IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Usage of Water Marking-Based Techniques for Performing Necessary Operations on a Plaintext Image in the Cloud

Prof. Sudheer Shetty, Brijesh Reddy K H, Prenita Prinsal Saldanha
Department of Information Science and Engineering
Alva's Institute of Engineering and Technology, Mangalore, Karnataka, India

Abstract: *To provide the image with security multiple encryption techniques are used. This way the image is converted to a form in which it is not read by a third party unless they have the watermark which is known to only the user. Some cryptographic protocols have been constructed, the emergence of quantum computers and quantum algorithms presents a problematic scenario for those protocols. Data-driven and Feedback-Enhanced Trust (DFET) is developed due to the multi cloud environment created by the multiple data centers. A method for quantum picture watermarking is provided to blend a grayscale quantum watermark into a quantum carrier image.Multiple image search protocols are used in which the image is searched based on their specialities. for example, Content-Based Image Retrieval (CBIR), Convolutional Neural Network (CNN). scale-invariant feature transform (SIFT) approach for encrypted images that protects privacy. PRISMA checklist in addition to a few components of the Cochrane Quality Assessment. social media and gaming applications have been widely adopted by the general public and the number of social media and gaming applications has increased, with the help of white hacking it has established a security technique, stealth robot conceals itself from the intended target/victim by using stealth tactics. Making it easier for protection.*

Keywords: Cloud

I. INTRODUCTION

In every single website image uploading is present and that is very common in applications like Facebook, WeChat, Instagram and so on and so forth. So the privacy and protection of these images is a very important measure to handle. Nowadays the cloud has been a very important source in every field, be it for storage or for processing. So in this paper we are discussing the Storage, display, erasing and retrieval of the image uploaded in the cloud using the many individual watermarking based protocols. the owners' submitted pictures can have private data, like an In order to protect privacy information, image owners erase the posted images from social media networks. Unfortunately, as cloud service providers retain several backups of data across different online or offline servers for fault tolerance, it is challenging for the picture owners to totally delete submitted photographs. By removing the relevant encryption keys, it is possible to delete the encrypted cloud data, rendering it inaccessible. Therefore, with the help of these SPIS (Secure Plaintext Image Storage)protocols we are able to provide all the privacy features along with preserving the resolution of the images till the end.

II. LITERATURE SURVEYS

[1]. **Data-driven and feedback enhanced trust computing pattern for large-scale multi-cloud collaborative services, By X. Li, H. Ma, W. Yao, and X. Gui.**

Multiple data centers make up a multi-cloud collaboration environment, which is a common processing platform for big data. This study develops a Data-driven and Feedback-Enhanced Trust (DFET) computing pattern across several data centers using a number of novel methods with a focus on the trust computing requirement of multi-cloud collaboration services. First, a distributed soft agent-based trust-aware service monitoring architecture is suggested for use as job scheduling and multi-cloud trust computing middleware. The next step is the proposal of a data-driven trust computation scheme based on multi-indicator monitoring data. This system is appropriate for service-oriented cloud

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

applications since it incorporates various important service indicators. More crucially, we suggest an improved and hierarchical feedback method that can successfully lower networking risk while enhancing system dependability, taking into account the inherent relationships between users, monitors, and service providers. Theoretical study demonstrates that the DFET pattern offers excellent protection from malicious and defamatory attacks. In order to confirm the viability of the DFET pattern, we also construct a prototype system. The experiments produce insightful results that can aid in the efficient application of DFET in the context of large-scale multi-cloud collaboration.

[2]. **Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things, By A. A. A. El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca,**

Due to the mathematical foundation upon which some cryptographic protocols have been constructed, the emergence of quantum computers and quantum algorithms presents a problematic scenario for those protocols. In several disciplines, including quantum algorithms and cryptography, quantum walks serve as a general-purpose quantum computational model. Due to their nonlinear dynamical behaviour and strong sensitivity to initial conditions, quantum walks can be used as a potent tool for the creation of contemporary chaos-based cryptography applications. In order to preserve the privacy of the patients, we suggest new encryption mechanisms in this study for Internet of Things-based healthcare systems. Processes for encryption and decryption are based on managed alternative quantum walks. The two steps of the proposed cryptosystem approach are substitution and permutation, both of which are based on separately calculated quantum walks. The outcomes of the simulations and the numerical analysis of our data are sufficient proof that our image encryption procedure is reliable and effective at safeguarding patients' privacy.

[3]. **Efficient quantum information hiding for remote medical image sharing. By A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta.**

The goal of information hiding is to include hidden information into text, image, audio, and other forms of multimedia. Two novel quantum information concealment strategies are presented in this study. It is suggested to use quantum steganography to conceal a quantum cover image with a quantum secret image. To show the security of the embedded data, the quantum secret image is first encrypted using a controlled-NOT gate. Utilizing the two most and least important qubits, the encrypted secret image is included into the quantum cover image. Additionally, a method for quantum picture watermarking is provided to blend a grayscale quantum watermark into a quantum carrier image. The two least and most significant qubits are used to incorporate the quantum watermark image into the quantum carrier image after it has been scrambled using Arnold's cat map. The embedded quantum watermark image can only be extracted using the watermarked image and the key. Sharing medical images between two distant hospitals has been used as an example of the intended novelty. The simulation and analysis show that the two recently proposed techniques have great embedding capacity, outstanding visual quality, and excellent security.

[4]. **Similarity search for encrypted images in secure cloud computing. By L. Yingying, J. Ma, M. Yinbin, Y. Wang, X. Liu, and K. K. R. Choo.**

The Content-Based Image Retrieval (CBIR) technique has received a lot of attention from several fields since the advent of intelligent terminals (i.e., cloud computing, social networking services, etc.). Existing privacy-preserving CBIR methods still have flaws while being able to guarantee image privacy and facilitate image retrieval (i.e., low search accuracy, low search efficiency, key leakage, etc.). In this work, we present a similarity search for encrypted images in secure cloud computing to address these difficult problems (called SEI). First, search accuracy is improved by using the feature descriptors that the Convolutional Neural Network (CNN) model has extracted. Then, in order to increase search performance, an encrypted hierarchical index tree is created using K-means clustering based on Affinity Propagation (AP) clustering. Then, to prevent the secret from being totally leaked to unreliable image consumers, a limited key-leakage k-Nearest Neighbor (kNN) approach is suggested. Finally, SEI is strengthened to further guard against the cloud server learning about image customers' search terms. Our rigorous security analysis demonstrates that SEI can safeguard both key and image privacy. Our empirical tests on a real-world dataset demonstrate how SEI provides better search accuracy and efficiency.

[5]. **Secure outsourcing sift: efficient and privacy-preserving image feature extraction in the encrypted domain. By L. Jiang, C. Xu, X. Wang, B. Luo, and H. Wang.**

Huge amounts of storage space are required for multimedia data, and high processing power is required for applications using multimedia data. Owners of multimedia material may find cloud computing useful in managing it. However,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

multimedia data stored in the cloud may expose the private information of the data owner, including sex, hobbies, addresses, physical characteristics, and so forth. Before uploading multimedia data to the cloud, the data owner might encrypt it for privacy. However, the use of multimedia data is made challenging by encryption. The first thing we learn in this research is that pre-existing schemes have issues with vast storage space, security, and low efficiency because of their inefficient and insecure algorithms. Then, we offer an efficient and useful scale-invariant feature transform (SIFT) approach for encrypted images that protects privacy. Based on our new encoding techniques, new homomorphic comparison, and levelled homomorphic encryption,division and derivative encryption. With the help of our new secure SIFT method, you may achieve more processing efficiency, significantly cut down on communication costs and interactive times between user and server, as well as correctly identify feature key points, accurately describe feature points, and match images. We assess the security and effectiveness of our new secure SIFT scheme and thoroughly contrast it with competing methods. It is most similar to the original SIFT algorithm, according to the outcome.

[6]. **A systematic review on the status and progress of homomorphic encryption technologies. By M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, and A. J. Aljaaf.**

Big data's debut and the ongoing expansion of cloud computing applications raised significant security and privacy issues. As a result, a number of researchers and cybersecurity professionals have set out on a mission to expand data encryption to big data platforms and cloud computing applications. As more people use public cloud services, secrecy becomes an increasingly challenging problem. Cloud users who store their data on a public cloud are constantly looking for answers to the confidentiality issue. Data from clients is secured in the cloud using homomorphic encryption, which enables some search and manipulation activities without the need for proper decryption. In this article, we give a thorough analysis of previously published studies on homomorphic encryption. In order to review studies gathered from diverse resources, this research uses the PRISMA checklist in addition to a few components of the Cochrane Quality Assessment. It was clear from the publications we evaluated that big data and cloud security had gotten the most attention. Although additional possible issues have been found by the thematic analysis, homomorphic encryption was recommended in the majority of studies. The explicit statement of research objectives, acknowledgment of the procedure, and sources of funding used in the study were three criteria that 38% of the articles did not meet. Additionally, the paper included a comprehensive textual examination of the various homomorphic encryption methods, their uses, and potential future research directions. The majority of research articles explored the potential use and application of homomorphic encryption as a response to the increasing needs of big data and the absence of security and privacy safeguards therein, according to the results of the evaluation through PRISMA and the Cochrane tool. 26 out of the 59 articles that met the inclusion criteria made this clear. In the word cloud created from the chosen articles, the term "homomorphic encryption" appeared 1802 times, indicating its ability to guarantee security and privacy while simultaneously maintaining the CIA trinity in the context of big data and cloud computing.

[7]. **A cloud-user watermarking protocol protecting the Right to Be Forgotten for the outsourced plain images. By X. Dong, W. Zhang, X. Hu, and K. Liu.**

This article explains how cloud storage significantly reduces people's need for local storage space while separating the ownership of data from private manipulation. As a result, it is challenging for the cloud user to verify that the cloud storage provider CSP complied with the request to delete all pertinent data. This article suggests an interactive cloud-user watermarking protocol called CUW that is built on homomorphic encryption to address the problem technically. The encrypted watermark is integrated into encrypted data to suit security needs. Additionally, the uploaded data is ultimately kept in the cloud server as plain text to take advantage of the practical cloud services. A prototype implementation is used to assess the CUW protocol's performance.

[8]. **P ROST: Privacy-preserving and truthful online double auction for spectrum allocation. By Q. Wang, J. Huang, Y. Chen, C. Wang, F. Xiao, and X. Luo.**

An efficient way to allocate limited spectrum resources is through auction. However, the majority of spectrum auction designs simply focus on economic soundness, ignoring the underlying issue of privacy loss. Existing techniques for secure spectrum auctions fall short in terms of security and all ignore how spectrum requests are submitted online. For the first time, we present PROST in this paper—a privacy-reserving and truthful online double auction mechanism for allocating spectrum in wireless networks. PROST offers a thorough and robust security for users' sensitive information, notably for location privacy and temporal dynamics, when compared to cutting-edge alternatives. Our carefully crafted

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

security building pieces, which support different arithmetic operations over encrypted real numbers and are useful in other spectrum auctions, are the foundation upon which PROST is built. Furthermore, we create a novel buyer grouping methodology for spectrum reuse that protects anonymity, which enhances the functionality of the current online spectrum auction processes. We thoroughly assess PROST's performance in addition to theorising that it can achieve all-around security against partially honest adversaries. The results of the experiments confirm that PROST manages to allocate spectrum with great efficiency and at low computational and communication costs.

[9]. **Efficient and privacy-preserving outsourced calculation of rational numbers. By X. Liu, R. Choo, R. Deng, R. Lu, and J. Weng.**

In this article, we put forth the POCR framework, which stands for Private Outsourced Calculation of Rational Numbers. With the aid of POCR, a user can safely delegate the processing and storage of rational numbers to a cloud server without jeopardising the confidentiality of the (original) data and the computed results. To ensure that frequently used outsourced operations may be done instantly, we provide the system architecture of POCR and the related toolkits needed in the privacy-preserving calculation of integers and rational numbers. Then, using simulations, we establish that the proposed POCR accomplishes the objective of safe integer and rational number calculation without exposing personal information to unauthorised parties.

[10]. **White-hat hacking framework for promoting security awareness. By S. Al Sharif, F. Iqbal, T. Baker, and A. Khattack.**

The number of associated possible vulnerabilities and associated attack vectors is growing at the same time as the diversity of new social media applications is being produced at an ever-increasing rate. Social engineering attacks have historically been a significant source of worry for information security departments. However, because social media and gaming applications have been widely adopted by the general public and the number of social media and gaming applications has increased, there has been an even greater prevalence of personal information theft, misuse, and manipulation for harmful purposes. Due to poor system design and coding methods, these recently released and constantly evolving apps continue to create new vulnerabilities, which have resulted in a wide variety of sophisticated assaults and cybercrimes. The stealthy application used for the proof of concept was partially developed using a commercial off-the-shelf application (Camera Mouse 2011). The recently created stealth robot conceals itself from the intended target/victim by using stealth tactics. The suggested method makes it possible for the created robot application to avoid detection by top-tier commercial anti-virus programmes. The created robot has been tested in a variety of settings using a range of operating systems shielded by a range of commercial antivirus programmes. The proposed method was evaluated on computers owned by individuals from various backgrounds, including graduate and undergraduate students, faculty, and staff (with their consent). The preliminary test results show that the suggested method works well as a tool to help raise awareness about various user-focused cyberattacks.

III. CONCLUSION

In this research, Baced on this above provided Literature Surveys we suggest multifunctional secure plaintext image storage (SPIS) algorithms. With the use of SPIS protocols, unencrypted images can be stored, shown, and deleted in a cloud environment while maintaining user privacy. The owner of the image has control over the uploaded photographs' quality and can monitor any improper behaviour by the cloud, such as image leaks and violations of the right to be forgotten. The unencrypted image can be stored in the cloud with less storage space required. Any conspiracy between a party and the third party is prevented while taking into account a semi-honest third party. Our security analysis and the results of the experiments have demonstrated that the SPIS protocols are effective and secure enough for a practical implementation. Future research will examine the secure outsourcing of the plaintext 3D model, allowing us to improve the system to handle larger and more complicated computations.

REFERENCES

[1]. X. Li, H. Ma, W. Yao, and X. Gui, ”Data-driven and feedbackenhanced trust computing pattern for large-scale multi-cloud collaborative services,” IEEE Trans. Serv. Comput., vol. 11, no. 4, pp. 671-684, Jul./Aug. 2018.

[2]. A. A. A. El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, ”Controlled alternate

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

quantum walks based privacy preserving healthcare images in Internet of Things," Optics & Laser Technology, vol. 124, 105942, 2020.

[3]. A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," IEEE Access, vol. 6, pp. 21075- 21083, 2018.

[4]. L. Yingying, J. Ma, M. Yinbin, Y. Wang, X. Liu, and K. K. R. Choo, "Similarity search for encrypted images in secure cloud computing," IEEE Trans. Cloud Comput., 2020.

[5]. L. Jiang, C. Xu, X. Wang, B. Luo, and H. Wang, "Secure outsourcing sift: efficient and privacy-preserving image feature extraction in the encrypted domain," IEEE Trans. Depend. Sec. Comput., vol. 17, no. 1, pp. 179-193, Jan./Feb. 2020.

[6]. M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, and A. J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," Journal of Inf. Security and Appl., vol. 48, 102362, 2019.

[7]. X. Dong, W. Zhang, X. Hu, and K. Liu, "A cloud-user watermarking protocol protecting the Right to Be Forgotten for the outsourced plain images," Int. Journal Digit. Crime Forensics, vol. 10, no. 4, pp. 118-139, 2018.

[8]. Q. Wang, J. Huang, Y. Chen, C. Wang, F. Xiao, and X. Luo, "P ROST: Privacy-preserving and truthful online double auction for spectrum allocation," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 374-386, Feb. 2019.

[9]. X. Liu, R. Choo, R. Deng, R. Lu, and J. Weng, "Efficient and privacy-preserving outsourced calculation of rational numbers," IEEE Trans. Depend. Sec. Comput., vol. 15, no. 1, Jan./Feb. 2018.

[10]. S. Al Sharif, F. Iqbal, T. Baker, and A. Khattack, "White-hat hacking framework for promoting security awareness," in Proc. 8th IFIP Int. Conf. on New Technologies, Mobility and Security, 2016.