JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Extended Information Hiding Procedure in Cloud Computing Environment using Random Security Codes

Arvind Kumar[1*], Ayush Gupta[2]

[1]Dept. of Computer Science, PCTI Group, New Delhi, India
[2]Dept. of Computer Science and Engineering, HMR Institute of Technology and Management, New Delhi, India

[*]*Corresponding Author:* *akdangi@gmail.com*, *Tel.: +0091-84700-03615*

DOI: https://doi.org/10.26438/ijcse/v7i4.848853 | Available online at: www.ijcseonline.org

Accepted: 16/Apr/2019, Published: 30/Apr/2019

***Abstract* –** Growth in the cloud computing evidenced in the recent past has accentuated the need for higher levels of security for obvious reasons. Various algorithms and techniques have been developed by the researchers to provide the security at multiple ends in multiple locations of the cloud data. The researchers have attempted to provide the security using various methodologies developed over time. However, there are frequent breaches of security in the recent times observed globally. Though the use of finger reference key in the security of data over the cryptography algorithm has enhanced the level of security, yet there are still loopholes in the framework providing opportunity for hackers for unauthorized access. In this paper, we propose a methodology to enhance the security by introducing the random security codes on the existing security framework. We establish that this procedure is more robust as compared to only using the finger reference key suggested by previous researchers and analysts.

Keywords - Cloud Computing, Random Security Code, Data Hiding

I. Introduction

Cloud Computing is an emerging technology that blends infrastructure, platforms, or applications that can be arranged and used through the internet. The infrastructure upon which cloud is built upon a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Based on the requirements and workloads, the services of cloud could be scaled dynamically. The payment mechanism for cloud services is based on the consumption and measurement of the resources utilized. Since cloud computing inherently involves a large number of users who store their personal data, the security of data is required on the storage media.

Data storage at cloud server has attracted an incredible amount of consideration or spotlight from different communities. In the year 2019, cloud revenue may touch 278.3 Billion US dollars according to Gartner Consulting. According to IDC estimates, public cloud revenue proportion of the total cloud revenue is expected to be around 66.3% and it may reach a level of 552 Billion US dollars in 2027. This massive growth of cloud services is coupled with a huge risk of a security according to the industry professionals and researchers.

The benefits brought by cloud storage – from scalability and accessibility to decreased IT overhead – are driving rapid adoption at enterprises around the world, and there are steps that companies should take to improve cloud storage security and keep sensitive data safe and secure in the cloud. It's a very convenient to tech user to store and access their data from any remote location or anytime (flexible availability of data) on any latest gadget which is capable cloud data access. Security is the major concern on cloud data storage at any IT related organization or concern security department. Today, all organizations and businesses use cloud services because it provides optimized cost, accessibility and customized services at local system. But running business on the trust of cloud storage base is critical on cloud means to compromise the confidential data files and sensitive information are coming into the new risks, as cloud-stored data residual outside of the range of many firewalls used to prevent sensitive data to be compromised held on-premise. As such, service providers must offer some add on measures to protect data at cloud storage beyond the fundamental protections given by providers. It is a fact that security and data protection are the main concerns for security professionals in moving to the cloud. In a recent study it has been established that the top concerns of the security professionals are–(a) protection against data loss, (b) threats to data privacy and (c) breaches of confidentiality.

In the recent past, we find a host of data breaches globally. Flaherty [1] has enumerated five major data breaches in 2018 viz. Facebook - leakage of a user's profile, Marriott - massive data breach affecting the records of up to 500 million customers, Quora – hacking of 100 million user's personal details, British Airways - cyber-attack on customer details, Ticketmaster - personal data of 40,000 customers was stolen by hackers. According to the recent report of PWC, India is vulnerable to security breaches in spite of the fact that businesses are keenly looking at innovative tools to protect themselves from cyber-attacks and threats. Siddhartha [2] envisages that cyber security trends in the Indian market would inter-alia include the use of machine learning, block chain algorithms and whether it is a business or individual or government, large investments and focus on security shall take place.

