Enabling Public Auditing for Data Integrity Checking using Ring Signatures Developed with Aes in Cyber Security

J. Achyuth sai, K. Kiran Kumar

***Abstract:** Now a days in our day to day life online data has most importance. Everything in todays world is connected to internet and mostly communication is carried through online only in the form of gmail, twitter, whatsapp, facebook etc., So, we need this data to be stored and transferred in a secure way without any manipulation and data misuse by the hackers. So, this online data is to be properly encrypted and transferred by using proper algorithms like Advanced encryption standard (AES) algorithm in cyber security. Public auditing is used as an efficient way of checking the data integrity who can verify the metadata of the original data for errors with the request of the user. Homomorphic authenticators are used as metadata for auditing purpose.*

***Keywords:** Advanced encryption standard (AES),Data Encryption standard(DES) algorithm, Homomorphic authenticators, Metadata.*

I. INTRODUCTION

The securable data transfer from data creator to user in the form of encrypted file is done by using particular algorithms like AES (advanced encryption standard), where in previous systems DES algorithm is used for this purpose.The data integrity is one of the more important concerned things in order to transfer data without any errors. So, public auditing plays prominent role in data transfer.

Existing system:DES Algorithm

By using DES(data encryption standard algorithm) ata a time 64 bit size plain text is processed to get the cipher text.It follows the fiestel structure.Here the plain text is processed in 16 rounds with a key size of 64 bit.In each we will have separate independent key,so in total we have to generate 16 sub keys with each sub key size is 48 bit.Finally cipher text size will also be 64 bit as plain text.

Revised Manuscript Received on April 07, 2019.

J. Achyuth sai, Professor, Department, of ECM,Koneru Lakshmaiah Education Foundation

K. Kiran Kumar, Professor, Department, of ECM,Koneru Lakshmaiah Education Foundation

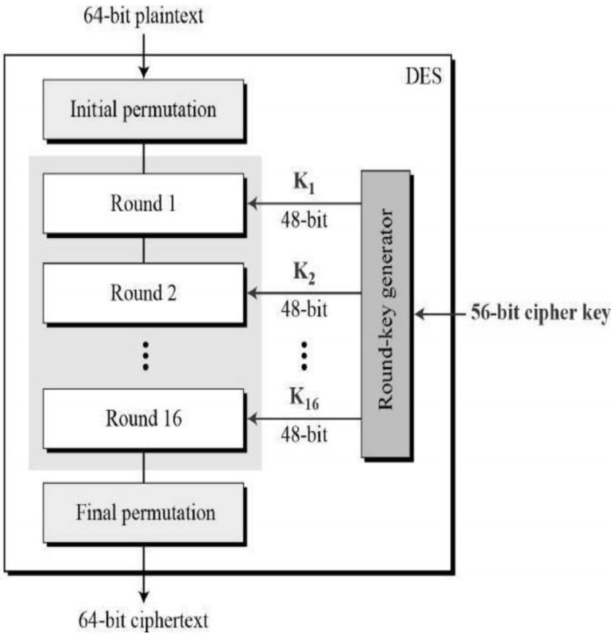


Fig 1: Block diagram of DES algorithm

Here the transposition order is called permutation, so where ever permutation concept came we will use transposition order .So here 64 bit plain text is input to intial permutation where we have to follow permutation order means we want to rearrange the bits and from this we will again get 64 bit output. This 64 bit is given to round 1,in this round we have to generate key so parallelly sub keys are generated to use in round functions. Now 64 bit key is taken and given to permutate choice 1 operation and output from this is 56 bit key. From here we have to apply left circular shift operation and from this we get again 56 bit key for this also permutate choice operation must be done to rearrange bit positions after that we will get 48 bit sub key as output and it is given to round 1.After round 1 again round 2 is applied ,as per circular shift once again left shift operation is done for round 2,for this left circular shift input will be 56 bit.The output of this shift is now applied to the permuted choice 2 where some bits are ignored and we will 48 bit sub key. This same procedure is followed up to round 16. After completion of all these rounds 32 bit swap is performed means 64 bit key is divide into two halves of left part 32 bit and right part 32 bit and both are swapped. The left 32 bit is copied to right side and right 32 bit is copied to left side. After this 32 bit swap inverse initial permutation is applied and this is also transposition order and output from this is a final “CIPHER TEXT”.

