Journal of Cardiovascular Disease Research

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

Securing Medical Image in the Cloud Using Decoy Techniques

Lipsa Nayak, Jayalakshmi V

Schoolof Computing Sciences, Vels Institute of science,Technology and Advanced Studies, (VISTAS), INDIA

E-mail: info.lipsa@gmail.com, jayasekar1996@yahoo.co.in

Abstract— Healthcare services make extensive use of information technology to reform and improve their services. As a result of this technological innovation, a large amount of data from various healthcare-related instruments is generated. The management and distribution of healthcare data have grown more critical in order to make quick and accurate disease diagnosis decisions and connect those decisions with suitable therapy. Medical Big data can be used to predict the recurrence of some avoidable infections. The Cloud allows for improved real-time access to a patient's medical data while also lowering the cost of healthcare delivery. Despite the many benefits of cloud computing for medical companies, there are still security concerns about our data kept in the Cloud. In this work, the main focus has been given to providing security for the medical image stored in the healthcare cloud system using the decoy technique.

Keywords— Cloud computing, Decoy image, Cloud Security

I. INTRODUCTION

The internet has become the cornerstone of information technology, and it has kept the world connected as a whole. With the development of technology, a massive amount of data is generated. Cloud computing provides an enormous storage capacity with flexibility. It operates on a pay-per-service basis and provides on-demand services.Traditional medical services are combined with sophisticated technologies in the healthcare industry to create unique therapy. Apart from these, the healthcare cloud has several security flaws. Security and protection are seen as vital requirements whenever sharing or gaining access to persistent information amongst collaborators[1].To provide security with low cost and high flexibility, the decoy technique is used in this work.

The use of decoys as a new paradigm for tackling computer security concerns that present defenses are unable to detect is proposed in this study. Decoys are artificial constructs that hold data that appears to be valuable but isn't. In the proposed work, a decoy gallery with a fog computing facility is used to limit the attack on the healthcare cloud.Because the images in the decoy gallery look so much like real medical images, it's impossible for an attacker to tell the difference. The term "decoy" stems from the act of hunting animals. A decoy is a creature that hunters use to lure in other animals. To confuse the attacker, the suggested framework employs the same technique. It's akin to the concept of a honey pot for attackers[2]. This tactic is intended to deceive the attacker into thinking they're using the real one.

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

A. Decoy Properties

There are a variety of characteristics associated with decoy documents that can be used to measure and ensure that their use will likely catch an inside attacker.The qualities of a decoy document should be as follows[3].

Believable: A good decoy should make it challenging for an enemy to tell whether they're looking at a genuine document from a reliable source or a decoy. It is hypothesized that an adversary's capacity to distinguish one decoy from another is a good indicator of its believability

Enticing: The attacker's intent or preference determines the level of enticement. Enticing documents are chosen with the same likelihood as an adversary's preference; enticing decoys are those selected with the same prospect as an adversary's preference.

Conspicuous: Conspicuousness and enticing influence the possibility of an attacker obtaining a document. Entictingness represents how interested an adversary is in a decoy, whereas conspicuousness refers to how easy a decoy is to find. A visible record is one that is easy to locate and use. The amount of effort necessary for an adversary to discover a decoy, or more formally, the number of steps required to access it, is referred to as conspicuousness.

*Detectable: D*etectability refers to a decoy's ability to alert its owner when accessed. Although an ideal decoy system would send an alarm every time a decoy is viewed, technological challenges such as network availability and software platform diversity imply that this isn't always attainable in practice.

Variability: A single search or test function may readily discern between the actual and the phoney. As a result, the decoys must be pretty diversified. A variable is defined as the probability of determining the believability of a decoy given any known decoy.

Non-interference: The likelihood that the file system's principal owner will access a specific standard document should be the same as before the decoy material was included. Similarly, delivering decoy apps to a mobile device's operating system should not affect a user's ability to access real apps as usual.