Cloud computing security needs, consider both technology and strategy, including: audit, compliance and risk assessment. According to Mudassir *et al.* [3], both the service providers and the clients must work together to ensure safety and security of cloud and data on clouds with a mutual understanding. Researchers have identified various issues concerning the security of cloud data. Of these issues we find a consensus on the issues like – (a) *Trust between the entities* - machine to machine, human to machine or machine to human like use of Gmail and Yahoo for securing important and confidential data, (b) *Fear of Anonymous (cryptanalyst) user* - authenticated person live the web who strikes on clouds data, (c) *Interceptor Intrusion* –hitting the traffic of the data over the cloud and forwarding on the cloud, (d) *Opportunism* – zeal to get restricted data, (e) *Malicious Action* of cloud service providers. In addition, data security in the cloud is the primary concern of the provider as well as used. Privacy measure to prevent the digitized data to protect from unauthorized access to nod sees associated with the data stores and many web based data storage. It also provides back up of data which help in recovery of the same data in case of failure.

We find that owing to several security issues, many organizations have ceased cloud computing fully. Various algorithms to protect the cloud data are in vogue and evolving continually. In spite of this fact, there is a dire need to evolve protection mechanisms for cloud data given the frequent cases of security breaches. Conventionally, a fair number of algorithms that have developed that primarily use a combination of cryptography and steganography techniques by the professionals and researchers. In an improved form, referenced figure key is merged with the crypto algorithm, but has proved to be inefficient because of data breaches as evidenced recently. In this paper, we are motivated to explore a further advancement of the security algorithm using the random security codes. The paper is organized as follows. In the introduction part (Section I) cloud computing and its related security risk have been described. Section II shows the major researches that have been conducted in the area of data security over the cloud and a gist of algorithms that have been used till recently are indicated. Section III shows the proposed procedure and results obtained followed by conclusion in Section IV.

II. Related Work

Security of data at rest in severs is the common topic of discussion among researchers. There are different mechanisms reported till date to ensure the security of data at rest and selection of any one of these for any particular system depends on various parameters like architecture of a system where security is to be enabled, the level of security required, amount of loss that may occur on loss of data and much more.

A review of various perspectives of cloud computing can be found in the literature like architecture and entities according to Nazir [4], cloud computing technologies Ashik *et al.* [5], data auditing and security in distributed computing as Geeta [6] defined. Kiran and Sharma [7] review of various data security techniques shows that none of the individual techniques are efficient, thus implying the need for a combination of different data security algorithms. The authors also express that the data classification is a futuristic approach that can reduce the user efforts in recognizing the category of data. Ibaida and Khalil [8] allows the ECG signal to hide its corresponding patient confidential data and other physiological information, thus guaranteeing the integration between ECG and the rest.

Ahmed and Hossain [9] present a sociological and a technological viewpoint of data security and establish that the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impacts. Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require to analyze the practicality in line with social, business, technical and legal perspectives – all these facets will incorporate security issues either in technical or strategic form.

Mudasir *et al.* [10] establish that simulation results of Apriori and Predictive Apriori algorithm are robust to secure data. Chang *et al.* [11] have constructed a recursive code that hides data over a special ternary cover suitable for any transform domain, such as DCT domain and density function of the transformed coefficients. According to Deepika [12] uses a technique in which randomly generated index values corresponds to the pixel values of picked image is sent on the cloud instead of actual data therefore it becomes very difficult to restore actual data without recognizing that what these bits and bytes actually point to. The control of the owner on the placement of data is a security challenge Hamlen *et al.* [13].Wid and Hashim[14] have proposed a new approach to secure data storage on cloud computing by hide secret English text file in cover English text file by generating a matrix of location. Lubacz [15], researcher discusses basic principles of network Steganography, which is a comparatively new research subject in the area of information hiding, followed by a concise overview and classification of network Steganography methods and techniques.

