REVERSE WATERMARKING TECHNIQUE TO ENHANCE CLOUD DATA SECURITY

Kapil Kumar[1] and Vikram Singh[2]

[1] M. Tech. CSE Scholar, Chaudhary Devi Lal University, Sirsa.

[1] Professor, Computer Science, Chaudhary Devi Lal University, Sirsa.

Abstract: The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. The existing technique of digital watermarking are also discussed here. Technique has been integrated. Along with the security of the data, it would be able to provide the comparatively analysis of the proposed mechanism with traditional mechanism.

Keywords: Cloud computing, Matlab, reverse watermarking, cloud security.

1. INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication (Guang 2019).

Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. While steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies (Singh 2013).

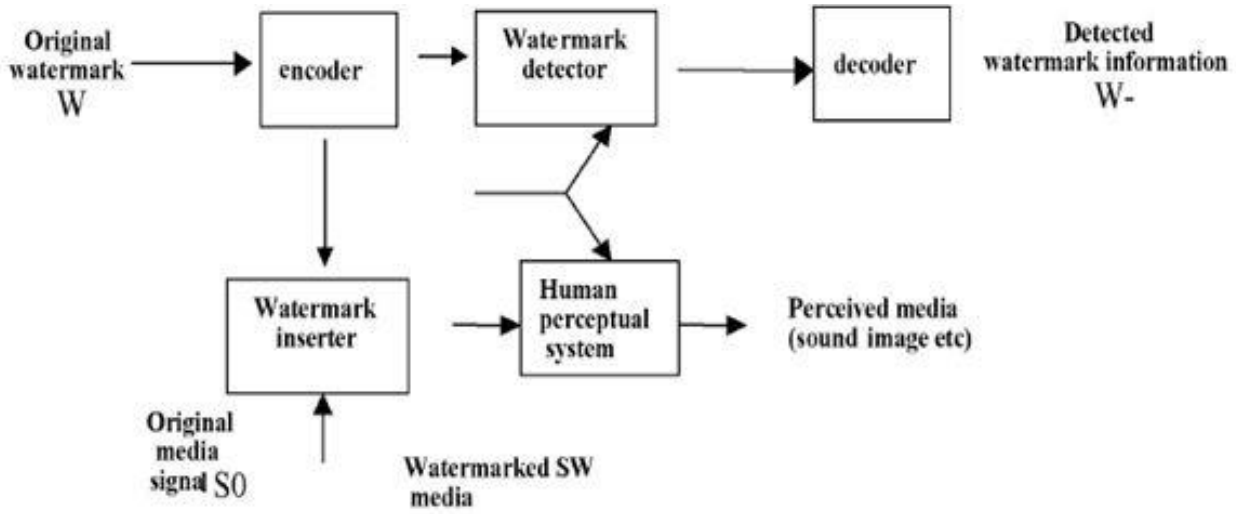

Figure 1. Digital Watermarking

1.1 Reverse Watermarking

Reversible watermarking techniques are also named as invertible or lossless and were born to be applied mainly in scenarios where the authenticity of a digital image has to be granted and the original content is peremptorily needed at the decoding side. It is important to point out that, initially, a high perceptual quality of the watermarked image was not a requirement due to the fact that the original one was recoverable and simple problems of overflow and underflow caused by the watermarking process were not taken into account too. Successively also, this aspect has been considered as basic to permit to the end user to operate on the watermarked image and to possibly decide to resort to the uncorrupted version in a second time if needed (Park 2017).

1.2 Cloud Data Security

System for cloud security is very useful in the condition of the perfect suspicious implementations. Cloud security systems which are efficient, recognize the hurdles in security management. It is the fact that such security management highlights such challenges along with security controls. Security of cloud computing, cloud security stands for the huge set of policies, techniques, apps, and controls. It has been used I order to secure the IP, data, apps. Along with this, the services as well as the associated systems are secured in cloud computing. It has been defined as a sub-domain related to computer security, network security etc. (Amalarethinam 2016).