Differentiable: In effect, the property of decoy non-interference means that true users must easily differentiate between spurious decoy content and authentic data. This can be thought of as the opposite of the believability property. Although decoys should seem as realistic as possible to adversaries, they should appear to be fake for users who should actually be accessing a system. A decoy can be considered fully differentiable if a real user always succeeds at this task.

Stealth: While it is certainly desired for all fake access events to be visible to system owners, caution must be exercised lest the alerts used to achieve this cause suspicion. The property of decoy variability would be violated if an overt method for issuing alarm beacons provided opponents with a clear signal that an element contains a trap. As a result, the messages conveyed by decoys must be as delicate and covert as feasible.

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

B. Decoy image generation

The process of manually introducing decoy content to a system is very tedious; however, since each time new information is saved on the system, an equal amount of spurious material would also need to be created[4]. Users would also be responsible for checking access events for these files. Needless to say, manual decoy creation would scale very poorly in a large organization with many computers and users.

Making, managing, and monitoring decoys is thus a nontrivial problem as an alternative to performing these steps manually. A system is suggested that does so with minimal user involvement. This is precisely the purpose of the Decoy Document Distributor (D3) System. D3 is a tool for generating and monitoring decoys that can be accessed by registered users in order to create decoys for download[5]. It can also be used as a source of data for decoy use in host and network components.

II. RELATED WORK

Y. Liu et al. suggested a paradigm for securing cloud data through data integrity and verification. The acquisition of security and operational risks, such as hardware failure, malware, software defects, and so on, is a significant challenge in cloud computing. As a result, outsourced data on the Cloud must be protected. Availability and dependability assurances are another challenge in public clouds[6].The inactive information's arrangement security is to be done by encoding the information or data and sending it to the server, which is how confidentiality and integrity of data are performed by encoding the data.

A user study was undertaken by Ben Salem et al. to assess the efficacy of decoys deployed with these qualities in mind. The ability of decoys to detect masquerader attacks was validated in this investigation[7]. It also discovered a number of trade-offs between decoy properties that may be adjusted to protect against specific types of attackers. Furthermore, these authors proposed ways for increasing the attractiveness of decoys to insiders while avoiding interfering with legitimate users' expected workflow.

Spitzner invented the concept of "honeytokens" to expand the concept of honeypots to the area of insider threat detection. Honeypots and honey networks are deceptive security mechanisms that work at a much finer granularity than honeytokens. They are discrete fragments of information designed to pique antagonistic interest but lacking in substance. Honeytokens can be anything from fabricated personally identifiable information to illegitimate access credentials[8]. To characterise a document that provides such alluring material, Yuill et al. invented the term "honeyfiles."

Mutlag et al. described a data breachas when an attacker hacks a mutual network to steal sensitive data. Data breaches can easily be seen in Personally Identifiable Information (PII) and financial information. Encryption Related Threat- One of the threats in encryption is that it limits the efficiency of Cloud services because large data is expensive. Time-consuming to get encrypted and need to be stored before encryption then decrypted in the mean. At the same time, one can manipulate the data, leading to data integrity violations.

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

Data Tampering is a data modification that could provide the attacker access to a service through several different methods listed in this document. Data Privacy Breach loss of corporate information such as trade secrets, sensitive corporate information, details of contracts, etc., or government[9]. Data Breaches, encryption-related threat, Data tampering, Data privacy breach, information disclosure, Token Stealing information is frequently unreported, as there is no compelling reason to do so in the absence of potential damage to private citizens.

Vijayakumar et al. explained that data deprivation could be viewed as deletion without a backup by loss of the encoding key or by unauthorized access; data is always in danger of being lost or stolen. This is one of the top concerns for the business sector as they stand to lose their reputation and are obligated by law to keep it safe. Incomplete data means data being deleted or modified without any backup of the original content. The storage of unlinked data on unreliable media creates unrecoverable data threats[10]. It has been seen that the record is often not altered or deleted correctly as well, as there is no backup of data, which leads to data deprivation, insecure data deletion, data loss, or leakage of data location to permanent loss of data. As a result, it can be stolen or leaked by unauthorized users.

Borda et al. discussed threats that could be generated due to the security problems concerning the location of the Cloud systems, such as multilocation of the private data, multilocation of the service provider, data combination, and commingling restrictions on techniques and logistics and data transfer across the borders. Cloud misapplication threat can be very harmful in centralized and shared systems like Cloud; abuse by cybercriminals can take place in many ways. For example, they can go undetected for a long in Cloud computing. There is no strict registration procedure. Anyone can use a credit card and register themselves online on Cloud or through free trial services of vendors. This opens a line of approach for nefarious users who exploit the Cloud resources to set up botnets, spamming, spreading the virus, etc.

III. PROPOSED METHODOLOGY

Medical data is susceptible as it contains much personal information about a patient. Any attacker can misuse this data to hamper a patient's health, the reputation of a hospital or a doctor. In the proposed work healthcare cloud is protected by a fog of decoy gallery, which disguises the attacker and protects it. Fog computing is a widely used standard for storing, processing and transferring data closer to the client. To give the look of a Cloud, fog computing concepts are applied. Anyone who tries to access the Healthcare Cloud without authorization will be greeted by the fog of a decoy gallery[7]. This collection contains fictitious images that give the impression of being real. The proposed framework is developed to stop the attack on the healthcare cloud. The Decoy images should follow some basic properties so that for the attacker, it is difficult to identify the difference between real and decoy images.

Process of Uploading an Image: This fog of decoy gallery is created to reduce attacks on the real Cloud that contains decoys to confuse the attacker. Whenever an image is uploaded in

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

the real Cloud, a decoy image is also uploaded in the fog of decoy. Decoy images are very much similar to real files so that the attacker cannot detect that they are accessing a fake cloud. For example, a decoy image is also an X-ray category if an X-ray image is uploaded to the real Cloud. Figure 1 shows the process how uploading an image in the fog of decoy occurs when an image is uploaded in the real Cloud.

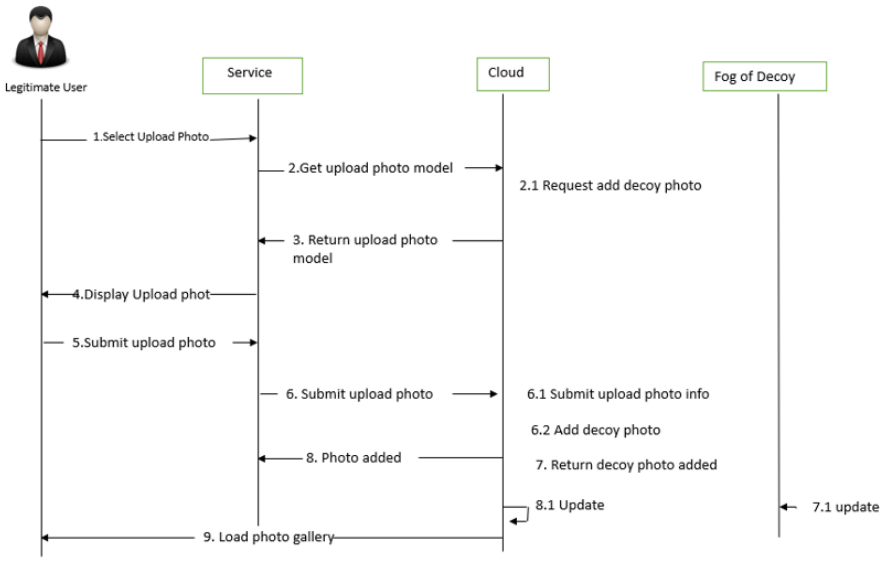

Figure:1 Process of Uploading an Image

IV. PERFORMANCE ANALYSIS

The performance of the proposed technique is measured using a decoy turning test and cost analysis.

A. Decoy Turing Test

The goal of these tests is to demonstrate that adversaries who rely on manual inspection of user behaviors will be adequately challenged. Although the simulations are designed to deceive crimeware, we focus on persuading humans, which is a more challenging task, making it significantly more difficult for adversaries to create malware that detects decoys. The task is performed by taking various medical images like MRI, CT scan,X- rays, ultrasound, and their respective decoys. Few demonstrators are selected to identify between real and decoy images. Based on the result, Figure:2 shows how effective decoy images are.

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

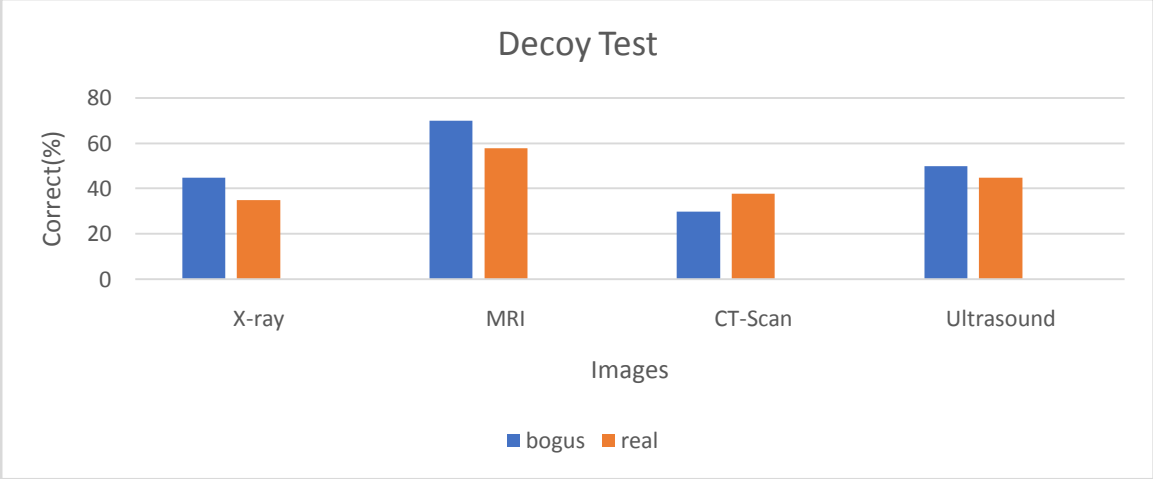

Figure:2 Decoy Test

B. Computational Cost Comparison

The cost of the proposed Decoying technique is compared with some of the existing techniques like DMBD and OCC. Few notations like ADD (modular addition operation), MUL (modular multiplication operation), DIV (modular division operation) were taken. It gives a comparison of computational cost analysis is given in Table 1. Figure 3 shows the efficiency of the proposed technique.

Table 1: Computational Cost Comparison

Techniques	***ADD***	***MUL***	***DIV***	***HASH***
DMBD	1	1	0	5
OCC	1	1	1	4
DECOYING	0	1	0	1

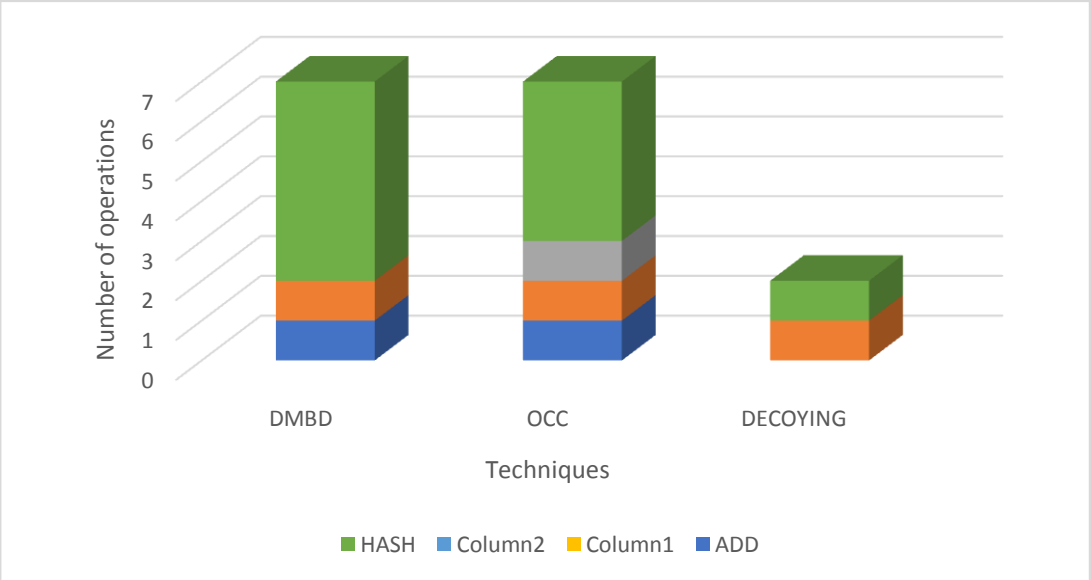

Figure:3Computational Cost Analysis

ISSN: 0975-3583,0976-2833 VOL13,ISSUE03,2022

V. CONCLUSION AND FUTURE WORK

Users can avoid the cost and hassle of establishing and maintaining their own storage infrastructure by shifting their healthcare data to the Cloud. Despite the numerous advantages, the cloud model struggles with one major issue that prevents widespread adoption: security and privacy concerns. But with proper adequate security measures, life in the Cloud will be more advantageous. The prime objective of this work is to address cloud data security concerns and mitigate concerns over confidentiality, authenticity, and integrity of data stored in the Cloud using the decoy technique.

Several interesting issues and unsolved problems that require further investigation have emerged during the course of this research. Future work can be done to improve efficiency by adding more metrics to the proposed work with a large dataset. In addition, any healthcare organization can use the proposed framework.

REFERENCES

[1] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework,"*IEEE Trans. Serv. Comput.*, vol. 9, no. 1, pp. 138–151, 2016, doi: 10.1109/TSC.2015.2491281.

[2] A. Singh, "Security concerns and countermeasures in cloud computing : a qualitative analysis,"*Int. J. Inf. Technol.*, 2018, doi: 10.1007/s41870-018-0108-1.

[3] J. Vincent, "Privacy Protection and Security in eHealth Cloud Platform for Medical Image Sharing," pp. 93–96, 2016.

[4] M. Moharana, M. Pandey, and S. S. Routaray, *Chapter 8 - Why big data, and what it is: basics to advanced big data journey for the medical industry*. Elsevier Inc., 2020.

[5] M. Yadav and M. Breja, "Secure DNA and Morse code based Profile access control models for Cloud Computing Environment,"*Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2590–2598, 2020, doi: 10.1016/j.procs.2020.03.317.

[6] A. Murugan, "Triple Encryption Scheme with Parallel Zigzag Pattern for Cloud Data Storage Triple Encryption Scheme with Parallel Zigzag Pattern for Cloud Data Storage Scheme," no. July, 2019.

[7] L. D. Singh and K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography,"*Procedia - Procedia Comput. Sci.*, vol. 54, no. 1, pp. 73–82, 2015, doi: 10.1016/j.procs.2015.06.009.

[8] R. Kanimozhi, "Adaptive and intelligent framework of data protection techniques for cloud storage," vol. 8, no. 1, pp. 50–67, 2019.

[9] H. A. Al-hamid, S. M. Rahman, and A. C. Security, "Securing Photos in the Cloud Using Decoy Photo Gallery," pp. 816–822, 2017.

[10] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing : Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," pp. 89–106, 2010.