Vasilakos *et al.* [16] have proposed data-sharing scheme with edge servers that generate 256-bit secret keys for both data sharing and searching purposes. They used the key generation method in constant time of each secret key is 1.4 milliseconds. Arora*et al.* [17] have focused on the need of providing security by having a public key infrastructure (PKI) on each layer especially the security holes associated with Iaas implementation. Conventionally private and public key has been used to secure the cloud data according to Sugumar [18]. Wang learning based steganalysis/detection method to attack spatial domain least significant bit (LSB) matching Steganography in grey scale images, which is the antitype of many sophisticated Steganography methods according to Baowei [19]. Douglas *et al.* [20], Steganography techniques applied in the protection of biometric data in fingerprints. It is novel in that we also discuss the strengths and weaknesses of targeted and blind steganalysis strategies for breaking Steganography techniques.

In a malicious environment, the private key can be generated for each Steganographed image that can be obtained from the auditor by only authorized users according to Balaji and Newcastle [21]. Garg and Kaur [22] have proposed steganography of the text data into the image data obtained in the form of 2-D of 3-D images. The random embedding method has been utilized to embed the secret text data into the image data using MATLAB tool. The work of Babu *et al.* [23] shows an alternative to security improvement using steganography and machine learning through a morphing technique. To secure data on cloud environment, authors have used hybridized techniques that inter-alia includes DST, RSA and Blowfish cryptographic algorithms Shelly and Bawa [24]; Gowthami *et al.*, [25] and encryption using steganography and cryptography Gupta and Kumar [26]. Pawar and Korde [27] find that the cloud security is a fantastic enabler, but suffers from the inherent weakness of the tools that operate across that data in aggregate and lay emphasis on digital image steganography especially for cloud service providers. Various authors have proposed steganography to enhance the data storage security on cloud computing by hiding secret English text file in cover English text file via generating a matrix of location. Rahman *et al.* [28] have proposed a combination of the Blowfish encryption algorithm for encrypting the secret message and E-LSB for steganographic imaging. RSA can be used for digital signatures and steganography for data hiding in an image Abdulkarim [29]. In an interesting work of Porwal [30], three layers of security can be used for cloud data - stenography to hide data, cryptography to encrypt data and using biometric authentic key generation for data access. Wendzel [31] says that network Steganography and highlights its potential application for harmful purposes. Various security tools have also been suggested by authors like Dhivyaprabha *et al.* [32], Mishra *et al.* [33]. Yadav and Aggarwal [34] proposed a methodology whereby a file is placed on the single server, encrypted shares of the file are stored on different servers, and key used for encryption and decryption is the fingerprint's key of the sender. Because of the fact that fingerprints have zero collision property, data security is ensured.

We find that in the previous studies, the focus is on security of data only at the cloud end by applying of a variety of techniques that may not be sufficient to make the data secure at clouds.

III. Proposed Procedure and Results

After a careful examination of the previous researches and opinions of users and cloud service providers, we propose the use of security code generated by an algorithm. The steps followed in the proposed algorithm are as follows:

- In the *first step*, the data in required format that needs to be stored on the cloud is prepared.
- In the *second step*, processing of data takes place for ensuring data security on cloud storage by generating the finger reference key (finger print) of a user and then embedding fingerprint reference key with data.
- In the *third step*, we apply a random security code generated by specific logic to the fingerprint referenced data.

In our proposed procedure, the user of the data is required to follow the reverse process identical to the generation of secured data as enumerated in the above steps. This multi layering of data is difficult to the hacker or unauthorized person. Illustratively, if the any one of the reference key or random security code is wrong in the decoding procedure, it becomes impossible to access the data by anyone.

Using this methodology, we can secure our data on physical device as well as on clouds. The data can be multi-layered in secure manner available over the clouds which we can ensure by using the reverse process of storing the data over the cloud. In 99.99% of the cases it is the same because of the nearly zero collisions, property of finger reference key (Fingerprint) with irreducible random security code. We show the flowchart to explain our proposed procedure (Figure 1).