*Published By:
Blue Eyes Intelligence Engineering & Sciences Publication*

PROPOSED SYSTEM:

In this public auditing mechanism the entire data integrity can be checked by using metadata of original data. We use ring signatures for constructing homomorphic authenticators for identification of user identity on each block of data.

To avoid data manipulation very effectively we use AES algorithm for secure data transfer. Ring signatures are nothing but digital signatures of 16 byte or 128 bit size. These signatures are created by data owner in the system digitally by typing. This 16 byte key will undergo several rounds of interchanging process to get final cipher text key, here the plain text size given will always be fixed to 128 bit. The key size may vary between 128,192 and 256 bits.

ADVANTAGE:

Multiple auditing processes can be done simultanuosly and accurately data integrity can be checked by public auditing.

II. Literature survey

Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE][1] has discussed about the secure public auditing using the technique of random masking using MAC and homomorphic linear authenticators where authenticators are used for identity checking of user, but main disadvantage here is individual auditing problem which must be overcomed by AES algorithm in our discussion.

Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data of1Y. Prasanna, 2Ramesh [2]has proposed the best way of auditing by using symmetric key encryption where same cryptographic key is used for plain text encryption and cipher text decryption and here the data base is stored in remote location for secure data storage and ranking method is efficient to return high relevant documents. The only disadvantage is communication and computation costs are very high which requires homomorphism encryption on both sides of server and user.

Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud(Boyang Wang, Baochun Li and Hui Li State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada Email:{bywang,bli}@eecg.toronto.edu, lihui@mail.xidian.edu.cn) has shared the ring signatures importance means how digital signatures are prominent in efficient and secure data transfer where the identity of user on each block is kept private. But the data is confidential within group and should not be revealed to any third party.

Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud

(Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE)has implemented resigned techniques by which users can easily share and modify data with data storage and sharing services as a group. But due to security reasons once the user is revoked from the group, the blocks that are signed previously by this revoked user must be resigned by existing user

Remote Data Checking for Network Coding-based Distributed Storage Systems(Bo Chen, Reza Curtmola Department of Computer Science New Jersey Institute of Technology {bc47,crix}@njit.edu, Giuseppe Ateniese, Randal Burns Department of Computer Science Johns Hopkins University {ateniese, randal}@cs.jhu.edu) has given the remote data checking technique by which data is checked and stored remotely and this is less expensive .

III. SYSTEM ARCHITECTURE

Admin: Group admin actually assembles the data owner ,auditor and user as a group for secure data transfer.

Data owner: According to the requirements of the user data owner creates the data along with 16 byte key and that key is send to authorized user of data for security purpose through mail using SMTP protocol. This data is encrypted with a 16 byte key that can be send to cloud server.

Auditor: The auditor here can only able to fetch the meta data means homomorphic authenticators to check the data integrity. After receiving the request from user to check and send the particular block of data to him, the auditor sends the request to the data owner to provide metadata of particular block and auditor checks the meta datas of both the user and data owner .If the meta data is same then he sends the data requested by user

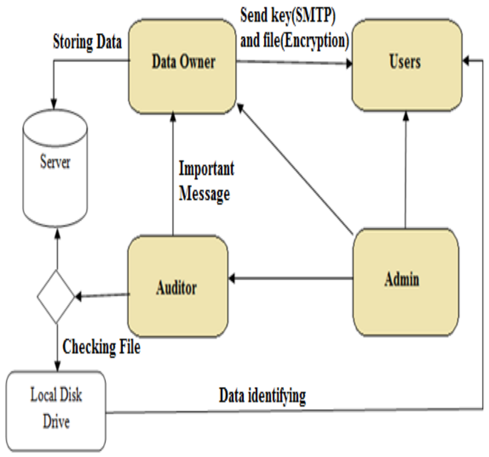


Fig 2: System architecture

User: User will receive the data from the auditor in the form of a code encrypted and user decrypts the data with the key he is having.