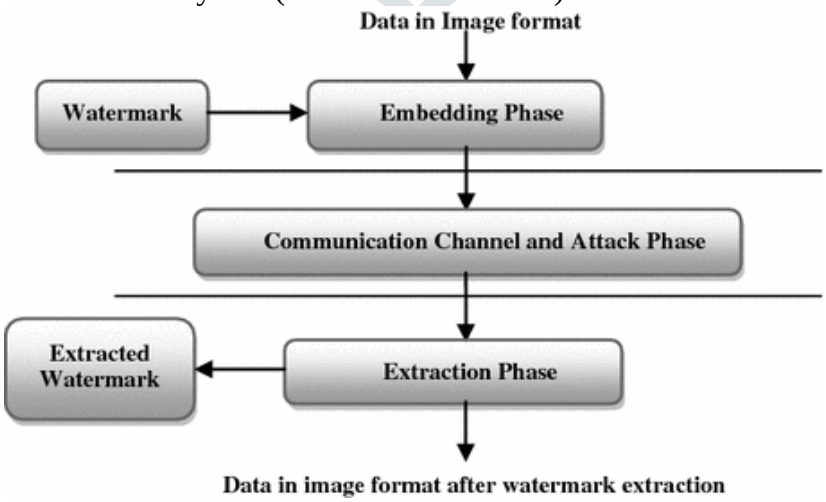

Figure 2. Attack in watermarking

2. RELATED WORKS

There have been several researches in field of reverse watermarking. Some of them have been discussed below:

Alattar (2003) provided the reversible watermark using the difference expansion of a generalized integer transform. A reversible watermarking algorithm with very high data hiding capacity has been developed for color images. Jensen (2009) has proposed technical security issues in cloud computing they presented a selection of issues of cloud computing security. They explored ongoing problem within application of XML Signature & Web Services security frameworks.

Lombardi (2010) proposed a Secure virtualization for cloud computing adoption & diffusion are threatened by unresolved security issues that affect both cloud provider & cloud user. Yu (2010) has proposed fine grained data access control in cloud computing. One challenge in this context is to achieve fine grain, data confidentiality, & scalability simultaneously, which is not provided by current work.

Reddy (2011) has proposed security problems at different levels of architecture of cloud computing services have been studied. Security of customer-related data is a substantial need for services which is provided by every model of cloud computing.

Iftikhar (2015) presented an effective & safe protocol by use ECC & Sobol sequence. This protocol provides integrity & confidentiality of data. Their system also supports active data operations that performed by client on data stored in cloud while maintaining same security assurance.

Padhym (2011) proposed on security issues & research challenges in this paper. Authors has been explain first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for cloud computing.

Mohammadi (2011) focused on protection of WSNs, separate it in four parts. They also consider them with the overview related to the WSNs. They also consider the security within WSNs. Threat model on wireless sensor network to attack of layer and comparison related to them. They allow the identification of purpose and capabilities consist by the attackers. In addition, they consider the objective and impact made by the link layer attacks has been explained.

Deshmukh (2012) wrote a paper. In this paper they have proposed a system which ensures data storage security using a distributed scheme. A set of Master servers are used which are responsible for processing users requests. Mathew (2012) explains of Implementation of Cloud Computing in Education. Author has explain main object to identify special of cloud computing which could be considered as a latest dawn to higher education & has full potential to make a revolution in field of education.

Kumar (2012) provide the discussion on system with the famous and well known platforms related to the cloud computing. They also addressed the hurdles with issues related to the cloud computing. Although they are numerous challenges with limitations, therefore there is the need of technique. It is the fact that the cloud computing is very attractive model. Especially it is very useful in huge enterprises. Proposal of cloud computing is able to make influence on business in two to three years. The cause is that potential for the important modification in IT consist by this technology.

Lee (2012) has proposed the Security Threats in Cloud Computing Environments. Clouds Computing can be define as growing field to study and for research work. They offered the security topic in the field of cloud computing. In the research work, they provided the analysis related to the cloud security issues. As well as, they also considered the treats and technical factors related to the Cloud Computing.