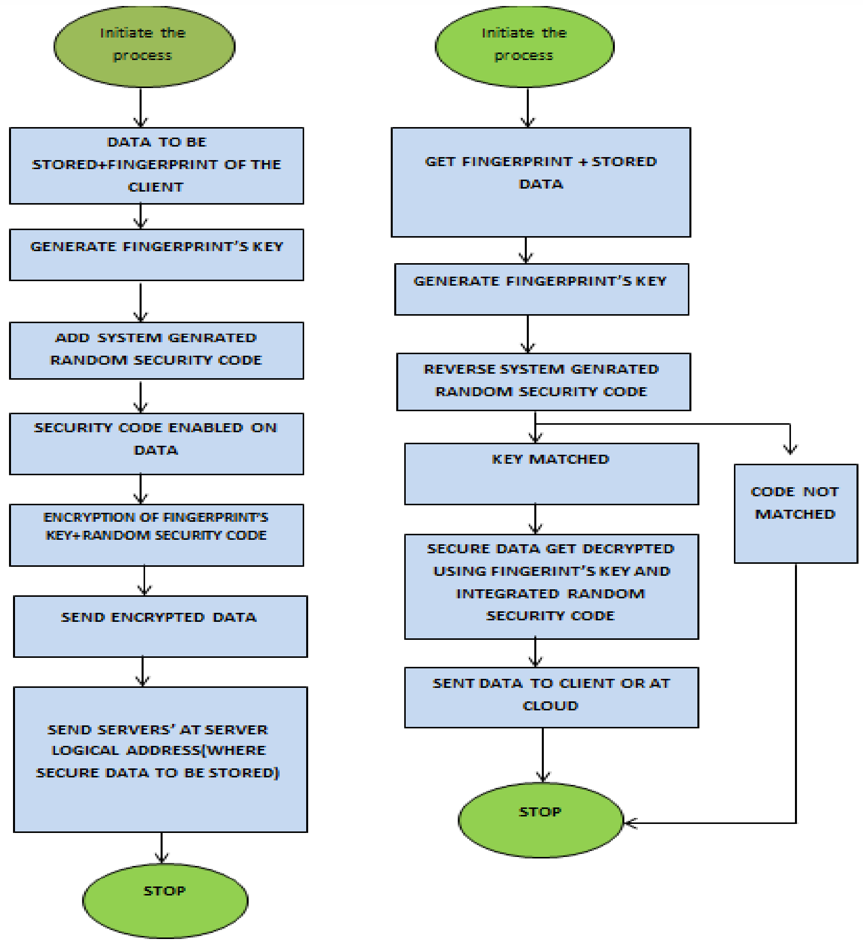
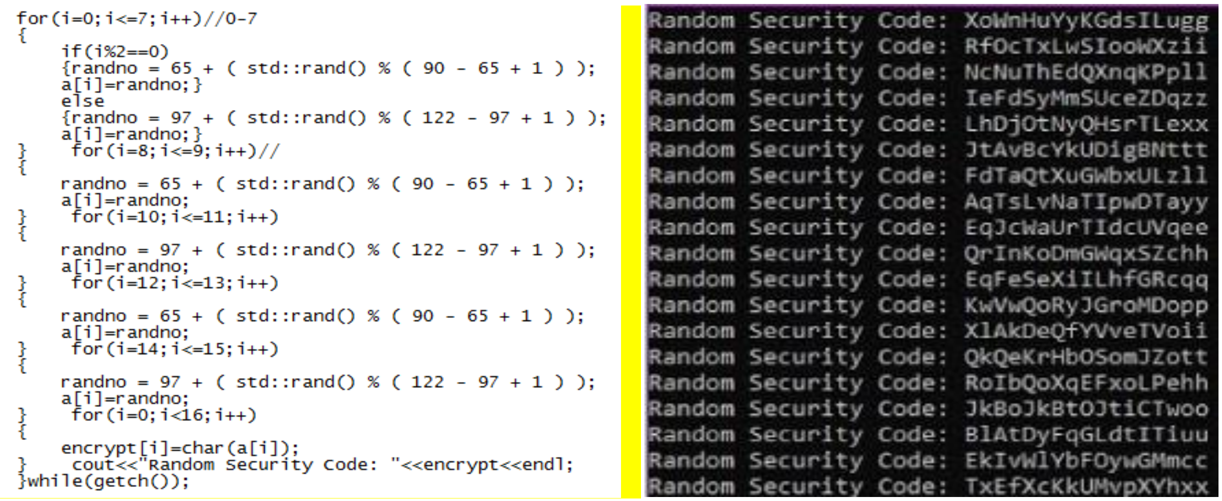

