AN EFFICIENT ASCII-BCD BASED STEGANOGRAPHY FOR CLOUD SECURITY USING COMMON DEPLOYMENT MODEL

[1] C.SARAVANAKUMAR, [2] C.ARUN

[1] Research Scholar, Faculty of Computer Science and Engineering,
Sathyabama University, Chennai, Tamilnadu, India
[2]Professor, Department of Electronics & Communication Engineering,
R.M.K College of Engineering and Technology, Chennai, Tamilnadu, India.
E-mail: [1]mailofcsk@gmail.com, [2]carunece@gmail.com

ABSTRACT

Cloud computing is a service oriented computing which offers everything as a service by following the pay-as-you-go model. It is more popular because the cloud data are accessed by variety of customers. An important issue of the cloud computing is to secure the customer data in geographical disperse locations. There are plenty of security standards and policies are available in order to secure the data, but these standards are exist only at the cloud end. It is a critical task for the customer as well as provider to store, retrieve and transmit the data over the cloud network and storage in a secure manner. The customer can store or process the sensitive data who needs a security during the time of travel over the network to the processing environment. The existing security algorithm secures customer data at the provider end which are not known by the customer and also multiple boundaries exists in the cloud resource access which leads the reliability problem. The main objective of the proposed algorithm is to develop a customer owned security algorithm and the encrypted data are send to the provider end. The provider can also apply the security over the customer's data by using efficient algorithm. The customer's data are in a secure manner at both the end to achieve maximum reliability. The proposed algorithm uses ASCII and BCD security with steganography that stores the encrypted data in an image file which will be send to the provider end. The security algorithm has to be implemented by using the CDM (Common Deployment Model) which also provides an interoperable security services over the cloud. In future, steganography can be applied to secure the virtual images in the cloud computing.

Keywords: *Cloud Computing, Cryptography, Steganography, Distributed Systems, CDM*

1. INTRODUCTION

The evolution of computing starts with desktop computing, client server computing, peer-to-peer (P2P) computing, distributed computing, collaborative computing and grid computing. These models have a plenty of advantages and faces lot of issues which exits in the current IT market. The cloud computing is a type of computing which provides the service to the customer for their current need i.e. pay-as-you-go basis. It has the features like resource sharing, resource pooling, on-demand service provisioning, multi-tendency, elasticity, security and privacy which are provided as a service. These services are classified into various service models they are Software-as-a-Service (SaaS), Platform-as-a-Services (PaaS), Infrastructure-as-a-Services (IaaS) and Everything as a services (XaaS). The cloud services are deployed into various deployment models such as private cloud, public cloud, hybrid cloud, and community cloud. The deployment models which are related to the cloud security are classified into Separation model, Cryptography model, Tunnel model, Availability model etc [16]. These models will not provide a complete solution because it follows only one standard. The customer data are stored in the cloud with a high level of security [13] by using various security measures and parameters. The cloud computing faces some problem in various perspectives they are privacy [18], trust management [19], interoperability [20] etc., Normally the cloud customer has locked into a single cloud provider only so that, it will not fulfill the customer's requirement. This problem is overcome by using more than one cloud provider to retain the customer in the cloud environment for a long time. The security over the cloud is always maintained at the cloud end with an efficient security algorithm by the cloud provider [14, 15] so, the customer doesn't know about what level of security exists in the cloud end and also lacks in the data protection during travel. The proposed algorithm is used to secure customer's data during the time of travel from one end to another, so that the customer's data are not disclosed by unauthorized person. This