Effective ASCII-HEX Steganography for Secure Cloud

S. Afghan[1], M. J. Qureshi[2], R. Abbas[3]

[1,2,3]Computer Science Engineering Department, University of Engineering and Technology, Lahore, Pakistan
[1]sherafghanmalik@live.com

Abstract-There are many reasons of cloud computing popularity some of the most important are; backup and rescue, cost effective, nearly limitless storage, automatic software amalgamation, easy access to information and many more. Pay-as-you-go model is followed to provide everything as a service. Data is secured by using standard security policies available at cloud end. In spite of its many benefits, as mentioned above, cloud computing has also some security issues. Provider as well as customer has to provide and collect data in a secure manner. Both of these issues plus efficient transmitting of data over cloud are very critical issues and needed to be resolved. There is need of security during the travel time of sensitive data over the network that can be processed or stored by the customer. Security to the customer's data at the provider end can be provided by using current security algorithms, which are not known by the customer. There is reliability problem due to existence of multiple boundaries in the cloud resource access. ASCII and HEX security with steganography is used to propose an algorithm that stores the encrypted data/cipher text in an image file which will be then sent to the cloud end. This is done by using CDM (Common Deployment Model). In future, an algorithm should be proposed and implemented for the security of virtual images in the cloud computing.

Keywords-Pay-As-You-Go Model, Cryptography, Steganography, CDM,ASCII-HEX, Cloud Computing

I. INTRODUCTION

In the history of computing, various models of computing have been developed to make the computing robust, efficient, intelligent and effective. Peer to Peer computing and client server computing has been developed for better interaction and communication of client. Distributed computing plays a big role to achieve high availability and accuracy of data. Grid computing is also a major development. Internet is continuously changing and growing from the start of its development. IT (information technology) is spreading everywhere. Above mentioned model gives us many advantages and services but there are some issues which cannot be handled by them. There are also services which cannot be provided by them. There is need to solve these issues and provide large and different variety of services capable of full utilization of computing resources. A new infrastructure deployment model is cloud computing to provide variety of services and resources on demand basis. These resources can be shared and pooled. It can also provide security and privacy to different clients on demand basis.

Classification of various services can be done into different categories. Online software services are provided to the customers using cloud computing so that customers don't have to install application in their system and this type of delivery model is called SaaS (software as a service). Different applications can be developed by using PaaS (platform as a service) delivery model. There are also other delivery models like IaaS (infrastructure as service) which can provide infrastructure environment and networking components, Taas (testing as a service) to provide testing environment and testing applications, and XaaS (everything as a service). For better deployment of these services, different models are used. Community, public, private, and hybrid clouds are types of these deployment models. In [xvi], cryptography and separation models are used to protect cloud computing and to make it more secure. Availability model and tunnels are also used for cloud security. All these models use same standard so they are not efficient and effective for better security of cloud computing.

This paper introduces mainly common security algorithms which are used to make cloud secure and efficient. Section 2, discusses the problem statement while section 3 covers the types of steganography and cryptography used in cloud computing. Section 4, discusses the architecture of CDM and its working. Proposed algorithm, working of encryption and decryption process is described in section 5. Section 6, summarizes the work of the paper and plans on the future work.

II. PROBLEM STATEMENT

The cloud environment uses various security measures and parameters to store the customer's data with high level of security. According to [xviii, xix, xx], customer wants to secure his personal and sensitive data on cloud but there are some privacy and trust

management issues which needs to be resolved. Sometimes the services of single cloud are not sufficient to fulfill the needs of cloud's customer. This issue can be resolved by combining the services of two or more cloud computing providers. The cloud provider always maintain the security of cloud environment with an efficient mechanism at the cloud end so that the client does not have information or knowledge about the security levels of cloud environment [xiv, xv]. How the data is being stored and moved over a medium in a cloud is also hidden from customer.

In this paper, we introduce an algorithm that is used to provide the security to the customer's data from unauthorized access. This algorithm uses combination of Hex (Hexa-decimal) and ASCII (American standard code for information interchange). Encryption process is performed to generate some different keys for security of data. By using these keys, decryption of data can also be done.

Data can be converted from readable form to a scrambled code and again from scrambled code to readable form through cryptography and the main components of cryptography are encryption and decryption [ix]. Cipher text is sent from sender to receiver as well as from receiver to sender to achieve authentication, confidentiality and integrity [x]. Original data remains same before encryption and after decryption process. Before decryption and after encryption process, the data is in the form of cipher text which is called intermediate representation of data. The process of hiding or merging one type of data into another type of data is steganography. There are different techniques to achieve steganography which use image, audio and video or any other form of objects [xii]. The proposed algorithm uses steganography and cryptography for high security of data and from its unauthorized access using ASCII and HEX code. In encryption, Queries are executed with monetary data. Linear secret sharing techniques are performed for evaluation of computational burden and organization acquirement. But particular portion in the cloud can be delimited by using this algorithm [i]. By using OTP (one time authentication/password), data and enterprise application can be secured. There exists a problem in this procedure like stealing of password or authentication key by unauthorized person. Rubbing encryption algorithm is used to find difference among several cloud based OTP techniques. Security of password from attacks is main goal of this algorithm [ii]. There are many security algorithms to remove vulnerabilities existing in cloud computing like illegal access, virtualization and IP level vulnerabilities. But, these algorithms do not provide appropriate solution from cloud site to customer site. As only one level of security is provided, which is not enough to secure the cloud, so dynamic algorithm gives solution and protect different levels of cloud [iii]. When accessing cloud services, mobile devices handle security and confidentiality as per their capability of storage, memory, operating system and processing power. Scalability and processing issues are needed to be resolved when applying digital credential based validation/authentication technique [iv]. In Mesh AMI (advanced metering infrastructure) attacks cannot be prevented using this technique. According to [v], this issue can be resolved by extending the framework to gateway conscious multipath routing. DOS (Denial of Service) attacks can be prevented by implementing IPC (IP Chowk) model and this model is very effective compared to many other models and techniques when using trace back, filtering and many other parameters. IP Chowk model is not recommended for large networks as compared to Hash function technique which is very suitable to implement [vi]. There is graph security problem while using virtualization as it does not prevent users from sharing and accessing the physical server and creates many problems of security among provider and user of cloud [vii]. According to [viii], there is very important role of governmental IT as maximum availability and reliability can be achieved by governmental IT. But there is need to maintain suitable strategies, procedures and there is also need to identify and measure tangible and intangible threats. Proposed algorithm's main goal is to achieve maximum security over the data of customer by ASCII-HEX key based steganography. Images are used for this purpose.

III. Literature Review

Maximum security can be achieved by using ASCII-BCD [xi], ASCII-HEX steganography. There are many type of this technique of data hiding.

A. Types of Steganography

Text Steganography: Text steganography can be achieved by using word shifting, line shift and feature coding. Working of these coding techniques is alteration of the text or by alteration of some certain characteristics of textual elements [xiii].

1) Image Steganography

Steganography can also be done by using images to cover the objects and this method is also very popular for steganography. There are many different file formats for digital images and different algorithms also exist for these file formats [xvii]. Encrypt and scatter, masking and filtering, redundant pattern encoding and LSB (Least significant bit) insertion are types of these algorithms.

2) Audio Steganography

This type of steganography works by embedding sensitive data into digitized audio signal. In this way slight alteration of binary sequence of the corresponding audio file is done. In this steganography,

Phase and LSB coding, and spread spectrum methods are used.

3) Video Steganography

Steganography can also be done in video files. Collection of images and sounds produce these video files and many techniques which are used for images and audio files can also be applied on video files. This type of steganography is useful for hiding large amount of data [xxi].

4) Protocol Steganography

In protocol steganography covert channels and network control protocols are used, and information is embedded within messages.

B. Types of Cryptography

Cryptography is used to provide security. In cryptography plain text is secured by encrypting the message with key. This key secures the message from intruders who can read the message and decrypt it to get the message back. Encryption and decryption of the message cannot be done without the key [xxii].

1) Secret key Cryptography

It is very traditional and also known as symmetric cryptography. Encryption and decryption of message is done by a single key. It is also very useful for authentication. Set of rules are followed by sender for better encryption of text and transmission of the cipher text to the receiver. Same set of rules are also followed by receiver to decrypt the message. The main problem is distribution of keys as it is necessary that sender and receiver have the keys. Generally, stream cipher and block cipher are categories of this secret key cryptography. The key is continuously changing because of feedback mechanism. This scheme encrypts one block at a time with same key for each block.

2) Public key Cryptography

Complementary assignment of two keys (one public, one private) to the individuals involved in a transaction is done by public key cryptography for securely exchanging messages. One of the key is called public key and it can be shared by the owner while other key is not shareable and is called private key.

IV. Related Work

Pay-as-you-go model is followed to provide everything as a service. Various deployment models are used for better deployment of services within restricted boundary. There is need of high security to secure valuable data of customers, stored and maintained at the server. Many security measures are imposed over the data of customer to achieve maximum security and reliability. There are many levels of security. The customer's data enters into various level of access from customer end to provider end for accessing a cloud utility. Different algorithms are used to safe the data at the cloud end but, they are not effective.

TABLE 1
Proposed Model Vs Previous Model

Attribute	Proposed Technique	Previous Technique
Cypher length	Smaller	Bigger
Effective	More Effective	Less Affective
Complexity	More Complex to break its code due to more keys	Less Complex to break due to less keys
Memory	Takes less memory	More memory
Processing	Takes less processing	Takes more processing
Composition	ASCII and HEX	Binary (1,0)

In [xi] this problem has been overcome by implementation of ASCII-BCD based steganography in order to achieve maximum security level and to overcome the problems of traditional algorithms. Encryption and decryption process uses two types of keys. Encryption and decryption process also has two phases to provide two cipher text; alphabets cipher and digits cipher. Conversion of characters of text into ASCII and then into BCD is done to generate complete cipher text which is placed on the image.

In Fig. 1, CDM is used which is used for the support of maximum security at client side. After encryption the cipher text is placed into image.In proposed algorithm's, encryption and decryption process, conversion of ASCII is done into HEX. When customer requests for the data from the cloud, a reverse process of an encryption with keys occurs. We have compared our model with the previous models [xii], and Table I is illustrating the comparison.

V. Proposed Work

The data coming from input section is placed into a matrix to get positions of characters in data to generate key 0.

Then this data is converted to ASCII form for encryption purpose. To achieve higher level of security, data is again converted from ASCII to Hex and matrix of HEX data is made and positions of HEX characters are extracted to make key 1.

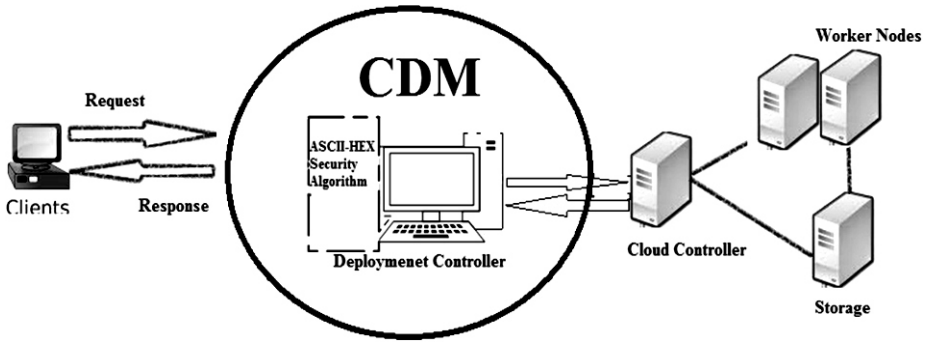

Fig. 1. Working of Cloud and CDM

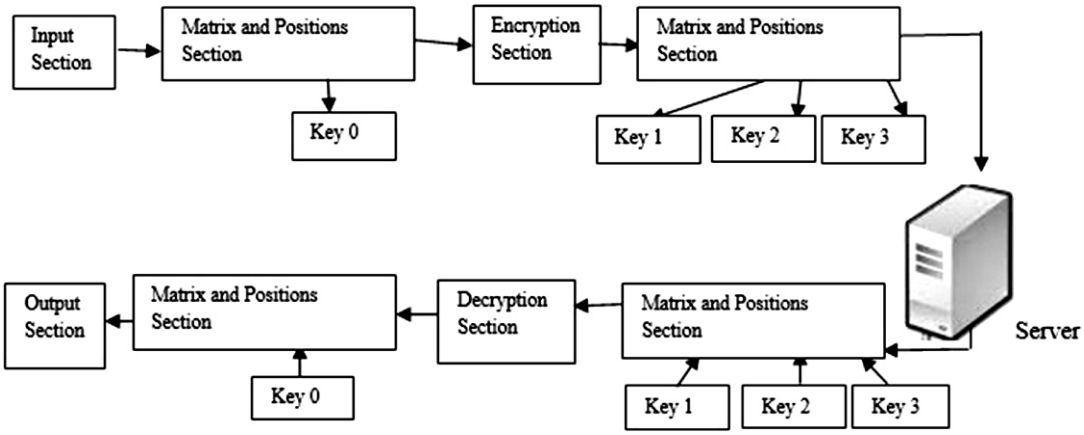

Fig. 2. Proposed Algorithm's Conceptual Diagram

HEX conversion gives us the data in the form of; 1-8 digits and A-F alphabets. Separate matrix of alphabets and digits is made and the positions of alphabets of HEX give us key 2 and key 3.The encrypted text is then placed into an image starting from some specific pixel and the position of that pixel will work as private key and this image is sent to server for storage purpose.When a customer requests for data, data is read from the image using private key. By using key 2 and key 3, alphabets and digits of HEX data is extracted while key 1 is used to get real Hex form of data for decryption purpose. By using Key 0, we get original position of data and send it to output section. Fig. 2 is the conceptual diagram of the proposed algorithm.

A. Encryption

We use image based steganography for encryption processof the proposed algorithm to highly secure customer's data as shown in Fig. 3. Image of any format can be used to secure and hide the customer's data. Encryption of a sample word is shown below. The sample word is 'known'. When 'k' from 'known' is put into matrix it gets position (01*01). 107 ASCII value is equivalent to character k. After converting 107 ASCII to 3-bit Hex, 06b is generated. This Hex value is put into Hex matrix and its position is obtained. Matrix of digits and matrix of alphabets is generated to get their positions. Same process is done for remaining characters of input file until it encounters space or EOF. Encryption of word 'known' gives us cypher text 'befe06060607706' which will be put into image. The pixel position of image where first character is placed is our private key. In this case let's say 072. 2 indicates 2nd column of the image pixel's coordination and 7 indicates 7th row of the image pixel's coordination. Other keys are shown in Fig. 4.

The input file of customer's data is transformed to matrix form to get the position of characters in the data. These positions are stored and act as a key (Key1). 3-bit ASCII based characters are generated from the text characters.3-bit Hex code is generated by reading and converting 3-bit ASCII data file character by character. There are some special characters whose ASCII to HEX conversion is not available. If there is any of those special character whose HEX conversion is not available then its ASCII will be moved into HEX data. Three bit ASCII digits of those special character are treated as HEX digits. The positions of digits is taken from the hex data file and stored as a second key

(Key 2). The position of alphabets is taken and stored as a third key (Key 3). When there will be any space between characters then both of the matrixes will be placed in the buffer and this cypher text will be placed on image; alphabet characters first and digit characters second. Again the process will start for remaining data until the end of file (EOF). If there is not EOF then next character will be read from input data file. When EOF is encountered then this image will be sent to cloud storage server for storage purposes. This image is used latterly for decryption purposes.

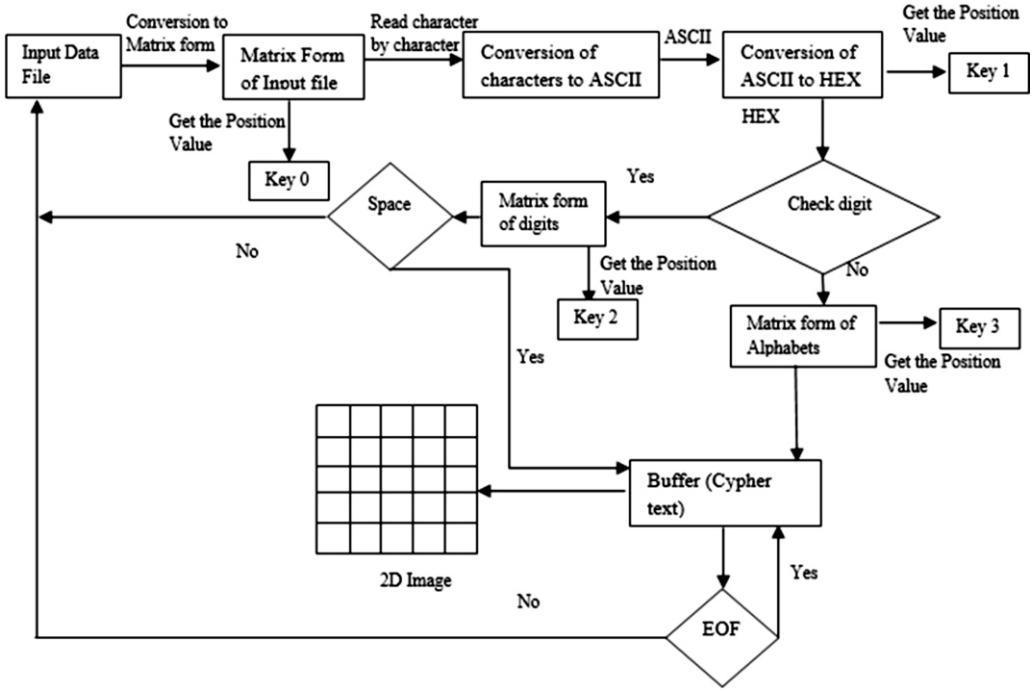

Fig. 3. Encryption Process Diagram

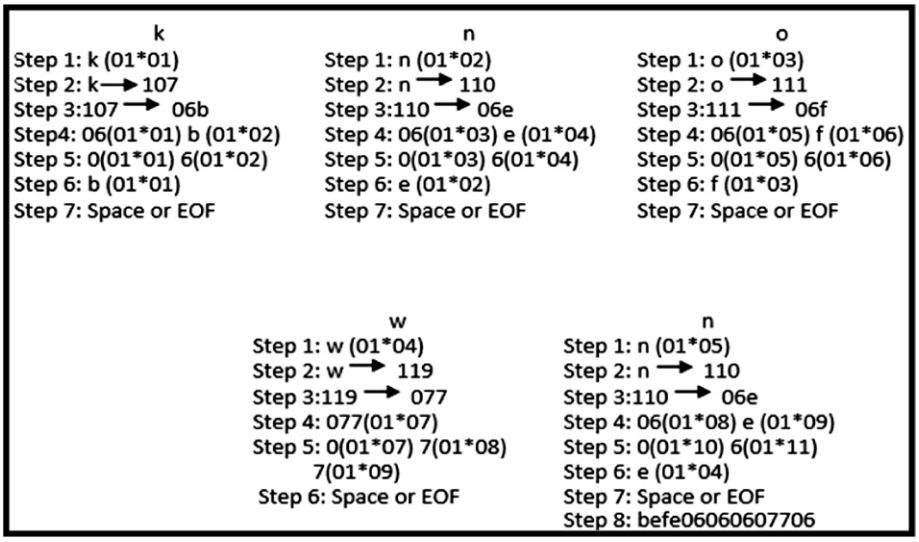

Fig. 4. Encryption Process Example

B. Decryption

We have stored the customer information in an image using our proposed algorithm and this image is stored on cloud. When customer needs its important data which is stored in the form of image on the cloud, cloud does some work, verifies the customer and its requirement. It selects the required image and sends it to the client or customer.

Here CDM uses two types of keys to decrypt it; first type is shared keys which are used for both

encryption and decryption while second type is private. The private key is used to identify the required pixel from where decryption process starts.

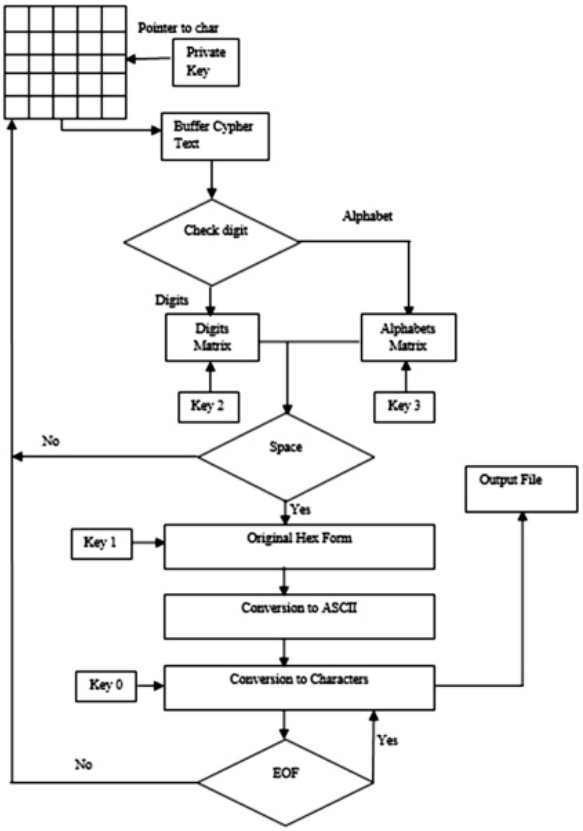

Fig. 5. Decryption Process Example

After getting the cypher text, the alphabets are placed on their positions in the alphabets matrix using key 3. Same process will be done for digits until it encounters space. Original HEX form is obtained using key 1 and decryption of HEX to ASCII is done. If some 3-bit HEX digits cannot be converted into ASCII then they are moved as it is into ASCII file because they are special characters. Then these ASCII characters are converted into original text and their positions are obtained using key 0. This process continues until the EOF. This decryption process of the image is described diagrammatically in the Fig. 5.

Cypher Text: **befe06060607706**

Private Key: Pixel Location of Image Let's say 072. 2 indicates 2nd column of the image pixel's coordination and 7 indicates 7th row of the image pixel's coordination. Using Key 3, 2 and 1, alphabet, digit and HEX matrix are generated. Conversion of three bit HEX data to ASCII and using key 0 original data is obtained.

Step1: b(01*01) e(01*02) f(01*03) e(01*04)
Step 2:0(01*01) 6(01*02) 0(01*03) 6(01*04) 0(01*05) 6(01*06) 0(01*07) 7(01*08) 7(01*09) 0(01*10) 6(01*11)
Step 3:06(01*01) b(01*02) 06(01*03) e(01*04) 06(01*05) f(01*06) 077(01*07) 06(01*08) e(01*09) 06b 06e 06f 077 06e.
Step 4: 107 110 111 119 110k(01*01) n(01*02) o(01*03) w(01*04) n(01*05)

Result: **known**

VI. Conclusion and Future Work

There are many deployment models which are used to provide services. These services are used within a limited boundary. Pay as you go model is used by cloud computing which provides services to the cloud customers. There is the need of high security to secure valuable data of customers, stored and maintained at the server. Many security measures are imposed over the data of customer to achieve maximum security and reliability. There are many levels of security and various security algorithms are used for security of sensitive data at the provider or cloud end but, they never ponder about the security methods in various layers existing between the customer and cloud. ASCII-HEX based steganography is implemented in order to achieve maximum security level and to overcome the problems of traditional algorithms. Encryption and decryption process of proposed algorithm uses two types of keys.Encryption and decryption process also have two phases to provide two cipher text; alphabets cipher and digits cipher. Alphabets and digits are generated from HEX values and these Hex values are generated using ASCII characters. These two types of ciphers are stored into image for storage purpose. Maximum security of the data at the customer's end is achieved by using CDM. After the customer's request of data, decryption process is performed at cloud end with the help of keys. Proposed algorithm's main goal to achieve maximum security of sensitive data with less complexity and processing. In future maximum reliability can be achieved using virtual images in this algorithm.

References

[i] Juan Camilo Corena, TomoakiOhtsuki, “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.

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

[iii] Chirag Modi , Dhiren Patel , Bhavesh Borisaniya, Avi Patel , MuttukrishnanRajarajan, "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.

[iv] 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.

[v] Binod Vaidya, DimitriosMakrakis, 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.

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

[vii] 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.

[viii] 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

[ix] CRYPTOGRAPHY, WEBSITE: HTTP://WWW.BARCODESINC.COM/ARTICLES/CRYPTOGRAPHY2.HTM [ACCESSED ON 5.12.14].

[x] Fundamental Security Concepts, http://cryptome.org/2013/09/infosec urity-cert.pdf,[Accessed on 11.9.14].

[xi] C. SARAVANAKUMAR,ARUN,"AN EFFICIENT ASCII-BCD BASED STEGANOGRAPHY FOR CLOUD SECURITY USING COMMON DEPLOYMENT MODEL", Www.jatit.org/volumes/Vol65No3/12Vol65No.3pdf, [Accessed on 11.11.14].

[xii] STEGANOGRAPHY, HTTP://EN.WIKIPEDIA.ORG/WIKI/STEGANOGRAPHY, [ACCESSED ON 31.11.14].

[xiii] Shareza Shirali, M.H, "A new Approach to persain/Arabic Text Steganography", Computer and Information Science, 2006, ICISCOMSAR 2006, Proc. 5th IEEE/ACIS International Conference, 10-12 July 2006 pp 310-315.

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

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

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

[xvii] Chandramouli, R., Kharrazi, M. &Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[xviii] Richard M. Thompson II, Cloud Computing: Constitutional and Statutory Privacy Protections, http://www.fas.org/sgp/crs/misc/R4 3015.pdf [Accessed on 11.12.14].

[xix] 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 11.12.14]

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

[xxi] "Video Steganography by LSB Substitution Using Different Polynomial Equations", A. Swathi, Dr. S. A. K Jilani, Proc. International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.

[xxii] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, Proc. IEEE Security Privacy Mag., 1 (3) (2003) 32-44.