Initiate the process
DATA TO BE STORED+FINGERPRINT OF THE CLIENT
GENERATE FINGERPRINT'S KEY
ADD SYSTEM GENRATED RANDOM SECURITY CODE
SECURITY CODE ENABLED ON DATA
ENCRYPTION OF FINGERPRINT'S KEY+RANDOM SECURITY CODE
SEND ENCRYPTED DATA
SEND SERVERS' AT SERVER LOGICAL ADDRESS(WHERE SECURE DATA TO BE STORED)
STOP
Initiate the process
GET FINGERPRINT + STORED DATA
GENERATE FINGERPRINT'S KEY
REVERSE SYSTEM GENRATED RANDOM SECURITY CODE
KEY MATCHED
CODE NOT MATCHED
SECURE DATA GET DECRYPTED USING FINGERINT'S KEY AND INTEGRATED RANDOM SECURITY CODE
SENT DATA TO CLIENT OR AT CLOUD
STOP

Figure 1: Flowchart of the procedure

The proposed algorithm for embedding the security code is as follows (Figure 2).



```
for(i=0;i<=7;i++)//0-7
{
    if(i%2==0)
    {randno = 65 + ( std::rand() % ( 90 - 65 + 1 ) );
    a[i]=randno;}
    else
    {randno = 97 + ( std::rand() % ( 122 - 97 + 1 ) );
    a[i]=randno;}
}    for(i=8;i<=9;i++)//
{
    randno = 65 + ( std::rand() % ( 90 - 65 + 1 ) );
    a[i]=randno;
}    for(i=10;i<=11;i++)
{
    randno = 97 + ( std::rand() % ( 122 - 97 + 1 ) );
    a[i]=randno;
}    for(i=12;i<=13;i++)
{
    randno = 65 + ( std::rand() % ( 90 - 65 + 1 ) );
    a[i]=randno;
}    for(i=14;i<=15;i++)
{
    randno = 97 + ( std::rand() % ( 122 - 97 + 1 ) );
    a[i]=randno;
}    for(i=0;i<16;i++)
{
    encrypt[i]=char(a[i]);
}    cout<<"Random Security Code: "<<encrypt<<endl;
}while(getch());
```

```
Random Security Code: XoWnHuYyKGdsILugg
Random Security Code: RfOcTxLwSIooWXzii
Random Security Code: NcNuThEdQXnqKPpll
Random Security Code: IeFdSyMmSUceZDqzz
Random Security Code: LhDjOtNyQHsrTLexx
Random Security Code: JtAvBcYkUDigBNttt
Random Security Code: FdTaQtXuGWbxULzll
Random Security Code: AqTsLvNaTIpwDTayy
Random Security Code: EqJcWaUrTIdcUVqee
Random Security Code: QrInKoDmGWqxSZchh
Random Security Code: EqFeSeXiILhfGRcqq
Random Security Code: KwVwQoRyJGroMDopp
Random Security Code: XlAkDeQfYVveTVoii
Random Security Code: QkQeKrHbOSomJZott
Random Security Code: RoIbQoXqEFxoLPehh
Random Security Code: JkBoJkBtOJtiCTwoo
Random Security Code: BlAtDyFqGLdtITiuu
Random Security Code: EkIvWlYbFOywGMmcc
Random Security Code: TxEfXcKkUMvpXYhxx
```

Figure 2: Proposed Algorithm

The schemata of the security embedding random code procedure are shown in Figure 3.