HARDWARE AND SOFTWARE REQUIREMENTS:

Software Requirement:

Java (JDK 1.7), MySql Server and NetBeans IDE 7.1.2

Hardware Requirement :

1 GB RAM,80GB of hard disk, data card and 2GHz Processor.

Registration of User:

The data owner randomly selects a number to give identity number for user and stores it in group user list .The private key is generated by data owner after that the key is given to user.

Public Auditing:

In public auditing homomorphic authenticators plays prominent role as a meta data. These are unforgeable metadata generated from separate blocks created by AES algorithm.

3. Data Sharing:

Data sharing can be efficiently done by data owner by using small keys generated by him. This key is distributed to each and every authorized user for data decrypting.

4. Integrity Checking:

In this integrity check the auditor can only download the metadata file but not the entire file.The auditor may also manipulate the data so this technique is useful from avoiding any type of data manipulation.

IV. ALGORITHM

Advanced Encryption Standard (AES):

AES algorithm always follows the structure of substitution permutation network, where data key is divided into substitution boxes and rearranging of bits is done in permutation box. AES uses 10 round keys depending on the master key size for 128 it will be 10 rounds,12 rounds for 192 bit key and 14 rounds for 256 bit key.

AES Algorithm Block Diagram:

First of all the plain text is divided into blocks and at a time each block is processed. Here block size is 128 bit of plain text and in AES algorithm the plain text is processed in 10 rounds .In each round a separate sub key is used to get the final cipher text. The size of master key means the key used at the starting is also of 128 bit size and this key is processed in terms of words, here one word is of 32 bit size. So ,128 bit master key is processed in terms of four words or 16 bytes. The number of subkeys we are using here is 44 subkeys. Each subkey size is 32 bit or 1 word or 4 bytes. In each round we are going to use 4 subkeys, that means 128 bit(32 *4)/4 words/16 bytes. Before starting the round in pre round calculation we are using 4 subkeys and in 10 rounds 10*4 = 40 subkeys is used plus 4 subkeys at starting to generate “CIPHER TEXT”.

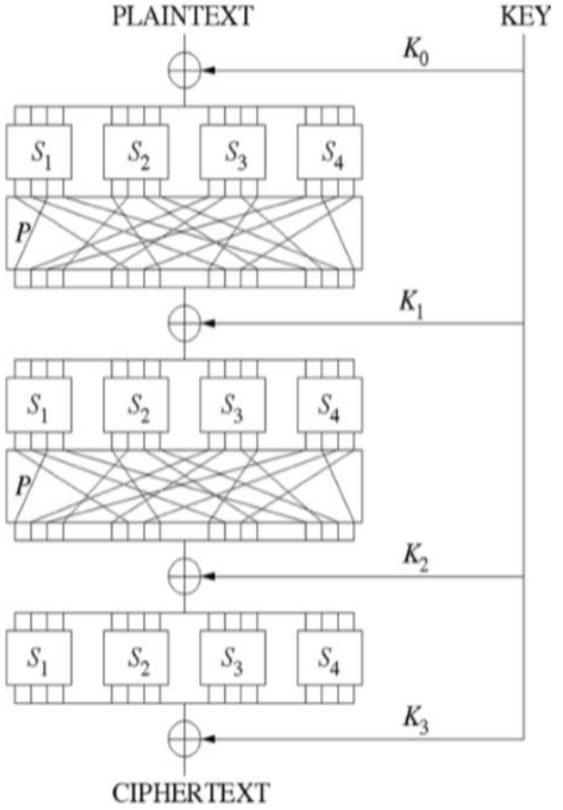


Fig 3 : AES BLOCK DIAGRAM

AES ALGORITHM PROCEDURE FLOW:

First of all consider the plain text which is 128 bit, and this is applied to “ADD ROUND KEY” by XOR operation. Here we will use 4 words that means one key represented as “round key 1” .After this operation we are going to apply substitute bytes and these are called “S boxes” in aes algorithm. Here in s box the input is 128 bit and output is also 128 bit.After the S box we need to apply “shift rows” operation. Here ,shift rows means applying the circular right shift operation. After this we need to apply “mix columns” operation. Here we have to multiply with a pre defined matrix of 4*4 .we have to consider one word and that is multiplied with this matrix. In all these three operations the input and output will be of 128 bit only. The output from mix columns is given to “ADD ROUND KEY” operation where we have to use “Round key 2”.This whole process of four operations is a “ROUND ONE”. So, we have to repeat the same process for 10 rounds in each we have to use separate sub key. Each sub key is of 1 word so in total after 10 rounds we will have 44 subkeys or 44 words to be used to get final cipher text from the given plain text. In last round mix columns is not used .

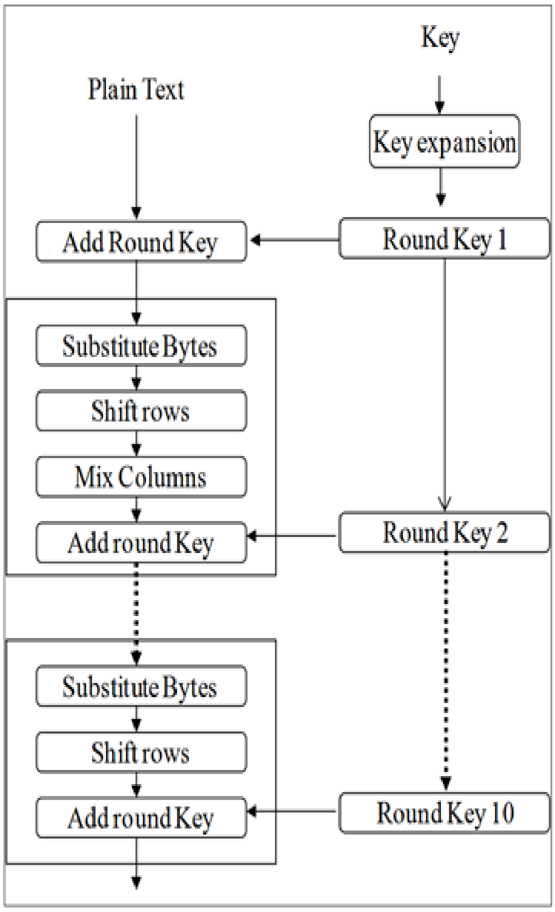
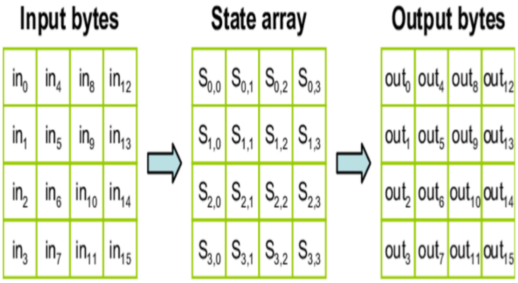


Fig 4: AES ALGORITHM FLOW

AES ARRAYS:

Here the 128 bit plain text is stored in input arrays and these input arrays is represented in 4*4 table. Each and every block is represented as 1 byte so in total we have 16 bytes or 128 bits. Here, intermediate results are stored in state array. Here, this state array is also 4*4 that means 16 bytes or 128 bit. Similarly , the output is stored in output array which is also 4*4 that means 16byte or 128 bit size. Here, each and every column is considered as a word that means we have four words in total. S(0,0) represents zeroth byte of zeroth word. S(1,0) represents first byte of zeroth word and so on. S(0,1) represents zeroth byte of first word. S(1,1) represents first byte of first word and so on.



in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

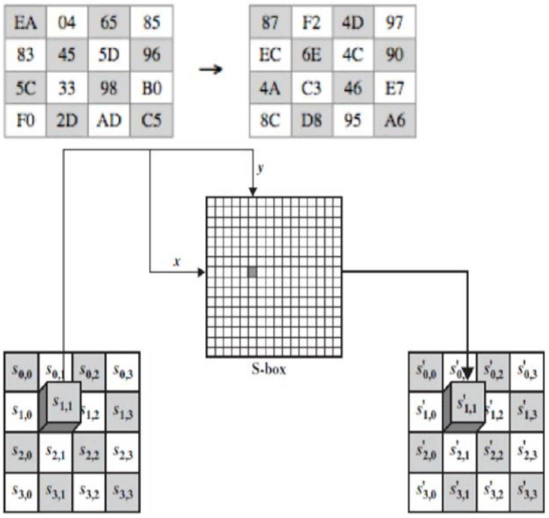
out_0	out_4	out_8	out_{12}
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

Fig 5 : AES ARRAYS

Similarly, a key is also of 128 bit and the key is stored as 4*4 table, from this 128 bit or 4 words we have to generate 44 words. So from this we will expand the key as W0,W1,W2------W43 that means 44 words.

SUBSTITUTION BYTES:

Here , the substitution bytes is nothing but implementation of S box. The input of S box is first 8 bits and in this first 4 bits is considered as row number and the next 4 bits represents the column number. Here the numbers 0 to 15 is represented for first 4 bits and also for next 4 bits and 15 is represented as F. The output is also 8 bits for S box and this 8 bits is again stored in state array. Here the size of S box is 16*16 table.



EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

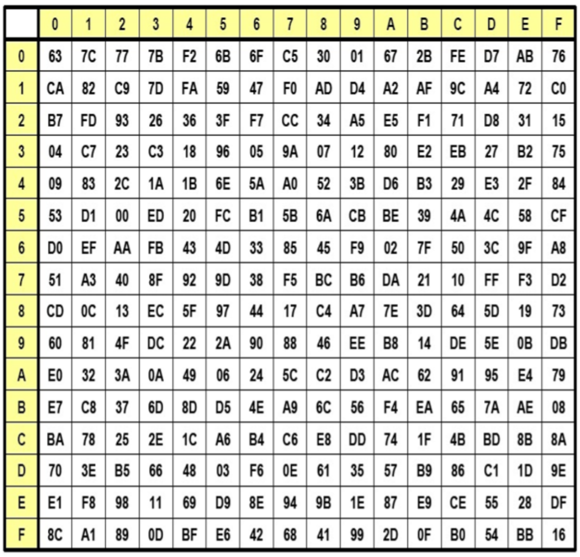
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Fig 6 : SUBSTITUTION BYTES

S BOX IN AES ALGORITHM:

In this S box of 16*16, if we consider as an Example : Let 0000 0101 be the input and here first four 0000 represent row and 0101 represents column of number.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig 7 : S BOX in AES

So row number is 0 and column number is 5, that means we have to get the value from 0th row and 5th column. In S box 0th row and 5th column represents 52. So,the result is 52 which is again converted to binary 0101 0010 and this is output from S box. This output will be stored in state array.

SHIFT ROWS :

As shown in the below diagram ,the first box represents the state array input for S box and the output is stored in another state array that means second box.

