REVERSE WATERMARKING IN CLOUD SECURITY: A REVIEW

Kapil Kumar[1] and Vikram Singh[2]

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

Abstract: There are several researches related to reverse watermarking which are discussed here. Digital watermarking applicable in relational databases is developed as a candidate solution. It has been used and efficient to provide the copyright protection. This technology is able to deal with tamper detection, traitor tracing. It is suitable to maintain the integrity related to the relational data. Here in this work, packet sender module with receiver module is discussed. It has been analyzed that the proposed integration of reverse watermarking technique is efficient for the security of system. In the research work, along with the security of data, the comparatively analysis is also provided. This comparison is between proposed model and traditional mechanism.

Keywords: Cloud computing, Digital Watermarking, Reverse Watermarking

1. INTRODUCTION

It is well know thing that for the cloud services the user are required to pay according to use. Operators on internet would be able to get remote applications as utilities. Cloud computing is offering online development tools. Operator can modify & configure application online any time. Operators has been provided platform independent availability of cloud resources which would be available over internet. Cloud computing is offering on-demand self-services& there is no necessity of interaction with cloud-based service provider. Cloud computing usually works at high efficiency. It is not going to optimum utilization thus it is cost effective highly. Cloud computing is more reliable due to Load Balancing feature. Cloud computing has feature of Load Balancing that indicates its reliability (Jensen, M. 2009)

1.1 Cloud computing

It is a mechanism which provides many types of facilities that is more usable for us to transfer the data or any other information. It is the delivery of computing services. Various services are servers, storage, database, software, networking and analytics over the network. Many Companies are offering these computing services. Such companies are called cloud service providers. They typically charge for cloud computing services based on usage. It is similar to how one user billed for water or electricity at home. Cloud computing provides several benefits and they are listed here. (Lombardi, 2010)

1.2 Digital Watermarking

A digital watermark has been known as marker. It has been covertly embedded in a noise-tolerant signal. For example signal may be audio, video or image data. It is specially applied for identification of ownership of this signal. It has been analyzed that Watermarking can be define

as a process used to hide the digital data in a carrier signal. The hidden data does not require a relation to carrier signal. Digital watermarking is able and used to confirm the authenticity. This technique has been used for the integrity of the carrier signal.

Usually the electronic watermarks are become visible after the usage of some method. In cases where the carrier wave are deforms by electronic watermark in a way which can be easily identified, they are less useful depending on its intention. It is possible to use conventional watermarks to detectable means such as pictures. In comparison to this in electronic watermarking, the signal may be a recording, image, written file as well as a three dimensional models. A signal has the ability due to which it can keep separate watermarks simultaneously.

On the basis of application for which electronic watermark is used, its necessary features are calculated. In application like recognizing of media document which contains transcript details, it essential that electronic watermark must be very strong with regard to changes which are implemented to the carrier signal. On the other hand in application where continuity of service is required it is essential to use vulnerable watermark. Similar to steganography inferential method are used in electronic watermarking. Due to this method information are secretly implanted in noisy signals. In comparison to steganography which is employed for imperceptibility to human senses, electronic watermarking tries to manage the strength as top priority. Since a digital copy of data is the same as the original document electronic watermarking is an idle safety device. It simply recognized records. It does not deteriorate it or control access to the data.

It is highly used in a field where monitoring of resources is required. In order to achieve this it is implanted inside an electronic signal at all the sharing point. In situation where replica of work is came in to notice in the later stage it is possible to retrieved watermark from the replica and its source of sharing is recognized. This method is used to stop piracy of movies.

.

Watermarking For Relational Databases

Digital watermarking used in relational databases is growing as a candidate solution. It has been used and efficient to provide the copyright protection. This technology is able to deal with tamper detection, traitor tracing. It is suitable to maintain the integrity related to the relational data. Several watermarking techniques are there, proposed in the past. It has been done to address such objectives. They provided the survey related to the present state-of-the-art. They also discussed the different techniques as per the purpose. (Singh, P. 2013)

1.3 Reverse Watermarking

The methods of reversible watermarking are also known from its second name which is invertible. It was introduced so that it can be used in conditions where the accuracy of electronic pictures is necessary and the real substance is required on the decryption side. It is highly essential to highlight that, in the beginning, a highly visible class of watermarked pictures was not necessary because it is possible to retrieve to the initial pictures and the overflow and underflow type of challenges created via watermarking methods were not considered 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)

