employing hybrid encryption algorithms

Hybrid encryption algorithms may be developed from combining the operating modules of two or more different encryption algorithms. Dr.R.ManickaChezian and C.bagyalakshmi [9] presents that just in case for a user to log into a system in cloud computing atmosphere as a login user one should give his/her login details at first by providing a username in plaintext kind. During this proposal, password is encryptedby the system as defined in algorithmic rule. In hybrid algorithm:

1) Password encryption by using Ceaser cipher.
2) Repeat encryption by using RSA substitution algorithmic rule.
3) Encrypt the resultant by the monoalphabetic substitution methodology. During this manner privacy to the secured cloud is provided and Developers will benefit by this method for better security. Though Blowfish algorithmic rule has been better than AES, DES and 3DES however the conclusion has been done by

throughput of algorithms. If the information size to be encrypted is increased the performance of Blow fish can sink.

C. A comprehensive approach to secure data in cloud

M. Sudha, Dr.Bandaru Rama avatar Rao and M. Monica [11] projected a information Protection Framework that secured the data confidentiality by doing authentication, info transfer by encrypting it and verification. The implementation of this framework issplit into 6 modules viz. study of system, authentication by client, key generation and encryption of data files by server, decryption of cipher text and analysis of client server interaction.

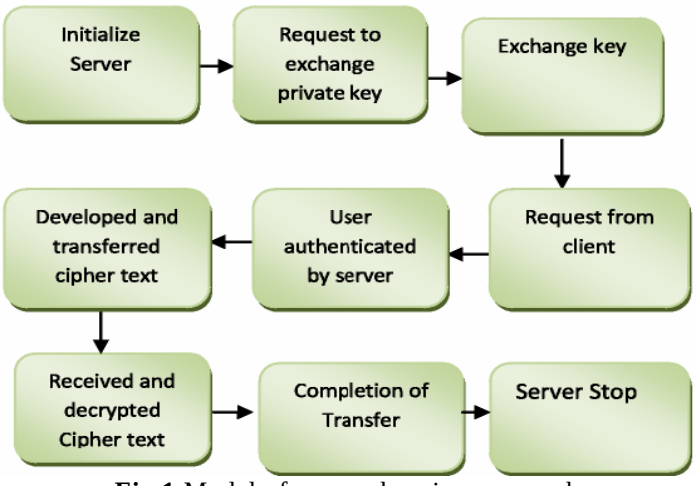


Fig 1 Model of comprehension approach

The projected system relies on client/server model. Client authentication is completed on the basis of username and password verification. Next module can give key to the client. This decrypted data is generatedby the server side using AES key generator category. As the all process of authentication is done by the client a key of 16 byte or 128 byte will be generated and provided to all of them. Then the data file required is requested by the client. Server uses AES before sending the file to the client and encrypts it. So client can receive a cipher text. The key received by the client in form of cipher text is again generated by the client by using the reverse of AES before the particular data record obtains. For easilyunderstanding the method associate analysis of the interaction between the server and client is performed in the 6th module. However, because the key generated at the server side is transferred to the client side, thus associate experience malicious act will effectively withdraw the key throughout the transfer within the network and thereby creating it inaccessible to the client.

D. Data security using RSA algorithm

ParsiKalpana and SudhaSingaraju [12] work on RSA for securing the data in cloud computing. The point with this paper is a way to secure the data and information that is at rest in cloud computing. The method is categorized into 3 steps.

A. Key generation
B. Encryption
C. Decryption

An effective cryptanalytic resolution for securing data. The key size is not outlined within the work. If a greater key size is provided then considerably the process speed of the algorithm get slow. Also, for higher key sizes it will be trouble to calculatethe value of ”e.No easy resolution to seek out this value is mentioned.

E. Data security using Elliptic Curve Cryptography.

Elliptic curve cryptography is mainly for the public key cryptosystem. VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi [10] proposed a way by implementing digital signature and cryptography with ellipticcurve cryptography. Thus authentication and encryption are the security solutions used in this system to secure information transmission from one cloud to another cloud. Elliptic curves indeed used enhancement to the diffie-hellman key exchange and digital signature algorithm.