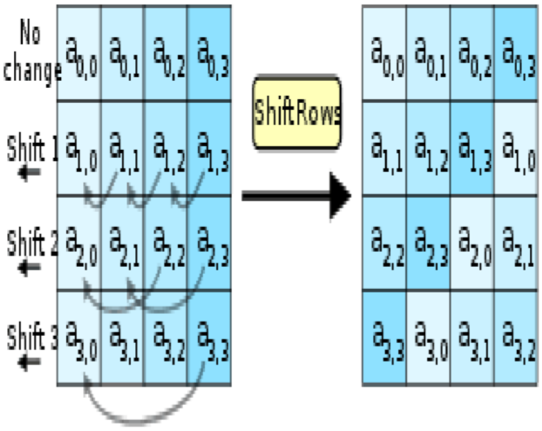


Fig 8: SHIFT ROWS

In shift rows depending upon the row number we have to shift the rows.If it is row 0 we have to shift the zero bits using circular right shift. If it is row one then one bit is shifted and for row 2 ,2 bit will be shifted and so on as shown in the above figure. The result is also stored in state arrays.

MIX COLUMNS:

The output from shifting rows resultant state array is considered as input to the mix columns. Consider each column as one word and take one word and apply multiplication operation with pre defined 4*4 matrix and we get again one word which is again stored in state array. As shown in the below diagram the input column is taken and multiplied with 4*4 matrix to get output state array. Here the output will be 4*1 column because by multiplying 4*4 matrix with 4*1 column we get 4*1 matrix and that result is stored in state array. This column output is of one word. Like this we will get four columns as output stored in state array.

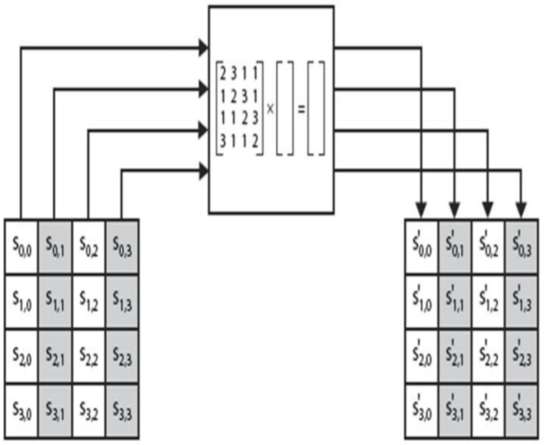


Fig 9: MIX COLUMNS

ADD ROUND KEY:

The result from this mix columns is again given as input to “ADD ROUND KEY” operation where we have to add four round keys.

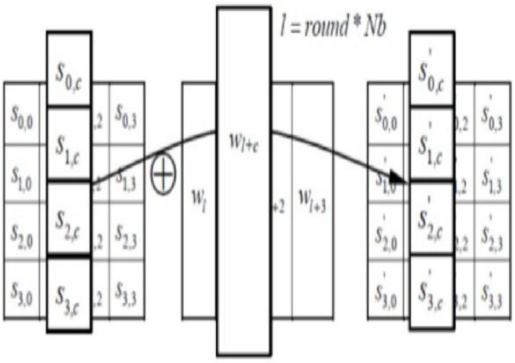


Fig 10 : ADD ROUND KEY

Here adding means performing XOR operation of state array output from mix columns with key(4 words) as shown in above figure.

V. PROCEDURE

DATA OWNER REGISTRATION:

Data owner must sign up with his username and password ,and now the data owner is able to create data security key in signup process. As soon as this process is done this security key of data will be send to user through mail.

Now in SQL software in public auditing phase,in the data owner registration table the owner name and password is stored.

USER REGISTRATION :

In this process the user must register his name with password along with email address,user can create his user id. Here the group name was created by data owner and user must select that group he preffer .