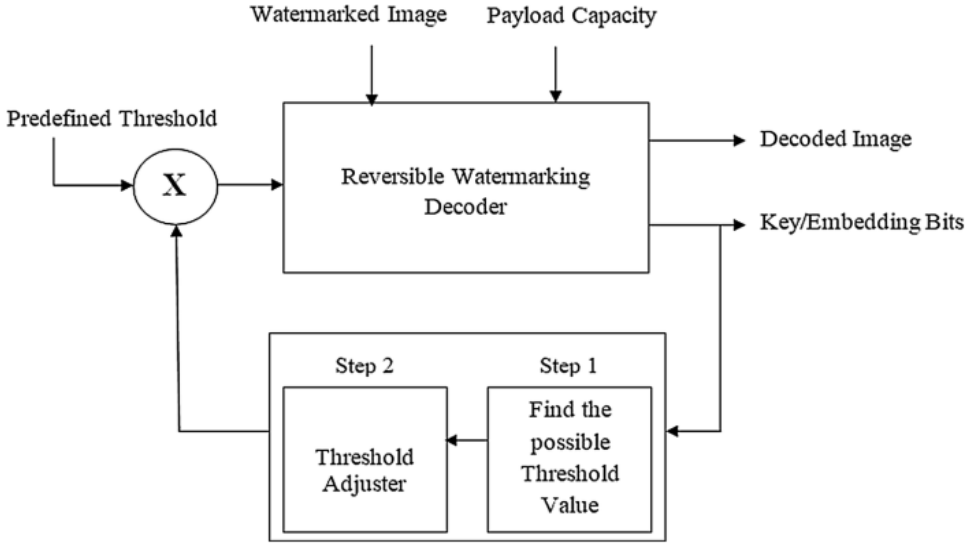

Figure1. Reverse Watermarking

2. RELATED WORKS

This section has summarised various researches related to the reverse watermarking in cloud data security.

Alattar (2003) has discussed the reversible watermark on the basis of difference expansion of a comprehensive integer transform. A reversible watermarking method which can conceal huge amount of information was introduced for color images.

Jensen (2009) has submitted the professional safety challenges in cloud computing. He described selected challenges of cloud computing security.

Lombardi (2010) anticipated a safe technology for the application and distribution of cloud computing. He also said that safety problems which remain undetermined can make a huge impact on both cloud supplier as well as its client.

Yu (2010) has discussed management of delicate information in cloud computing. The major problem from this point of view is the collection of delicate information secretly and responsibly simultaneously. It is not offered by existing research.

Reddy (2011) described safety challenges at various stages of design. Protection of client details is the primary requirement in each and every services which is offered via all designs of cloud computing.
Kumar (2011) on the basis of ECC and Sobol string determined a useful and protected protocol. This protocol assured decency as well as privacy of data. They give support to ongoing information functions which are executed from user side on the information which are placed inside a cloud and it will provide similar type of safety assurance.

Padhym (2011) has measured safety and research problems. Writer described already mentioned separate designs of cloud computing and safety and research problems inside a cloud computing. Protection of client details is the primary requirement in each and every services which is offered via all designs of cloud computing.

Mohammadi (2011) concentrate on safety of WSNs, split them into four sections & would address them, It contains summary of WSNs, protection in WSNs, threat design on wireless sensor network to attack of layer and a correlation between them. Due to this one can become so much capable that he can easily recognize the purpose as well abilities of offenders. At the same time the objective and impact of link layer attacks on WSNs are also put forward.

Deshmukh (2012) submitted a report. In this report they introduce a design which ensures data storage security on the basis of a distributed scheme. A set of Master servers are used which are responsible for processing users requests.

Mathew (2012) illustrate the application of Cloud Computing in Education sector. Writer highlighted the essential things, so that one can easily recognized the importance of cloud computing. It is assumed that this is one of the latest beginning to higher education and it is so much capable that it can produce a revolution in education sector.

Kumar (2012) discussed the architecture & popular platforms of cloud computing. It also takes in to account the difficulties and problem of cloud computing in detail. Cloud computing has various loopholes and it requires fresh methods, but still it is very popular paradigm. With the adoption of Cloud Computing technology, businesses are highly influenced because of its abilities.

Lee (2012) described the possible safety dangers in the surroundings of Cloud Computing. Cloud Computing is is growing field where lot of research work is still required. In this paper they consider matters related to safety in terms of cloud computing on the basis of assessment of Cloud safety treats & engineering parts of Cloud Computing.

Gharibi (2012) put in to writing the growth of current technology. He also submitted that social networking sites would generate innovative safety hazards which provide new opportunities for malicious attacks and essential loggers.

Singh (2013) was put in to place method of electronic Watermarking for the very first time the Digital Watermarking Techniques. Due to the growth of the Internet, consumers can easily access electronic records such as recording, images and footage to the community.

Hashemi(2013) composed a report. In this report he tried to examine and outlined the problems which are associated with safety specially safety of information which is placed inside cloud surrounding.

Ni (2013) explained the features of DDoS attack. He introduced an innovative method for the identification of DDoS attacks. They put a lot of effort so that they can manage each and every parameter in separate application scenarios in a proper way.

Dai (2013) explored using directional antennas in wireless sensor networks to improve network security in terms of reducing eavesdropping probability. They has been explains to directional receiver in one hop network or some hop network could important reduce eavesdropping probability.

Verma(2013) has proposed an approach in order to capture the packets via packet sniffing. It consist of several negative aspects. On the other hand such negative factors are there. It has been analyzed that it is very helpful for packets sniffing.

Rashid (2013) described the use of IP spoofing. It has been considered as a method of attacking a network. It has been explained to get the unauthorized access. Here the detection and prevention related to technique of IP spoofing are considered.

Barapatre(2013) explained the data security into client-server communication. Therefore, true WLAN security has been defined as a game related to balancing acceptable risk and countermeasure to mitigate those risks.

Lenka(2014) wrote a paper. In the research work, they implemented a combination of RSA encryption with the digital signature method. It is easy in all kind of attack related to the cloud computing features.

Bollavarapu(2014) stated the data storage security system in cloud computing. This system use algorithms like RSA, ECC and RC4 to encrypt and decrypt the different techniques.

Iftikhar(2015) defined on a robust and reversible watermarking technique for relational data. Advanced IT is very useful to increase the role and use of IT systems comprise relational databases.

Zhang (2017) has proposed the adaptive reversible image watermarking algorithm. This algorithm is related to IWT as well as the level set. For the improvement of robustness, imperceptibility of reversible image watermarking has been considered. Anti-malicious extraction capability of watermarking, an adaptive reversible image watermarking algorithm has been considered. It is dependent on IWT as well as the level set has been proposed in the research work.

Park (2017) evaluated the non-fragile high quality reversible watermarking. It is very applicable in compressed PNG image format. For this Haar Wavelet Transforms as well as the Constraint Difference Expansions has been used.

Guang(2019) has proposed the research work on obfuscation-dependent watermarking. It has been used in mobile service application copyright security in the cloud. The contributions given by the cloud computing in the avoidance of software piracy are not similar.

3. A REVERSE WATERMARKING TECHNIQUES IN CLOUD SECURITY

Here the review of Reverse Watermarking Techniques has been presented such as:
In the research work, the researcher discussed the Reversible Watermark. For this they have used different expansion related to generalize Integer Transform. A reversible watermarking algorithm is developed. It is efficient to provide the capacity of data hiding. It has been done for color images. Additionally, for the maximization of amount of data the embedding algorithm can be applied. It is possible to hide the data into an image. Simulation results with the use of spatial triplets, spatial quads etc have been presented. Here the cross-color triplets as well as the cross-color quads have been offered. They also presented and provide the comparison within traditional reversible watermarking algorithms. Such results are indicating that spatial quad-based algorithm enable to hide the payload. It is at the highest SNR. (Alattar2003)

In this work, the researcher proposed an effective and safe protocol with the use of ECC and Sobol sequence. The protocol is able to offer the integrity with confidentiality related to the data. The system is able to support the active data operations. It is able to performing the client on data which is stored in cloud at time of maintain the assurance of security. This protocol provides integrity & confidentiality of data.(Syam2011)

In the research work,the researcher proposed an concept in order to detect the packets via packet sniffing. It involves the negative aspects, on the other hand the negative aspects, it has been considered as very helpful in sniffing of packets.(Verma2013)

In the research, the researcher presented a report. In this report an integration of RSA encoded & electronic signature approach was implanted by them. It is similar to each and every type of cloud computing characteristics. A three way protection is provided by this integration process. It means it provides information protection, authentication & identification. In this research work, RSA encoded approach for privacy of records & MD 5 approach for identification have been submitted by them. (Lenka 2014)

In the existing research, the researcher addressed a forceful and reversible watermarking procedure in relation to comparative information. The growth in the the field of computer science perform a vital function in the field of information systems which contain associative records. This type of method is normally not strong with regard to malicious attacks. It does not give any method due to which watermark basic features can be determined by considering its importance in knowledge recognition. As a result, reversible watermarking is needed which conform; (i) watermark encryption as well as their decryption by considering their function in the knowledge discovery; and, (ii) actual information recovery in the existence of dynamic malicious attacks. A strong and semi-blind reversible watermarking (RRW) method for mathematical associative records has been introduced in this work. It respond the above aims. Practical examination shows the usefulness of RRW with respect to spiteful assault. It represents that the method which are introduced in this work outperforms the method which are available at this moment. (Iftikhar2015)

On the basis of IWT and level set the researcher introduced a flexible reversible picture watermarking scheme in this research work. The main intention behind its invention is the recovery of forceful, concealment, and anti-malicious extraction ability of reversible pictures watermarking. In the beginning with the help of Laplace operator in conjunction to level set techniques the stable edge profile is extracted. After that the unit circle in the stable edge profile is calculated. At last, the inscribed square area of the determinate unit circle is split into non-overlapping blocks in an appropriate manner. Each and every sub-block works through IWT. The use of HVS is required for the implementation of watermark. It is represented through simulation outcomes that the approach has excellent invisibility and can withstand in the favor different attacks. This approach is very strong and lossless recovery of actual picture can be achieved (Zhang 2017)

In the work, on the basis of Haar Wavelet Transforms and Constraint Difference Expansions researcher evaluated the strong and excellent Reversible Watermarking for condensed PNG form of pictures. Different types of electronic techniques are formed for proper sharing of electronic documents with the help of Internet based approach. This approach contains lossy characteristics. In order to reduce the possibility of incurring such characteristics, an excellent reversible watermarking approach for lossless picture compression of PNG picture was introduced in this work. In this method, robustness with respect to unwanted outside attacks is taken into account for the utilization of physical world. The data to be hidden are binary, comprising zeros and ones, and the cover image is in the compressed PNG format with a size of 512 × 51 2 or 256 × 256. The proposed algorithm is based on a constraint difference expansion (DE) algorithm and discrete wavelet transforms (DWTs) with Haar filters for achieving both reversibility and robustness. They generate low visible distortions, e.g., Gaussian noise, in the image to demonstrate the robustness of the prosposed algorithm. The result shows that the proposed algorithm is robust against noise attacks within a specific range. (Park 2017)

In the research work, the researcher proposed the research work on Obfuscation-dependent Watermarking used in Mobile Service Application. It has been used for Copyright Protection in Cloud. The contributions of cloud computing to maintain the piracy of software are not same. The research work has navigated the mobile service apps. Method of modern is applied for the obfuscation the source code of apps. These methods are able to remove a part related to the

semantics. Such also add it in order to recover the module. The cause is that such obfuscation rules retrieved to watermarks. The watermarks are mapped into the rules. The recovery module is a recognizer to prove the watermarks when the original program is recovered. The experimental results indicate that the obfuscated code becomes difficult to reverse engineering and the watermarks are robust. (Guang 2019)

4. CONCLUSION

In conclusion, it has been analyzed that development of packet sender and receiver module is provided in the research work. The research work is able and efficient to provide the security because the reverse watermarking technique is used in the proposed work. It has been explained in the research work that Invisible watermarking techniques are used to hide copyright, authentication, etc in the graphical content. These are able to identify the author in order to secure the right of author. Along with this, it has been used to limit the ability of intruder. It is necessary to restrict the intruder because they can access the unlimited copying and can get the unauthorized data. Like steganography, watermarking is a relatively new area of computer science related to hiding information in a digital carrier. There are some similarities between steganography and watermarking.

Also, such watermarks can add different useful data. Here, in the research reverse watermarking has been integrated to steganography to secure the data of cloud. In the research work, along with the security of data, the comparatively analysis is also provided. This comparison is between proposed model and traditional mechanism.

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".