3. METHODOLOGY:-DES:-

It uses block cipher. It encrypts the data in block size of sixty four bits every. Same algorithmic rule and key square measure used for encryption and decryption .Key is fifty six bits long. The position of 8,16,24,32,40,48,56,64 square measure discarded. DES relies on 2 basic attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting sixteen rounds. In every spherical key and data bits square measure shifted, permuted, XORed and sent through, 8 s-box. Within the initial spherical sixty four bit plaintext is handed to initial permutation (IP).Then science generates2 halves left plaintext (LPT)and right plaintext(RPT).Each LPT and RPT goes through sixteen rounds. At the last LPT and RPT square measure rejoined. Decryption is same method perform rounds in reverse order.

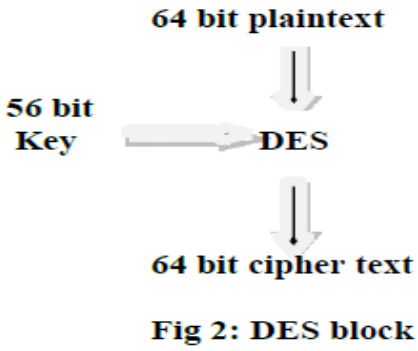


Fig 2: DES block

Fig 2: DES block

UTF8:-

UTF-8 (UCS Transformation Format²8-bit[1])is a variable-width encoding that may represent each character within the Unicode list. It absolutely was designed for backwardcompatibility with

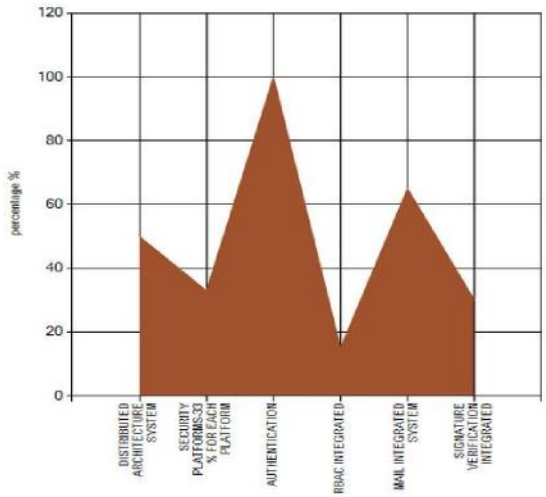
ASCII and to avoid the complications of endianness and byte order marks in UTF-16 and UTF-32. UTF-8 has become the dominant character secret writing for the WWW, accounting for over 1/2 all web pages. The web Mail Consortium (IMC) recommends that every one e-mail programs be ready to show and make mail mistreatment UTF-8.[5] UTF-8 is additionally more and more being used because the default character encoding in operative systems, programming languages, APIs, and software package applications.UTF-8 encodes every of the 1,112,064 code points within the Unicode character set using one to four eight-bit. Code points with lower numerical values area unit encoded using fewer bytes. the primary 128 characters of Unicode, that correspond matched with ASCII, are encoded using a single octet with an equivalent binary value as ASCII, making valid ASCII text valid UTF-8-encoded Unicode also.

Steps of Algorithm:-

1. Initialize K=0
2. For K=0 : length(uploaded.format)
3. If char.count.uploaded.format>0
4. Char(k)=Encoding.Des();
5. Utf8array[k]=char(k).merge.start.bit
6. Utf8arrayend[k]=char(k).merge.end.bit
7. String allcharacters[]=0;
8. For j=0:encodedbits
9. Allcharacters[j]=encoding.utf8
10. End
11. End
12. for pp=0:j
13. publish.allcharacters(pp);
14. if(allcharcters[pp]==null)
15. pp=pp+1
16. end
17. end

4. RESULT GRAPHS

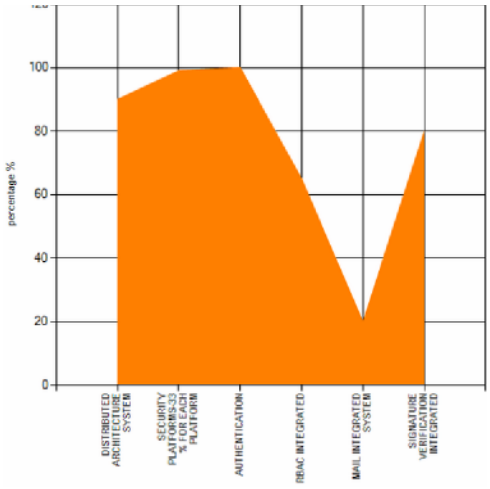
PREVIOUS APPROACH:-



Graph: 1

The above figure represents the analytical study of the different parameters like RBAC integration system ,Mail Integration System ,Distributed Architecture System and other values. Other than the mail integration system ,there are several drawbacks of the previous system.

Our Approach:-



Graph : 2

The above figure represents the analytical study of the different parameters like RBAC integration system, Mail Integration System, Distributed Architecture System and other values. Other than the mail integration system ,there are several benefits of the previous system.

Comparison between previous approach and our approach:-
We can compare our approach from different previous approaches by taking different attributes.

Distributed Architecture Scheme:- As shown in graph our Distributed Architecture scheme is better than previous one because in our approach we use three type of architecture together which are Gmail, Window Azure, and local Host for distribution of data which also beneficial for security purposes.

Security Platform:-For security platform we keep our data in different servers. If any user wants to access the data he have to access all the three servers. In previous approaches mainly one server is used for storing the data. So the security platform stands only 33% .but in our approaches its 3 time better which is 33% of window Azure, 33% of Gmail-SMTP and 33% of Local host.

Authentication:-It is same for all the approaches. Only authenticated users are allowed to access the data or enter the site.

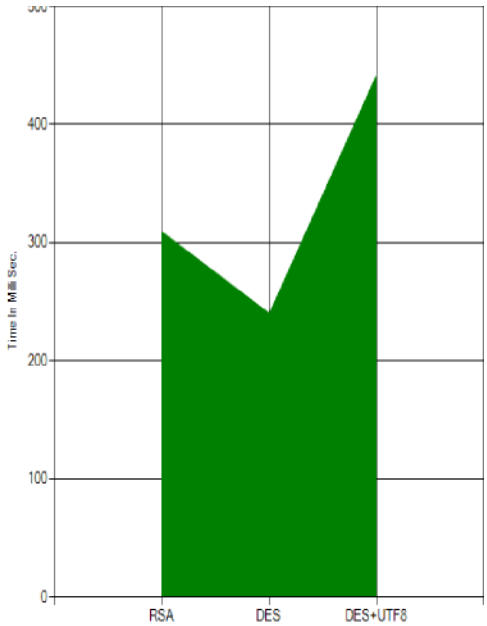
Role Based Access Control (RBAC):- In this only authenticated user can access the data. User can not download the data whichis uploading by their self. Users can notpermitted

to access other'suser's data.

Mail Integrated System:-In this our approach is weaker than previous ones. In this we only use Gmail for mail but in previous approaches many other mail system are using like yahoo, hot mail, r etc.

Digital Signature:-This is much better than previous approaches. Because we provide the facility to user upload different type of signature for security. This can be any image, audio and video file. But other approaches only provide one type of signature to users for security.

Comparisionbetween different Algorithms:-



Graph 3: representing decryption time comparison for various algorithms

The above graph shows the numerical representation of different algorithm which also includes the sophisticated approach of DES and UTF8.Using a single algorithm for the purpose of data encryption can secure the data up to some extent but it is not necessary that it would be the best algorithm which may provide the highest security. The efficiency of an encryption algorithm can be determined by the time it takes to get decrypted. It is not necessary that if we combine two algorithms, it would take more time to get decrypted. It completely depends upon the complexity of the algorithm through which it has been designed. In the graph shown above, we have provided detail about the time of decryption which an algorithm takes when a similar size of file has been provided it to be encrypted. From the graph is it quite clear that the hybrid algorithm consisting of DES & UTF8 compels more time in the decryption in comparison to alone RSA or alone DES.

Result Table:-

File Size	RSA (Av) Time in ms	DES(Av) Time in ms	UTF8+DES(Av) Time in ms	No. of iterations Time in ms
512 kb	163.40	90.04	508.30	10
1024 kb	176.40	101	501.30	10
1536 kb	149.80	88.27	547.50	10
2048 kb	164.52	102	501.80	10
2560 kb	169.40	111.90	499	10
3072 kb	165.42	107.47	485.5	10

This table shows the different decryption time for different algorithms. In this tables we take different iterations for each algorithm and then take average of all values because in our system different processes are running and it gives different value for each time .From this table we conclude that the decryption time for RSA and DES is less than UTF8 & DES because when we merge two algorithms than when any file is decrypt it have to pass through both algorithms.

5. CONCLUSTION

With the presented work, we can conclude that hybridization of two algorithms namely UTF8 encoding and DES enhances the security at the file as the time taken to decrypt the file (file size) is more in comparison to others. We also conclude that, even at cloud servers, keeping data at multipath environment is much safe as compared to the previous single path environment.

REFERENCES

[1] John Harauz, Lori M. Kaufman and on cloud services" in 2010 IEEE 3rd international conference on cloud computing.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds : A Berkeley View of Cloud Computing, 2009.

[3] NabenduChaki, "A Survey on Security issue in Cloud Computing " in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication

and Information Technology, May 2009

[4] Nils Gruschka and MeikoJensen,"Attacksurface : A taxonomy for attacks on cloud services" in 2010 IEEE 3rd international conference on cloud computing.

[5]A. Das and D. Grosu, "Combinatorial auction-based protocols for resource allocation in grids," Parallel and Distributed Processing Symposium, 2005. Proceedings.19th IEEE International, 2005.

[6]PalivelaHemant , Nitin.P.Chawande, AvinashSonule, HemantWani, Development of Server in cloud computing to solve issues related to security and backup¶, in IEEE CCIS 2011

[7] Cong.Wang and KuiRenWenjing Lou and Jin Li "Towards Publicity Auditable Secure Cloud Data Storage"

[8] J. Shneidman, C. Ng, D.C. Parkes, A. AuYoung, A.C. Snoeren, A. Vahdat, and B. Chun, "Why Markets Could (But Don't Currently) Solve Resource Allocation Problems in Systems," Challenges, 2005, p.

[9]Dr.R.ManickaChezian and C.bagyalakshmi "a survey on cloud data security Using encryption technique" in International journal of advanced research in computer engineering & technology , Volume 1, Issue 5, July 2012.

[10]VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, "Data Security i l d computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 223 1-2307, Volume 2, Issue 3, July2012.

[11]M. Sudha, Dr. Bandaru Rama Krishna Rao, M.Monica, A comprehensive approach to ensure secure data communication in cloud environment"

International Journal of Computer Application (0975-8887), Volume 12- No 8, Dec 2010.

[12]ParsiKalpana, SudhaSingaraju, "Data security in cloud computing using RSA algorithm", International Journal of research in computer and communication

technology, IJRCCT, ISSN 2278- 58,Volume 1, Issue 4, September 2012

[13]Jianyong Chen, Yang Wang, and Xiaomin Wang, "On demand security Architecture for cloud computing", 0018-9162/12, published by the IEEE Computer society in 2012

[14]Jonathan Katz,"Efficient cryptographic protocol preventing man in the middle attacks", Doctoral Dissertation submitted at Columbia university, ISBN: 0-493-50927-5,2002.

[15]Salvatore J. Stolfo, Melek Ben Salem, Angelos D. Keromytis, "Fog computing: Mitigating Insider data theft attacks in the cloud".

[16]Ferguson,N.Schnier,B and KonhoT(2010),"Cryptography engineering designprinciple and practical application"

[17]Aman Kumar, Dr.Sudesh, Jakker,Mr.SunilMaakar "Distinction betweensecret key and public key cryptographywith existing Glitches"IJEIM-0067,vol1,2012

[18]Yogesh Kumar, Rajiv Munjal, "Comparison of Symmetric and asymmetriccryptography with existing vulnerability "IJCMS-oct 2011