algorithm performs encryption and decryption process by combining ASCII (American Standard Code for Information Interchange), BCD (Binary Coded Decimal) and image based steganography. Cryptography is the process of enciphering and deciphering the data that involves in the operation of converting the data into a scrambled code and again into a readable form [9]. Cryptography ensures the Confidentiality, Integrity, Non-repudiation and Authentication [10] for us while transferring the encrypted code from the sender to the receiver. Plain text is the original message that exists before enciphering and after deciphering the data. Cipher text is the scrambled message which is an intermediate representation of the data between enciphering and deciphering process. An image is a collection of numbers that constitutes different intensities of light in different areas. This numeric representation forms a grid and the individual points are referred as pixels. There are plenty of popular image formats available they are JPEG (Joint Photographic Experts Group), PNG (Portable Network Graphic), TIFF (Tagged Image File Format), GIF (Graphics Interchange Format) [17]. These file formats uses either lossy or lossless compression techniques which maintain the image quality at the maximum level. The lossy compression is used to save space but discards some image data which does not give the effects in the original image. The lossless compression never discards any image data [11]. Steganography is a process which is used to hide one object into another object. The objects are referred as image, audio, video etc., for transferring the data in more secure way from sender to receiver [12]. There are plenty of issues exits in the steganography techniques which are resolved by using ASCII based steganography. The efficiency of the steganography is improved by hiding an encrypted text within the image which is more powerful than the existing algorithms. The proposed algorithm is used to improve the efficiency by combining ASCII and BCD code for securing the customer's information. The homomorphic encryption performs some queries with aggregated financial data. The computational load and infrastructure acquisition is analyzed by using homomorphic cryptosystems and linear secret sharing schemes. This algorithm is restricted to a specific part in the cloud application [1]. OTP (One-Time Password) is a technique which is used to secure an enterprise application but it faces a problem like lost or stolen by the unauthorized parties. This problem is overcome by using the REAL (Rubbing Encryption Algorithm) and also it compares various cloud based OTP methods with security. The main objective of this algorithm is to secure OTP from any attack [2].The vulnerabilities present in the cloud computing can be categorized into virtualization level, IP level, unauthorized access level. There are plenty of security solutions exit in the cloud but they are not suitable for all the layers from customer end to cloud end. The dynamic security algorithm is developed to achieve a different level of cloud security and privacy. This security algorithm requires a multi-level security because it is restricted to only one level [3]. The security and privacy issues are handled according to the capacity of processing and storage over the mobile devices in order to access the cloud services. The mobile user can access the cloud by implementing a digital credential based authentication scheme for identification but it lacks in scalability problem. The dynamic credential generation scheme is needed to enhance the scalability and reduce the processing burden [4]. The security framework is used to provide an end-to-end security over wireless multi-hop mesh AMI (Advanced Metering Infrastructure) network. It is not suitable for worm-hole attack prevention in wireless mesh AMI networks. This framework can also be extended to gateway-aware multipath routing over internet-based wireless mesh AMI network [5]. The privacy and security threats exist in the vehicular Ad-Hoc network has been identified and analyzed at the maximum level. IP-CHOCK is a model used to prevent the DoS (Denial of Service) attack. The proposed model is compared with the existing algorithm by using various parameters such as filtering, trace back, small and large DoS attack prevention etc. This model is not suitable for large