AUDITOR REGISTRATION:

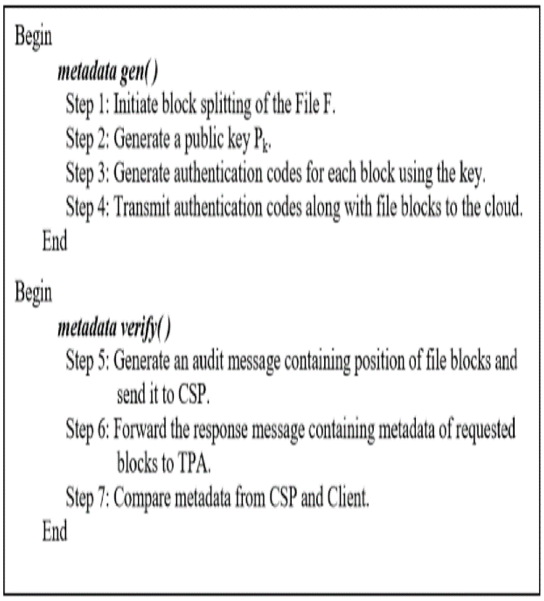
In auditor registration the auditor is provided with user id of whose data he is going to check and auditor also must register his username with password for auditing process.

After all these registrations the data owner must login to upload the data file that is to be encrypted using AES algorithm. After this uploading the data file will be successfully encrypted with 16 byte key. After this user must login with his details to gather that data by presenting the correct 16 byte key ,if the key is wrong then user cant get the required file. Usercan now send the request to auditor to check the data for any errors.

PUBLIC AUDITING:

Public auditing is checking the correctness of the data stored in cloud server database as per the request of the user(client). In public auditing, Third party auditor(TPA) uses the metadata of the original data to verify the correctness of the data. TPA can only access the metadata to check the correctness of original data.

ALGORITHM FOR META DATA



```
Begin
    metadata gen( )
      Step 1: Initiate block splitting of the File F.
      Step 2: Generate a public key $P_k$.
      Step 3: Generate authentication codes for each block using the key.
      Step 4: Transmit authentication codes along with file blocks to the cloud.
  End
Begin
    metadata verify( )
      Step 5: Generate an audit message containing position of file blocks and
              send it to CSP.
      Step 6: Forward the response message containing metadata of requested
              blocks to TPA.
      Step 7: Compare metadata from CSP and Client.
  End
```