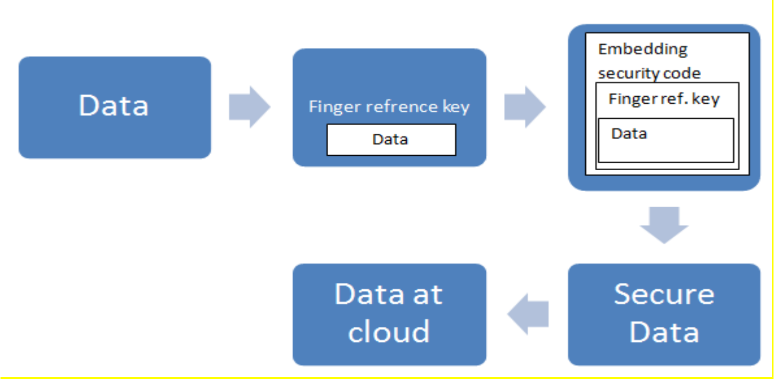


Figure 3: Schemata of embedding

The above figure presents the sequence of activities that are required to be performed to get the expected outcome as desired to be saved on cloud which can be accessed anywhere and anytime. The random security code on the data and finger reference key as combined in the manner -(((data)+finger reference key)) +random unique security code).

We establish that this procedure is robust as compared to only using the finger reference key as suggested by previous researchers and analysts. We illustrate the advantages of this procedure using an example of one of the world largest data storage–database of Unique Identification Authority of India popularly known "Aadhar Card". In 2018, there was a breach of UIDAI database known to be largest in the world. This breach reflects that the exclusive use of the finger reference key is vulnerable, thus pointing out the need for a more robust security framework. Use of a randomly generated security code as per proposed procedure can be more secure compared to the existing frameworks.

IV. Conclusion

Our proposed methodology is implemented in two folds – Data embedding with finger reference key and then the same data are embedded with random security which is generated by the programming or by logical code which every time generate the new combination of alphabetical letters. It is used like checksum value for both sender side and receiver side. This methodology helps in maintaining confidentiality and integrity of data at clouds. The property of proposed algorithm that makes it different from existing data storage techniques on clouds. This property may help in gaining more trust on the storage of data on clouds. There is scope for further enhancing the complexity of the algorithm to make the model more robust.

References

[1] Flaherty K.O., "*Breaking Down Five 2018 Breaches -- And What They Mean For Security In 2019*", Forbes Report, **2019**.

[2] Siddharth V., "*Seven Cyber security trends that India will witness in 2019*", PWC Report, **2018**.

[3] Mudasir Ahmed Muttoo, Pooja Ahlawat, " *A Secure Information Hiding Approach in Cloud Using LSB*", International Journal of Science and Research, Vol. **4**, Issue.,**7**, pp.**1171-1776**,**2013**.

[4] Nazir Mohsin, "*Cloud Computing: Overview & Current Research Challenges* ",IOSR Journal of Computer Engineering, Vol. **8**, Issue.,**1**, pp. **14-22**,**2012**.

[5] Ashik Mohamed M., Sankara Nayanan A., Nithyananda Kumari, "*Typical Security Measures Of Cloud Computing*",International Journal of Computer Trends and Technology, Vol. **5**, No.,**6**, pp.**299-304**, **2013**.

[6] Geeta C. M., RaghavendraS, RajkumarBuyya, Venugopal K R, S SIyengar, L M Patnaik,"*Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions*", International Journal of Computer, Vol. **28**, No.,**1**,pp.**8-57**, **2018**.

[7] Kiran, Sandeep Sharma, "*A Comparative Review Of Various Approaches To Ensure Data Security In Cloud Computing* ", International Journal of Engineering Research and General Science, Vol.**5**, Issue.,**2**, pp.**124-130**, **2017**.

[8] Ayman Ibaida, Ibrahim Khalil, "*Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems*" , IEEE Transactions on Biomedical Engineering ,Vol. **60** , Issue., **12**, pp.**3322-3330**, **2013**.

[9] Ahmed Monjur, Mohammad Ashraf Hossain,"*Cloud Computing and Security Issues in the Cloud*" International Journal of Network Security & Its Applications, Vol.**6**, No., **1**, pp.**25-36**,**2014**.

[10] Mudasir Ahmed Muttoo, Pooja Ahlawat," *A Secure Information Hiding Approach in Cloud Using LSB*", International Journal of Science and Research, Vol. **4**, Issue.,**7**, pp.**1171-1776**,**2013**.

[11] C.-C. Chang, C.-C. Lin, C.-S. Tseng, W.-L. Tai, "Reversible hiding in DCT-based compressed images", Information Sciences, Vol. **177**, Issue**.,** 1**3**, pp. **2768–2786**, **2007**.

[12] Deepika," *Enhancement of Data Security for Cloud Environment Using Cryptography and Steganography Technique*" International Journal of Innovative Research in Computer and Communication Engineering, Vol. **5**, Issue.,**1**, pp.**225-237**, **2017**.

[13] Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham," *Security Issues for Cloud Computing*", International Journal of Information Security and Privacy, Vol. **4**, Issue.,**2**, pp. **39-51**, **2010**.

[14] Wid A. Awadh, Ali S. Hashim," *Using Steganography for Secure Data Storage in Cloud Computing*", International Research Journal of Engineering and Technology, Vol. **4**, Issue., **4**, pp. **3668-3772**, **2017**.

[15] Lubacz Józef; Wojciech Mazurczyk ; Krzysztof Szczypiorski," Principles and overview of network steganography", INSPEC, Vol. **52** , Issue., **5** , pp. **225 – 229**,**2014**.

[16] Athanasios Vasilakos, Muhammad Baqer Mollah, Md. Abul Kalam Azad, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things", IEEE Cloud Computing, Vol. **4**, Issue.,**1**,pp. **34-43**, **2017**.

[17] Pankaj Arora, RubalChaudhry, Wadhawan Er. Satinder Pal Ahuja," *Cloud Computing Security Issues in Infrastructure as a Service*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.**2**, Issue.,**1**, **2012**.

[18] Ramalingam Sugumar, K. Arul Marie Joycee, "*FEDSACE: A Framework for Enhanced user Data Security algorithms in Cloud Computing Environment*", International Journal on Future Revolution in Computer Science & Communication Engineering, Vol. **4**, Issue., **3**, pp. **49-52**, **2018**.

[19] Baowei Wang,Zhihua Xia ,Xinhui Wang and Xingming Sun, "*Steganalysis of least significant bit matching using multi order differences*", Wiley online liabrary,2013; https://doi.org/10.1002/sec.864.

[20] Mandy Douglas, Karen Bailey, Mark Leeney, Kevin Curran," An overview of Steganography techniques applied to the protection of biometric data" July 2018, Volume 77, Issue 13, pp 17333–17373.

[21] Balaji. S, Mandy Sonio Newcastle,"*SECURE DATA TRANSMISSION BY STEGANOGRAPHY USING PRIVATE KEY IN CLOUD*" International Journal of Pure and Applied Mathematics,Vol. 119, No., 14, pp. 1653-1660, 2018.

[22] Nancy Garg, Kamalinder Kaur, "*Data Storage Security Using Steganography Techniques*", International Journal of Technical Research and Applications, Vol. **4**, Issue.,**6**, pp. **93-98**, **2016**.

[23] A. Mahesh Babu, G.A. Ramachandra, M. Suresh Babu, "*Implementation of Security in Cloud Systems Based using Encryption and Steganography*", International Journal of Electrical, Electronics and Computer Systems, Vol. **3**, Issue., **11**, **80-84**, **2015**.

[24] Shelly, Rajesh Kumar Bawa," *Secure Image Transmission for Cloud Storage System Using Hybrid Scheme*", International Journal of Engineering Research and Development, Vol. **11**, Issue., **9**, pp. **18-26**, **2015**.

[25] Gowthami Garikapati, Yakobu D, Gnaneswara Rao Nitta, Amudhavel J," *AN ANALYSIS OF CLOUD DATA SECURITY ISSUES AND MECHANISMS*", International Journal of Pure and Applied Mathematics, Vol. **116**, No. **6**, pp. **141-147**,**2017**.

[26] Ayush Gupta, Arvind Kumar, "*Information Security using the ensemble approach of Steganography and Cryptography*", in the proceedings of International Conference on Sustainable Computing in Science, Technology & Management, SUSCOM-2019, pp. **66-73, 2019,** http://dx.doi.org/10.2139/ssrn.3350895.

[27] Pramod Ambadas Rao Pawar, Aparna G. Korde, "*A Solution to Cloud Security: Image Steganography*", International Journal of Multidisciplinary Research, Vol. **2**, Issue. ,**2**, pp.**83-90**, **2016**.

[28] Mohammad Obaidur Rahman, Muhammad Kamal Hossen, Md. GolamMorsad, Animesh Chandra Roy, Md. Shahnur Azad Chowdhury, "*An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique* ", IJCSNS International Journal of Computer Science and Network Security, Vol. **18**, No.**9**, pp.**85-93**, **2018**.

[29] Adamu Ismail Abdulkarim, Boukari Souley, "*An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography*", International Journal of Scientific & Engineering Research, Vol. **8**, Issue.,**7**, pp. **1512-1517**, **2017**.

[30] Anuradha Porwal, "*Hybrid Protocol Employing Steganography &Cryptography for Cloud Storage Security*", International Journal of Advanced Research in Computer Science & Technology, Vol. **4**, Issue.,**2**, pp. **208-209**, **2016**.

[31] Steffen Wendzel, Wojciech Mazurczyk, Luca Caviglione, Michael Meier, "*Hidden and Uncontrolled – On the Emergence of Network Steganography Threats*", ISSE 2014 Securing Electronic Business Processes Conference Proceedings, pp. **123-133**.

[32] Dhivyaprabha E. , R. Madhubala, M. Abarna, "*Security Framework for Cloud Data Sharing*", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol.**3**,Issue.**3**, pp. **665-671**, **2018**.

[33] Mishra Ajeet , Umesh Kumar Lilhore, Nitesh Gupta, "*Review of Various Data Storage and Retrieval Method for Cloud Computing*", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol.**2**,Issue.**5**, pp. **584-588**, **2017**.

[34] Varsha Yadav, Preeti Aggarwal," Fingerprinting *Based Recursive Information Hiding Strategy in Cloud Computing Environment*", International Journal of Computer Science and Mobile Computing, Vol. **3**, Issue., **5**, pp. **702 – 707**, **2014**.

Authors Profile

Arvind Kumar is a Senior Faculty at PCTI institute affiliated from IGNOU, New Delhi and is also a research scholar at Centre for Management Studies, JMI University, New Delhi. He obtained his Master of Technology (Computer Science) from MDU, India and Master of Computer Applications from GGSIPU, New Delhi. Besides he holds a PG Diploma in Information Security from IGNOU, New Delhi and is a Microsoft Certified Technology Specialist (MCTS). He holds a PG Diploma in information security with Gold Medal. He is a renowned trainer and consultant on Cyber Investigation, Cyber Security, Ethical hacking and Network Security. He has handled various international e-learning projects and has delivered various training sessions and conducted various workshops on Information Security/Ethical Hacking to different organizations like Delhi Police, New Delhi, Central Bureau of Investigations, Government of India, Amazon.com etc. and has also presented papers in various national and international conferences.

Ayush Gupta is a student pursuing Bachelor of Computer Science and Engineering from HMR Institute of Management and Technology, New Delhi. He has presented papers in national and international conferences in the area of information and data security. His area of research interest is cryptography and information security.