Gharibi (2012) wrote on advancement of latest technology related to the general and social websites. In particular they consider the innovative security threats. It is possible that current chances for the malicious users as well as the key loggers.

Singh (2013) has provided the research work on Techniques of Digital Watermarking. They provide the expansion related to the internet. It has been seen that the frequently enhancing to feasi of digital data such as audio, images and videos to the public.

Hashemi (2013) wrote a paper. In this paper he attempted to review & highlight security challenges, particularly security of data storage in a cloud environment.

Ni (2013) described the characteristics of DDoS attack; they propose a novel approach to detect DDoS attacks. They provide a review of the pattern to set all type of parameters in multiple apps adaptively.

3. ENHANCING CLOUD SECURITY USING REVERSE WATERMARKING

Invisible digital watermarking is comparatively new area of research; however it is useful and important and therefore quickly developed. This research is gives, first, a literature survey of existing digital watermark techniques; second, a practical implementation of some of methods described, third, testing the images with watermarks embedded for the purpose of analyzing different watermarks features.

The research has focused on Enhancement working of water marking System. Here we would perform all these using socket programming. Packet contains information about sender receiver, data and length of contents. We have to remove UN authentic data during data transmission to increase the performance of Intrusion detection system. To do this we would perform following tasks:

1. Establish a data transmission mechanism to send and receive packets using socket programming in java. Here we would use port number more than 1024 because these port are free to use.
2. To perform data transmission from client to server and server to client.
3. To trace the network route and detect the anomalies during data transmission
4. To verify the data packets during transmission and removal of anomalies.
5. To make the data secure using watermarking mechanism.