Fig 11 : META DATA VERIFICATION

CODING

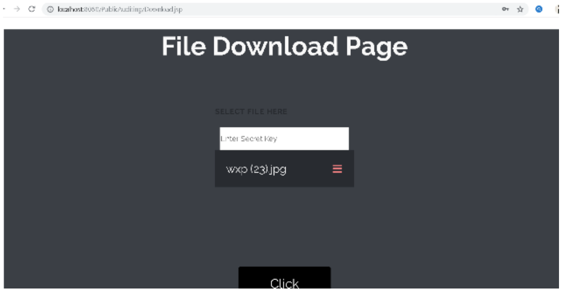
AdminServlet.java

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package com.auditing;
import java.io.IOException;
import java.io.PrintWriter;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;
import java.sql.*;
public class AdminServlet extends HttpServlet {
  protected void processRequest(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
      response.setContentType("text/html;charset=UTF-8");
      PrintWriter out = response.getWriter();
      try {
        /*
         * TODO output your page here. You may use following sample code.
         */
        out.println("<html>");
        out.println("<head>");
        out.println("<title>Servlet AdminServlet</title>");
        out.println("</head>");
        out.println("<body>");
        out.println("<h1>Servlet AdminServlet at " + request.getContextPath() + "</h1>");
        out.println("</body>");
        out.println("</html>");
      } finally {
        out.close();
      }
    }
    // <editor-fold defaultstate="collapsed" desc="HttpServlet methods. Click on the + sign on the left to edit the code.">
    /**
     * Handles the HTTP
     * <code>GET</code> method.
     *
     * @param request servlet request
     * @param response servlet response
     * @throws ServletException if a servlet-specific error occurs
     * @throws IOException if an I/O error occurs
     */
    @Override
    protected void doGet(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
      processRequest(request, response);
    }
/**
```

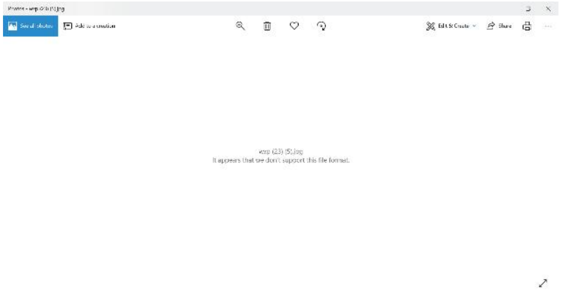
```
    * Handles the HTTP
    * <code>POST</code> method.
    *
    * @param request servlet request
    * @param response servlet response
    * @throws ServletException if a servlet-specific error occurs
    * @throws IOException if an I/O error occurs
    */
   @Override
   protected void doPost(HttpServletRequest request, HttpServletResponse response)
           throws ServletException, IOException {
       HttpSession session1=request.getSession();

       Connection con=null;
       Statement st=null;
       ResultSet rs=null;
       try
       {
           String Username=request.getParameter("username");
           String Password=request.getParameter("password");
                   Class.forName("com.mysql.jdbc.Driver");
con=DriverManager.getConnection("jdbc:mysql://localhost:3306/publicauditing","root","password");
           st=con.createStatement();
           rs=st.executeQuery("select * from admin where username='"+Username+"' and password='"+Password+"'");
           if(rs.next())
           {
              response.sendRedirect("AdminLinks.jsp");
           }
           else
           {

           }
       }
       catch(Exception ex)
       {
           ex.printStackTrace();
       }

   }

   /**
    * Returns a short description of the servlet.
    *
    * @return a String containing servlet description
    */
   @Override
   public String getServletInfo() {
       return "Short description";
   }// </editor-fold>
}
```

VI. RESULT

We get result using softwares called NET BEANS and SQL ,the file is encrypted in the local host server.The below pic shows the page where scret key is typed to get the file.

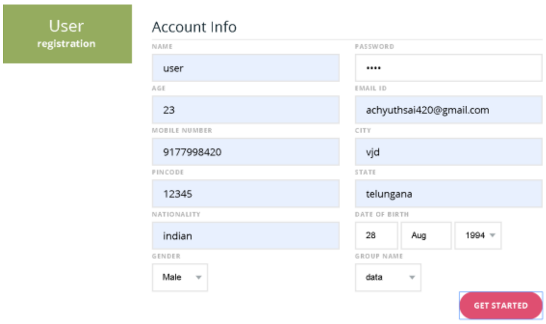


When the key is wrong then the file shows it is corrupted like this



wxp (23) (5).jpg
It appears that we don't support this file format.

Like this the file is encrypted. After user,owner and auditor registrations.



Account Info

NAME	PASSWORD
user	••••
AGE	EMAIL ID
23	achyuthsai420@gmail.com
MOBILE NUMBER	CITY
9177998420	vjd
PINCODE	STATE
12345	telungana
NATIONALITY	DATE OF BIRTH
indian	28 Aug 1994
GENDER	GROUP NAME
Male	data

The above picture shows the user registration process.

VII. CONCLUSION:

By this method the data to be transferred to the user encrypted securely and verified by public auditor with the privacy of the data owner preserved.

REFERENCES:

1. The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.
2. B. Wang, B. Li, and H. Li, “Certificate less Public Auditing for Data Integrity in the Cloud,” Proc. IEEE Conf. Comm. and Network Security (CNS’13), pp. 276-284, 2013.
3. C. Wang, S.S. Chow, Q. Wang, K. Ren , and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
4. B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” Proc. IEEE INFOCOM, pp. 2904-2912, 2013.
5. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud (Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE)