JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review on Privacy Protection for Cloud Based Online Transaction Using Steganography & Visual Cryptography.

[1]Vaishnavi S Kshirsagarr, [2] Prof. Namdev M. Sawant

[1]PG Student, [2]Assistant Professor,
[1]Department of Computer Science and Engineering,
[1]SKN Sinhgad College of Engineering, Korti, Pandharpur, Solapur University, India

Abstract: **now a days cloud computing important paradigm for IT industry with reduced cost, pay as you use, scalability ,easy accessibility and improved flexibility. In online transactions clients data can be accessed by other party which makes privacy and security issues. To ensure the privacy of data over cloud it is good outsource the data is in encrypted format .while sharing personal data with third party ,it should be fine-grained access control, security, data confidentiality, authorization and authentication is crucial challenge. At the time of uploading of personal data in the cloud the owner of data losses the physical control also it can be hacked by hackers. Hence the providing the security is a big issue while sharing personal data in cloud environment. This can be solved by using cryptography mechanism at the time of data sharing that will increase the confidentiality of the data and Steganography hide the data in another file for storing the data securely in the third party storage service. By making use of several encryption techniques user can store the data on cloud without worrying about the security.**

Keywords: Steganography, Cryptography, Stegoimage

I. Introduction

Cloud Computing is the one of the popular technology in IT world that provides various services to the user via Internet. Cloud system empowers the information sharing system which gives the variety of services to the user. According to the studies all the companies shares 74% of their information with the users as well as 64% of their information with the suppliers using cloud storage system. In this way sharing of data is the higher priority task which plays an important role in any organization by which the productivity in the cloud environment is increased. The shared cloud services are effectively available by the request network access service as well as it is adaptable which is accessible at lower cost. At the time of the sharing of information the personal information or data sharing assumes a fundamental part of the customer data is effortlessly open with least cost. In day to day life the personal record of the person is trading technology in applications that are utilized for generating, managing as well as modifying the personal data related to the person in very effective way. The personal records of the person has different data related to the applications such as identification sheet, issues, personal important transactions, progress notes, details of consultation, etc. Such data records must be stored on the cloud for the sharing as well as access mechanism that is utilized for controlling the activities of the person.

In the personal record, sharing of the data is fine-grained access control, security, data confidentiality, authorization and authentication is crucial challenge while sharing the personal records in the third party storage. At the time of uploading of personal data in the cloud the owner of data losses the physical control also it can be hacked by hackers. Hence the providing the security is a big issue while sharing personal data in cloud environment. This can be solved by using cryptography mechanism at the time of data sharing that will increase the confidentiality of the data and Steganography hide the data in another file for storing the data securely in the third party storage service. By making use of several encryption techniques user can store the data on cloud without worrying about the security. In the next segment we will go through some of the researches provided the different authors on Medical Data Sharing Systems.

STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the practice of hiding a file, message, image, video within another file. For the transmission of the message. Steganography is having key concept of transmitting the message cannot be detectable to casual eyes.text,video,audio are used to hide the data in Steganography in text Steganography message can be hide by shifting word. text Steganography is useful over others because it requires small memory.

Visual cryptography is cryptographic technique used for image encryption which is based on visual secret sharing. this technique uses k out of n (k,n) shares. secret image is encrypted in shares and forms another image which is meaningless. This image is transmitted over entrusted communication channel .only k shares or more gives the original secret image.

II. LITERATURE RIVIEW

In paper [1] author build up a novel health care system by utilizing the flexibility of cloudlet. The functions of cloudlet consist of privacy protection, data sharing and intrusion detection. In the stage of data collection, firstly utilize Number Theory Research Unit (NTRU) method to encrypt user as body data collected by wearable devices. Those data will be sending to nearby cloudlet in an energy efficient fashion. Secondly, present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps identical patients to communicate with each other about their diseases. Thirdly, divide users medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, design a novel collaborative Intrusion Detection System (IDS) method depend on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks.

In paper [2] author build up a novel in the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the customer from its bank account. A payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant’s side.

In paper [3], for the first time, define and solve the challenging issue of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). They establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, they choose the efficient similarity measure of “coordinate matching”, i.e., as many matches as possible, to capture the relevance of data documents to the search query. They further use “inner product similarity” to quantitatively evaluate such similarity measure. First propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough study of inspecting privacy and efficiency guarantees of proposed schemes is given.

In paper [4], author developed a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources involving computing power and energy can be opportunistically collected to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m healthcare emergency, They introduce an efficient user-centric privacy access control in SPOC framework, which is depend on an attribute-based access control and a new privacy preserving scalar product computation (PPSPC) technique, and permits a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security study display that the proposed SPOC framework can efficiently achieve user centric privacy access control in mHealthcare emergency.

This paper [5] first introduces the main aim of this special issue and gives a brief guideline. Then, the present situation of the adoption of EMRs is reviewed. After that, the emerging data technologies are presented which have a great impact on the healthcare provision. These include health sensing for medical data collection, medical data study and utilization for accurate detection and prediction. Next, cloud computing is discussed, as it may offer scalable and cost-effective delivery of healthcare services.

This paper [6] developed a practical solution for privacy preserving medical record sharing for cloud computing. On the basis of the classification of the attributes of medical records, they use vertical partition of medical dataset to achieve the consideration of distinct parts of medical information with different privacy concerns. It mainly consisting four components, i.e.,
(1) Vertical data partition for medical information publishing,
(2) Data combining for medical dataset accessing,
(3) Integrity checking, and
(4) Hybrid search across plaintext and cipher text, where the statistical analysis and cryptography are innovatively combined together to provide multiple paradigms of balance among medical data utilization and privacy protection. A prototype system for the huge scale medical data access and distributing is implemented. The usage of electronic health data from distinct sources for statistical analysis requires a toolset where the legal, security and privacy concerns have been taken into consideration. The health data are typically placed at different general practices and hospitals. The data analysis includes of local processing at these locations, and the locations become nodes in a computing graph. To support the legal, security and privacy concern.

The proposed [7] toolset for statistical study of health data uses a combination of secure multi-party computation (SMC) algorithms, symmetric and public key encryption, and public key infrastructure (PKI) with certificates and a certificate authority (CA). The proposed toolset should cover a wide range of data analysis with different data distributions. To accomplish this, huge set of possible SMC algorithms and computing graphs have to be supported.

In paper [8],author propose a priority based health data aggregation (PHDA) scheme with privacy preservation for cloud assisted WBANs to improve the aggregation efficiency between different types of health data. Specifically, first explore social spots to help forward health data and enable users to select the optimal relay according to their social ties. According to distinct data priorities, the adjustable forwarding methods can be selected to forward the user as health data to the cloud servers with the reasonable communication overheads. The security analysis describes that the PHDA can achieve identity and data privacy preservation, and resists the forgery attacks.

III. FLOW DIAGRAM

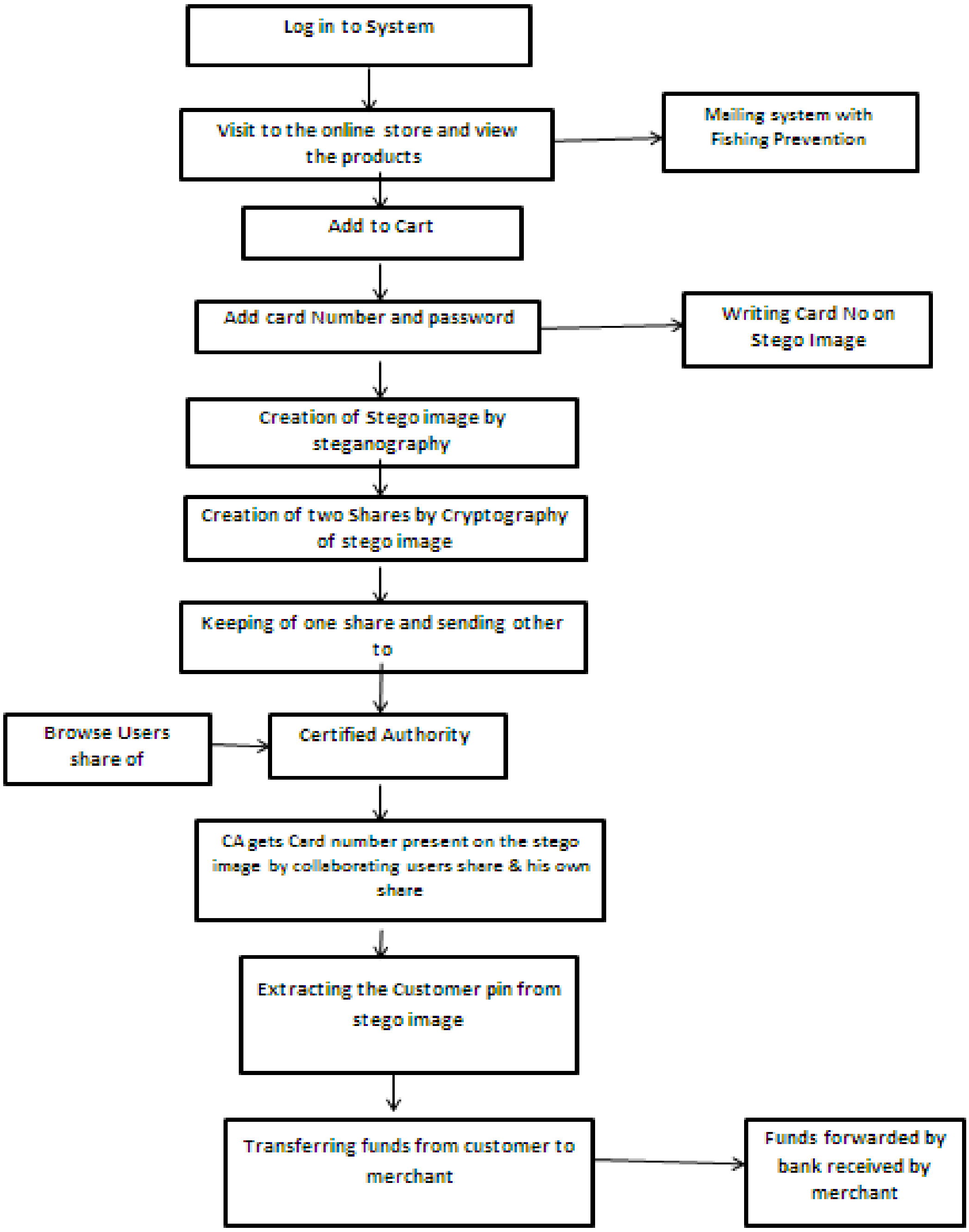
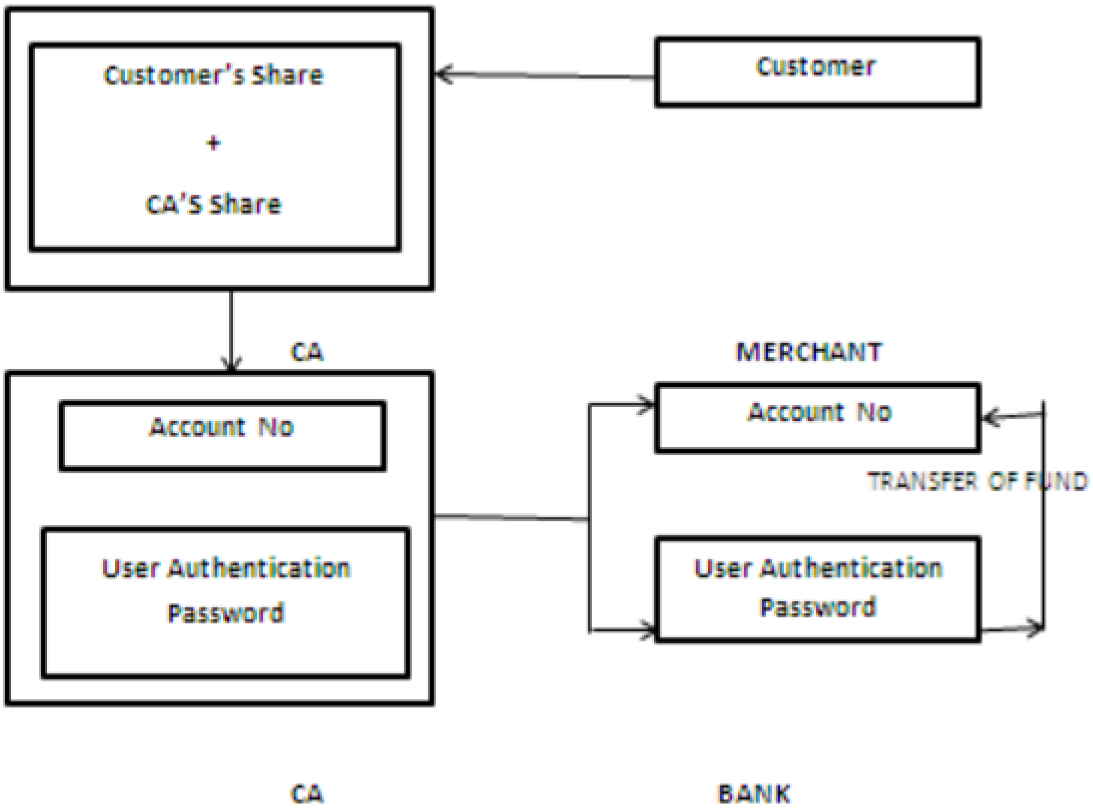

Log in to System
Visit to the online store and view the products
Mailing system with Fishing Prevention
Add to Cart
Add card Number and password
Writing Card No on Stego Image
Creation of Stego image by steganography
Creation of two Shares by Cryptography of stego image
Keeping of one share and sending other to
Browse Users share of
Certified Authority
CA gets Card number present on the stego image by collaborating users share & his own share
Extracting the Customer pin from stego image
Transferring funds from customer to merchant
Funds forwarded by bank received by merchant

Fig: Methodology



When you log in the online shopping website after adding the product you have to write the card number on stegoimage using Steganography technique after making the stegoimage make the two parts of that stegoimage by cryptographic technique one is for customer and second for certified authority. Now certified authority collaborates the stegoimage which is from his own share and another is from customer's share and extract the pin from stegoimage and transfers the fund from customer's account to merchant's and fund will be received by merchant.

In this method customer does not need to provide all the information to merchant ,there is certified authority which minimizes information sharing between customer and merchant. Two parts of stegoimage are distributed to customer and CA. after combining this images CA can get account no and password from the customer and did the transaction from customers account to merchants account and complete the transaction. By using this method the confidential information of customer is not accessed by the merchant and frauds in transactions can be avoided..

IV. CONCLUSION

Our review shows that, while sending the personal or important data through cloud there will be any third party attack occurs. By the combination of Steganography and visual cryptography we are providing secure transaction in online Data sharing System. It secures customer's confidential information at merchant side and hence prevents misuse of data. This method is mainly concerned with preventing identity theft and providing customer data security. It also prevents phishing. The system authenticates client as well as merchant server.

References

1. Souvik Roy1 and P. Venkateswaran "Secure Online Payment System using Steganography and Visual Cryptography" Jabalpur University, Kolkata-700032, India [2014]
2. Guangdong Xu,"Web Mining Techniques for Recommendation and   Personalization", Victoria University, Australia, March 2008.
3. Bashed Mobster "Data Mining for Web Personalization,", LCNS, Springer-Verleg Berlin Heidelberg, 2007.
4. Dr. R. Krishnamurthy and K. R. Sabetha," Identifying User Behavior by Analyzing Web Server Access Log File", International Journal of Computer Science and Network Security, April 2009.
5. Arya, S., and Silva, M.," A methodology for web usage mining and its applications to target group identification", Fuzzy sets and systems, 2004, pp.139-152.
6. R. Kosala, and H. Bloc keel," Web mining research: a Survey", SIGKDD Explorations, 2010, 2, pp.1-15. "Log files formats", http://www.w3c.org, Access Date: [5th of Dec, 2012-10 PM].
7. S. K. Pain, "Web Usage Mining: A Survey on Pattern Extraction from Web Logs", International Journal of Instrumentation, Control & Automation, January 2011.
8. Min Chen, Jing Chen Shiwen Mao `Privacy Protection and intrusion avoidance for cloudlet based medical data sharing` ,IEEE Transaction on cloud computing.