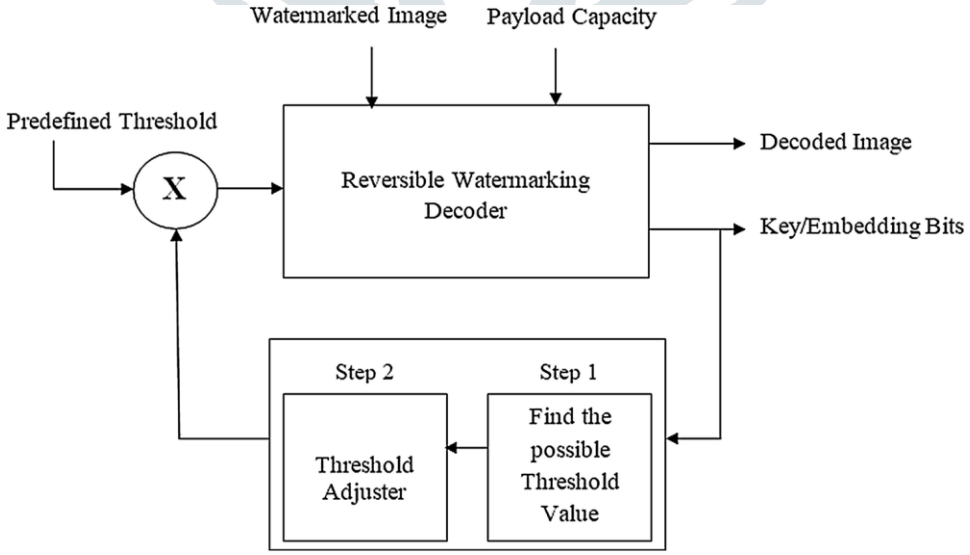

Figure 3. Reversible Watermarking Decoder

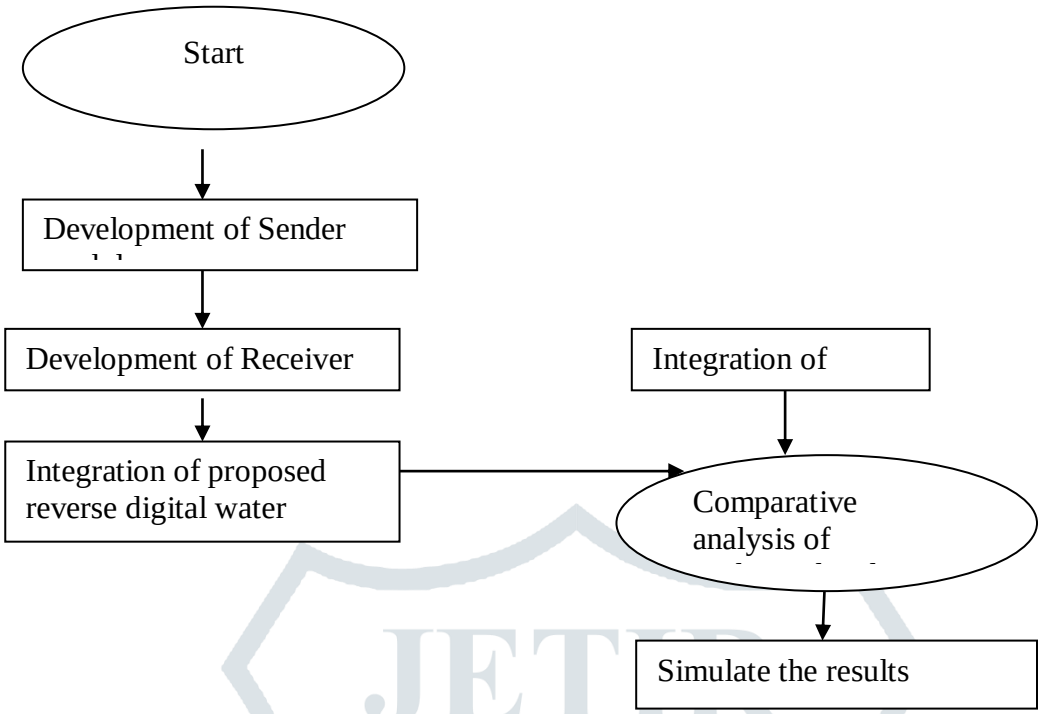

Figure 4. Process flow of research work

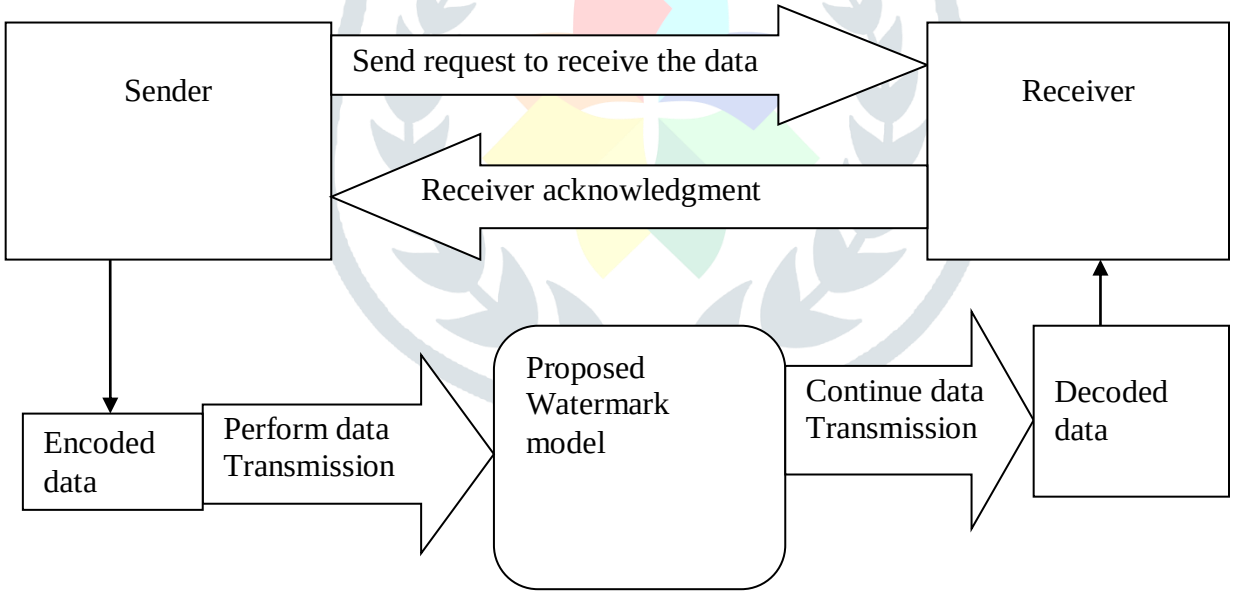

Figure 5. Proposed transmission model for water marking on cloud

4. SIMULATION EXPERIMENT

In the research work, the below given tools have been used.

Client server model: In client server model, it is feasible to possible to begin two network applications simultaneously. On the other hand, it is not practical to use it. Thus, it is necessary to design the communicating network app. Such will be used in order to execute the different operations of complementary network in sequence. It has been analyzed that server performs in starting, after that

it waits for receiving. The client performs secondly and transfers the network packet to the server. After the starting contact, the client along with server can send and receive the data.

Ip4 addresses: The length of IP4 addresses are thirty two bits. Generally, these addresses have been indicated as dotted decimal notation. Each byte making the thirty two addresses has been expressed as an integer value. This integer value may be 0 to 255. Such values have been differentiated using a dot. 138.23.44.2 Can be given as an example of an IP4 address. It is in dotted decimal notation. Conversion functions are there that able to change a thirty two bit address in dotted decimal string as well as vice versa.

Port: Internet address, end-to-end protocol and also port no uniquely identified the sockets. When a socket has been generated initially, it is necessary to make sure that it matches to valid IP address as well as to a valid port number. Basically in labs, TCP sockets have been applied. Ports perform as software which objects to multiplex input among several app. Here it is possible to consider a user performing an ftp client, a telnet client. Here the web browser can be performed concurrently.

Java socket programming: Java Socket programming is applicable in communication of applications. Such apps are performing on different JRE. Java Socket programming may be two types such as connection-oriented or may be connection-less.
Socket has been used in connection-oriented socket programming. On the other hand, Datagram Socket is applicable in connection-less socket programming.

Matlab: It is a simulation tool. It has been known as a high-performance language. It has been used in technical computing. It is able to integrate the computation, visualization and programming within easy-to-use system. In this system, the problems and their solutions have been denoted in mathematical notation which is familiar. Matlab is the combination of Math and computation.
Simulation has been carried out in Matlab and in order to implement the simulation the following Matlab based code has been written.

Pseudocode representing reverse watermarking

i. Reversible digital image watermarking using triangular number generator functions
ii. Dimensions of Images using following steps:
iii. Preserve msb of watermark using following steps:
iv. Extracts the lsb of cover image using following steps:
v. Preserves the msb of cover image using following steps:
vi. Divide LSB of cover and shifted msb by 4 using following steps:
vii. Add wmark to cover using following steps:
viii. Preserve the msb of wmi image using following steps:
ix. **P**reserve the lsb of wmi image using following steps:
x. Generate the matrix of lsb_covr combined with msb_wm using following steps:
xi. Determine the sum of the 2 numbers using following steps:
xii. Determine lsb of cover using following step:
xiii. Extract the watermark using following steps:
xiv. Regenerating cover image using following steps:

5. RESULT AND DISCUSSION

Results of the research experiment performed in Matlab has been discussed in this section.

Figure 6. The cover Image

The watermark image has been represented in figure 7.

Figure 7. Water mark

The image in figure 8 is representing the MSB of watermark.

Figure 8. MSB of watermark

Figure 9 is representing the output after shifting watermark

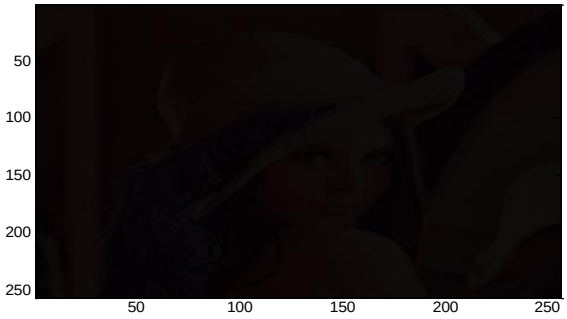

Figure 9. Shifted watermark

Figure 10. is representing the output after applying LSB of cover

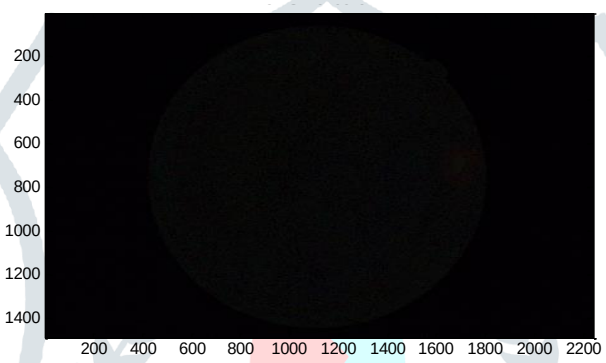

Figure 10. LSB of cover

Table 1. Comparison of Tradition work with Proposed Work

Traditional work	**Proposed work**
Limited security	More secure
Degraded performance	Better performance
Lack of flexibility	More flexible
Could be applied on limited image types	Applicable on mostly all type images
Lack of reliability	More reliable

By the comparative analysis, it has been come to know that the proposed work is better than all existing techniques. The proposed model based on digital watermarking provides better security than the existing techniques. It is able to apply on all type of graphical content whereas it was not possible with the traditional techniques. The proposed model provides more reliability and more efficiency in performance.

6. CONCLUSION

In the research work the development of packet sender & receiver module has been made. Invisible watermarking techniques hide some specific copyright, authentication, or other information inside the image for author's identification to protect author's right and restrict the intruder's ability of unlimited

copying and unauthorized using the information. Also, these watermarks might add some other important information. In the research work two technology, reverse watermarking and Steganography has been used to secure the cloud data. Along with the security of the data, it the comparatively analysis of the proposed mechanism with traditional mechanism has been made. In the research work the development of packet sender & receiver module has been made. The research work would be capable to provide the security as in the proposed work the reverse watermarking technique has been integrated. The research work would be better than the existing researches.

REFERENCES

Guang S., Xiaoping, J. Wangdong, L. Fenghua, and J. Yuewei, "Obfuscation-Based Watermarking for Mobile Service Application Copyright Protection in the Cloud," IEEE Access, vol. 7, pp. 38162–38167, 2019.

Zhang, L. Wu, S. Xiao, and S. Gao, "Adaptive reversible image watermarking algorithm based on IWT and level set," 2017.

Alattar A.M., "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," 2003.

Park J., "Non-fragile High quality Reversible Watermarking for Compressed PNG image format using Haar Wavelet Transforms and Constraint Difference Expansions," vol. 12, no. 5, pp. 582–590, 2017.

Singh P. and Chadha, "Review on Digital Watermarking Techniques Apps and Attacks," vol. 2, no. 9, pp. 165–175, 2013.

Iftikhar, Kamran M., and Z. Anwar, "RRW - A Robust and Reversible Watermarking Technique for Relational Data," pp. 1–14, 2015.

Coltuc, "Reversible Watermarking," no. 2003, pp. 7280–7282, 2015.

Meiko Jensen, Jorg Schwenk (2009) On Technical Security challanges in Cloud Computing 2009 IEEE International Conference on Cloud Computing.

Flavio Lombardi a, Roberto DiPietro (2010) protected virtualization for cloud computing Journal of Network and Computer Applications.

Shucheng Yu, Cong Wang, (2010) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, IEEE Communications Society subject matter experts for publication in IEEE INFOCOM 2010.