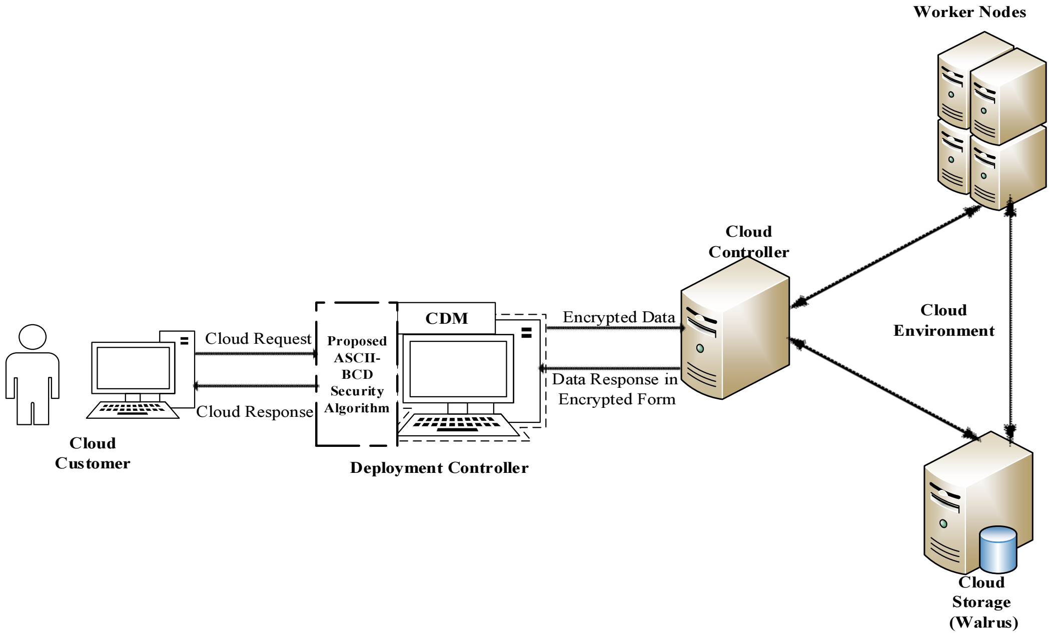

Figure 1. Architecture Of The Proposed Algorithm

real network, which can be achieved by introducing adaptive hash function mechanism with maximum utilization in the hash table [6]. The virtualization allows various users to access and share the physical server which leads security issues between the cloud customer and provider. The technologies uses various security handling algorithm so, this also leads a severe security problem [7]. The governmental IT has to maintain a suitable measures and policies for preventing the unwanted security risk in order to handle all government operation. The tangible risks and intangible risks are identified in the cloud for achieving maximum reliability over the information [8]. The existing technique focused on the security measures over customer data at the cloud provider end. The main objective of the proposed algorithm is to provide security over the customer's data by applying ASCII-BCD based image steganography.

2. ARCHITECTURE

Figure 1 shows that the architecture of the proposed algorithm. The customer needs to store the confidential information in the cloud for effective access. The customer information is applied into ASCII-BCD based encryption algorithm which is used to generate the encrypted information. This algorithm is deployed in the deployment manager with Common Deployment Model (CDM). The CDM has various features to enable effectiveness over the cloud. The encrypted data are handled by the cloud controller who controls the entire cloud. The node controller controls all worker nodes and handles the virtual machines properly. The data are stored at the cloud storage (Walrus). The cloud can store customer's data with various security measures which are not known by the cloud customer. A multi-level security is applied over the cloud in order to protect the data during the travel between the two end i.e. customer end to cloud end and vice versa. The data comes from cloud to the customer is in the form of encrypted manner. The CDM get the response from the cloud and applies the decryption algorithm and the original text will be recovered. The overall process of the proposed ASCII-BCD algorithm is based on image steganography technique. There are two phases of encryption are available they are ASCII-BCD conversion phase and image steganography phase. The main objective of the proposed system is to secure the customer data using various level of security from customer end to cloud end and vice versa.

3. CONCEPTUAL DIAGRAM

Figure 2 describes that the conceptual diagram of the proposed algorithm. An input section reads the data from input source file then it is converted into ASCII-BCD based data by using security keys. The conversion section generates all the cipher text and then this partial cipher text are converted into a complete cipher text using another

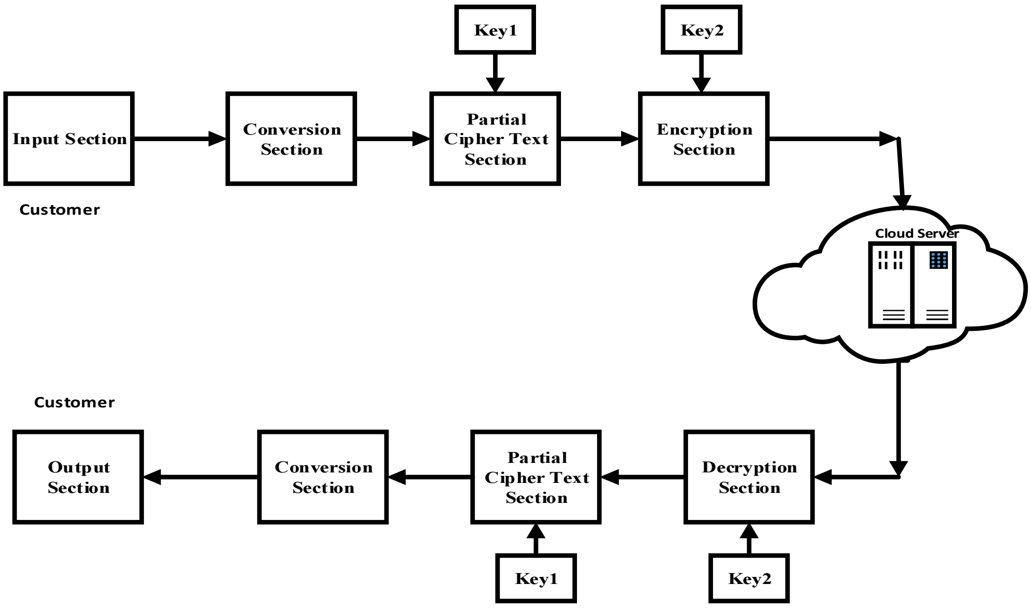

Figure 2. Conceptual diagram of the proposed algorithm

key. A complete cipher text is send to the cloud for storage using encryption section. If a customer need the data from the cloud, first it reads an image, identifies the position in the image and then it converts the image into BCD form. The partial cipher text is then converted to an equivalent ASCII character by using the decryption key. The original text is recovered by using another key with decryption process.

4. ENCRYPTION

Figure 3 shows that the encryption process of the proposed algorithm. The encryption process uses an image based steganography for securing customer's data. The 2D picture is used to hide the information with any image file format. The customer data is stored in an ASCII based text characters for transmission. This data file is converted and represented to align matrix format then each character are assigned based on the position numbers. The BCD code equivalent is generated from an ASCII value of the data i.e. 16bit BCD conversion. The position of the character is taken from the matrix and the position number is converted into 16-bit BCD. The BCD value of the position and the data are XORed which gives the resultant with 16-bit BCD value. The resultant value is considered as a partial cipher text. The private key is XORed with the partial cipher text which provides a complete cipher text and then it will be sent to the cloud by the customer. The customer can able to recover the information by using the private keys. A complete cipher text is also in the form of BCD representation. This process will continue until all the data file contents are accessed i.e. EOF file is reached. These complete cipher texts are maintained at the buffer which is suitable for steganography process. This cipher text is embedded with 2D image which is related to pixel position. The pixel position is marked with BCD values in two parts namely row and column. The first part determines the row of the pixel whereas the second part determines the column of the pixel. The address and value of the first cipher text in the image is determined by another private key. The first cipher text is taken from the buffer and placed in the image with related position value i.e. key value. This process is repeated until all the cipher texts are placed into an image. This image holds all the cipher text in various pixel positions which gives the same appearance and quality and it is send to the cloud provider who maintains the information by applying another level of security at the cloud.

5. DECRYPTION

Figure 4 shows that the decryption process of the proposed algorithm. The customer needs the information which is already stored in the cloud as an image. The cloud provider verifies the requirement of the customer, selects the image and sends to the customer. The received image is decrypted using the key which is already used for the encryption process. The first key is a shared key

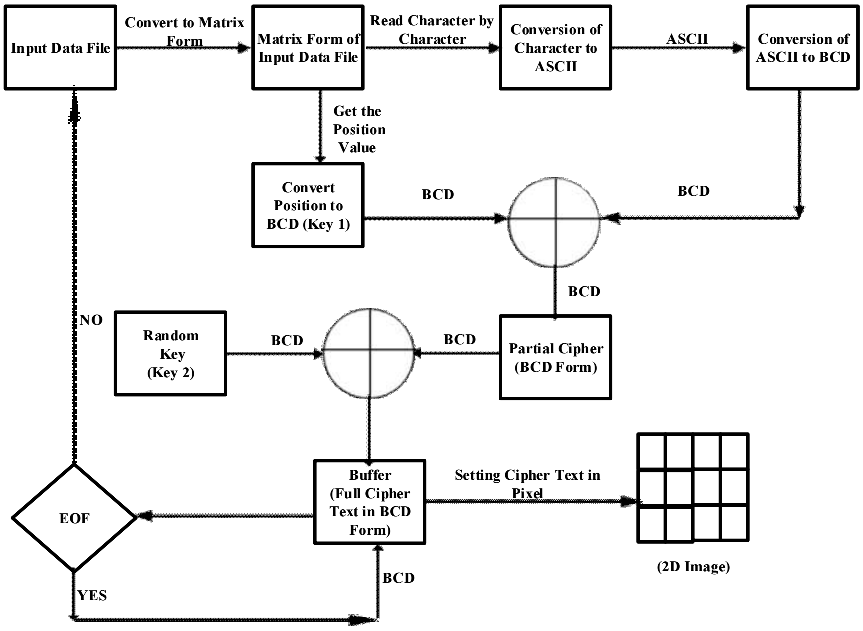
Input Data File
Convert to Matrix Form
Matrix Form of Input Data File
Read Character by Character
Conversion of Character to ASCII
ASCII
Conversion of ASCII to BCD
Get the Position Value
Convert Position to BCD (Key 1)
BCD
BCD
BCD
NO
Random Key (Key 2)
BCD
BCD
Partial Cipher (BCD Form)
Buffer (Full Cipher Text in BCD Form)
Setting Cipher Text in Pixel
EOF
(2D Image)
BCD
YES

Figure 3. Encryption process

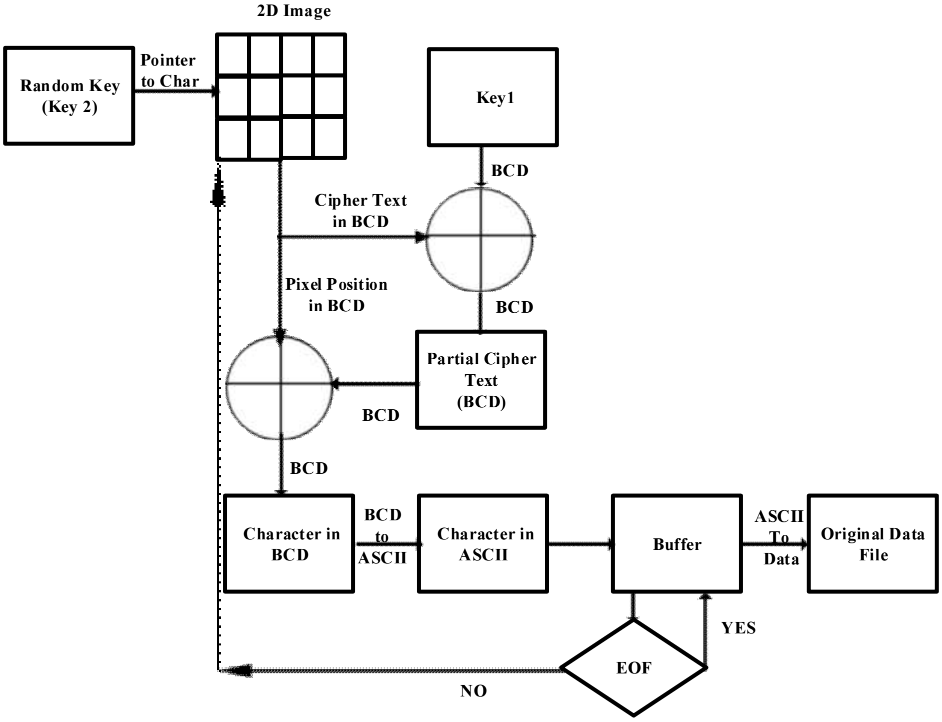

Fig 4. Decryption Process

for both encryption and decryption process whereas another key is only used for decryption process. The second key is used to identify the pixel position and also to locate the first cipher text character in the image. Once the position of the first cipher character is found out it will be converted into BCD value. The second cipher text is identified based on the first cipher text and so on. The partial cipher text is generated by XORed with BCD and another key. The BCD value of the partial cipher text is converted into the ASCII character representation. This process continues until no more position exists i.e. EOF is reached. The original text is recovered by combining all partial cipher text into a complete cipher text which are available in the image.

6. ALGORITHM

6.1 Encryption Algorithm

```
ASCII_Based_SteganoEncryption ()
Begin
i=0;
TextFile ← Input_Read (); //Reading the Text file
for each (character ← TextFile) do
                              // Reading the character
begin
IM [] ←character;
IC←IM[i];
 AIC←ASCII (IC); // ASCII conversion of input
character
BIC←BCD (AIC); // BCD conversion of AIC
PIC←Position[IC];
                        // Position of the input character
APIC←ASCII (PIC); // ASCII value of PIC
BPIC←BCD (APIC); // BCD value of APIC
Partial_Cipher [] ← (BIC) XOR (BPIC);
                        // generation of partial cipher text
Key1← Key_Gen ();          // key generation
Full_Cipher [] ← (Key1) XOR  (Partial_Key []);
                        // generation of full cipher text
BFC [] ← BCD (Full_Cipher []);
            // BCD conversion of full cipher text
IImage←Image_Read ();
PIImage [] ← Pixel_Position (IImage);
for each position ← PIC do
Image_Position ← Set_Pixel (BFC []);
            // set the pixel over the image
end;
i++;
end;
*FirstCiphetText←Key2 [Full_Cipher[0]];
                        // pointer to the first cipher text
End: Encrption_Process ()
```

6.2 Decryption Algorithm

```
ASCII_Based_SteganoDecryption ()
Begin
i=0;
ImageFile ← Image_Read ();
                         //Reading the image file
for each pixel ← ImageFile do
                        // Reading the pixel position
begin
IM [] ←pixel;
BIP←IM[i];
Key2← Key_Gen ();          // key generation
BPartial_Cipher [] ← (Key2) XOR (BIP);
                // generation of BCD partial cipher text
BIMPP← get_Image_Pixel_Position ();
                // reading the image pixel position;
OBC []←(Key1)XOR(BPartial_Cipher []);
                // BCD based output character
AOBC [] ←ASCII (OBC [])
// ASCII conversion of BCD based output character
OC [] ← character(AOBC []);
                    // character conversion of AOBC
end;
for each character ← OC [] do
 TextFile← character;
end;
End: Decryption_Process ()
```

7. EXPERIMENTAL RESULT

Fig 5 describes that the resultant screen of the proposed algorithm. Table 1 shows that the image representation after embedding the information.

Plain Text : **Hi How are you**

7.1 Keys

KEY A-002
KEY B-51

7.2 Encryption Process

Plain text = H
ASCII of H = 072
BCD code of 72(H)=0000000001110010 (1)
Character Position in text file = 01*01
BCD code of character position =
0000 0001 0000 0001 (2)
XOR Operation of (1) & (2) =
0000 0001 0111 0011 (3)
Decimal value of partial cipher = 0173
Random key (key A) = 002
BCD code of key A=0000 0000 0000 0010 (4)
Partial cipher of H (3) = 0000 0001 0111 0011
XOR Operation of (3) & (4) =0000 0001 0111 0001
Full Cipher text of H (key B) =
0000 0001 0111 0001 (5)
Decimal value of Cipher = 0171.
Key B-051.

0171 is stored in 051 image position. Where in 051, 5 indicates 5th row of the image pixel's coordination.1 indicates 1st column of the image pixel's coordination.

Table 1 Data Representation In The Encrypted Text With Image (Embedded Image)

				1*5,23		
		1*6,32				
	1*7,41					
1*8,67						
1*11,61			**1*3,77**			
1*1,67						**1*2,54**
1*9,72						
	1*10,26					**1*4,15**

7.3 Decryption Process

Key B =051
051 have the cipher text 0171. 051=0171(5th row 1st column)
0171 is the cipher text of 1*1 position character According to the text file.
0171=01*1(which means 1st row 1st column of text file has cipher (061).
Decimal value of cipher Text = 0171
BCD code of the Cipher text =
0000 0001 0111 0001 (6)
BCD code of Key B = 0000 0000 0000 0010 (7)
XOR Operation of (6) & (7) =
0000 0001 0111 0011 (8)
Decimal Value of partial cipher =0173
BCD code of the partial cipher (8) =
0000 0001 01110011.
Character's Position in text file = 01*01
BCD code of the character position =
0000 0001 0000 0001 (9)
XOR Operation of (8) & (9) [key A] =
0000 0000 0111 0010 (10)
ASCII value of the BCD value = 072
Plain text =H

7.4 Output screen shots

a) b) c)

Fig 5 Screen Shots [A) Original Image, B) Embedded Image, C) Output Image]

8. CONCLUSION AND FUTURE WORK

Cloud computing provides the resources to the customer by following pay-as-you-go basis model. The cloud services are deployed at the server using various deployment models which provide the services only within the restricted boundary. The customer data are maintained at the server which needs security. Cloud security imposes various measures over the customer data for achieving maximum reliability. The customer data are maintained by the provider with maximum security level in order to protect from unauthorized access. The customer's data enters into various level of access from customer end to provider end for accessing a cloud utility. Traditional or existing security algorithms are used to secure the data in the cloud end but, it never concentrates on the security measures in various layers exist between the customer and cloud. This problem is overcome by implementing the proposed algorithm by using ASCII-BCD based steganography in order to achieve the maximum security level. This algorithm uses two keys for encryption as well as decryption process. There are two phases exists in the security algorithm at both process which provides two cipher text namely partial cipher text and complete cipher text. The ASCII characters are converted into the BCD value then it identifies the pixel position in the image. The deployment manager has CDM which gives maximum support to secure the data at the customer end. The encrypted data are embedded within the image without compromising the quality and appearance. The customer needs the data from the cloud which performs a reverse process of an encryption with two keys. The main objective of the proposed algorithm is to control and send the data in an encrypted manner by the customer to the provider. The provider also maintains the data with a standard security algorithm in order to protect the data from unauthorized access. In future this algorithm can be extended to virtual images by achieving the reliability at maximum level.

REFRENCES:

[1] Juan Camilo Corena, Tomoaki Ohtsuki," Secure and Fast Aggregation of Financial Data in Cloud-Based Expense Tracking Applications", Journal Network System Management (2012) 20: DOI 10.1007/s10922-012-9248-y,Page 534–560.

[2] Fred Cheng," Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm", Mobile Netw Appl (2011) 16, DOI 10.1007/s11036-011-0303-9,Page 304–336.

[3] Chirag Modi , Dhiren Patel , Bhavesh Borisaniya , Avi Patel , Muttukrishnan Rajarajan," A survey on security issues and solutions at different layers of Cloud computing", Journal of Super Computing (2013) 63:, DOI 10.1007/s11227-012-0831-5,Page 561–592.

[4] Abdul Nasir Khan , M.L. Mat Kiah ,Sajjad A. Madani , Atta ur Rehman Khan ,Mazhar Ali," Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing", Journal of Super Computing, DOI 10.1007/s11227-013-0967-y,Page 1-20.

[5] Binod Vaidya ,Dimitrios Makrakis „Hussein Mouftah," Secure and robust multipath routings for advanced metering infrastructure", Journal of Super Computing (2013) 66,DOI 10.1007/s11227-013-1009-5, Page 1071–1092.

[6] Karan Verma , Halabi Hasbullah , Ashok Kumar," Prevention of DoS Attacks in VANET", Wireless Personal Communication (2013) 73:DOI 10.1007/s11277-013-1161-5,Page 95–126

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013, 4:5,http://www.jisajournal.com/content/4/1/5„ Page 1-13

[8] Scott Paquette, Paul T. Jaeger, Susan C. Wilson ," Identifying the security risks associated with governmental use of cloud computing", Government Information Quarterly 27 (2010) Page 245–253.

[9] CRYPTOGRAPHY, WEBSITE: HTTP://WWW.BARCODESINC.COM/ARTICLES/CRYPTOGRAPHY2.HTM [ACCESSED ON 5.2.14]

[10]Fundamental Security Concepts,http://cryptome.org/2013/09/infosecurity-cert.pdf,[Accessed on 31.1.14]

[11] Susen Rabold,Image Representation, http://www.inf.ed.ac.uk/teaching/courses /il1/slides09/IL-Image-0311.pdf, [Accessed on 30.1.14]

[12] STEGANOGRAPHY, HTTP://EN.WIKIPEDIA.ORG/ WIKI/STEGANOGRAPHY,[ACCESSED ON 31.1.14]

[13] P.G. Dorey, A. Leite ,"Commentary : Cloud computing e A security problem or solution?", informationsecuritytechnicalreport 1363-4127/$ doi:10.1016/j.istr. 2011. 08.004,Pp 1-8

[14] Piers Wilson," Positive perspectives on cloud security", informationsecuritytechnicalreportxxx(2011), 1363-4127/$,doi:10.1016/j.istr.2011.08.002,Pp 1-5.

[15]Balachandra Reddy Kandukuri, Ramakrishna paturi V, Atanu Rakshi,"Cloud security Issues",978-7695-3811-2/09/$26.00,IEEE 2009, DOI101109/SCC2009.84.

[16]. Gansen Zhao,Chunming Rong, Martin Gilje Jaatun, Frode Eika Sandnes," Deployment Models: Towards Eliminating Security Concerns from Cloud Computing",DOI: 978-1-4244-6830-0/10, 2010,IEEE, Pp 189-195.

[17] Tim Vitale,Digital Image File Formats – TIFF, JPEG, JPEG2000, RAW and DNG, http://cool.conservation-us.org/coolaic/sg/emg /library/pdf/vitale/2007-07-vitale-digital_image_file_formats.pdf [Accessed on 31.1.14]

[18]Richard M. Thompson II,Cloud Computing: Constitutional and Statutory Privacy Protections,http://www.fas.org/sgp/crs/misc/R43015.pdf [Accessed on 1.2.14].

[19] Siani Pearson,Privacy, Security and Trust in Cloud Computing,HP Laboratories,HPL-2012-80R1,http://www.hpl.hp.com/techreports/2012/ HPL-2012-80R1.pdf [Accessed on 2.2.14]

[20] A V Parameswaran and Asheesh Chaddha,Cloud Interoperability and Standardization, SETLabs Briefings, VOL 7 NO 7,2009,Page 19-26