Reddy K., Dr. L.S.S.Reddy, "Security Architecture of Cloud Computing", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

Kumar P.S. and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011. Rabi Prasad Padhy Manas Ranjan Patra Cloud Computing: Security Issues and Research Challenges International Journal of Computer Science and Information Technology and Security (IJCSITS) Vol. 1, No. 2, December 2011.

Shahriar Mohammadi, Reza Ebrahimi Atani, (2011) A Comparison of Link Layer Attacks on Wireless Sensor Networks Journal of Information Security, 2011

Punyada M. Deshmukh, Achyut S. Gughane, Priyanka L. Hasija, Supriya P. Katpale, "Maintaining File Storage Security in Cloud Computing", International Journal of Emerging TechnologyandAdvanced Engineering, Volume 2, Issue 10, October 2012.

Mathew S.(2012) Implementation of Cloud Computing in Education – A Revolution International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012

Kumar S. and Goudar (2012) Cloud Computing Research Issues, Challenges, Architecture, Platforms and Apps: Review, International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

Lee K. (2012), "Security challenges in Cloud Computing system" International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012

Gharibi W. and (2012) Cyber threats in social networking websites, International Journal of Distributed & Parallel Systems (IJDPS) Vol.3, No.1, January 2012

Hashemi S, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.

Ni, Xiaoqing Gu, Hongyuan Wang, & Yu Li (2013) Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis, Journal of Control Science & Engineering Volume 2013,

Dai, QiuWang, Dong Li, (2013) On Eavesdropping Attacks in WSNs with Directional Antennas, International Journal of Distributed Sensor Networks Volume 2013,

Verma A.,Singh A., An Approach to Detect Packets applying Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.3, June 2013

Sharmin Rashid, Subhra Prosun Paul (2013) Proposed method of IP Spoofing Detection as well as the Prevention, International Journal of Science and Research (IJSR), Volume 2 Issue 8, August 2013.

Mukesh Barapatre, (2013) A Review on Spoofing Attack Detection in WAN, International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013

Sudhansu Ranjan Lenka, Biswaranjan Nayak," Increasing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014.

Swarnalata Bollavarapuand Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

Salah H. Abbdal, Hai Jin, DeqingZou, Ali A. Yassin, "Secure and Efficient Data Integrity Based on Iris Features in Cloud Computing", 7th International Conference on Security Technology, © 2014 IEEE.

Gajender Pal," A Review Paper on Cloud computing international journal for research in applied science and engineering technology", Vol. 2 Issue IX, September 2014.

S. Venkata Krishna Kumar, S.Padmapriya, "A Survey on Cloud Computing Security Threats and Vulnerabilities international journal of innovative research in electrical, electronics, instrumentation and control engineering", Vol. 2, Issue 1, January 2014.

Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud computing and security issues in cloud International Journal of Network Security and Its Applications (IJNSA)", Vol.6, No.1, January 2014.

Suraj R. Pardeshi, Vikul J. Pawar, "Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques", 2014.

E. Chandanapriya ,"Effective Data Sharing using Advanced Ring Signature with Forward Security",2014.

Singh, "A review of cloud computing security issues International Journal of Advances in Engineering and Technology", June, 2015.

Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil,"Cloud Computing – A market Perspective and Research Directions", I.J. Information Technology and Computer Science, 2015

Kumar R., " Research on Cloud Computing Security Threats using Data Transmission" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015. ISSN: 2277 128X

Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.

Babitha. M. P, K.R. RemeshBabu, "Secure Cloud Storage Using AES Encryption", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), ©2016 IEEE.

Aaron Zimba, Chen Hongsong, Wang Zhaoshun," An Integrated State Transition-Boolean Logic Model for Security Analysis in Cloud Computing", First IEEE International Conference on Computer Communication and Internet.2016.

D. I. G. Amalarethinam, "Data Security increment in Public Cloud Storage applying Data Obfuscation with Steganography," 2016.

Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. Kailash D. Kharat, "Enhancing Information Security in Cloud Computing Environment applying Cryptographic Techniques" 2017.