Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1061

ORIGINAL RESEARCH ARTICLE

Defending against phishing attacks in cloud computing using digital watermarking

Sasidhar Attuluri[1], Mona Ramesh[2], Raja Rao Budaraju[3], Sumit Kumar[4,*], Jhum Swain[5], Jitendra Kurmi[6], Bhupati[7]

[1] *Security Engineer, Savin Technologies Inc, 9901 Valley Ranch Pkwy E, Irving, 75063 TX, USA*

[2] *Department of Computer Science & Engineering, Syracuse University College of Engineering, 223 Link Hall, 1324 Syracuse, NY, USA*

[3] *Department of Computer Science & Engineering, Oracle, 3990 Scottfield street, 94568 Dublin CA, USA*

[4] *Department of Computer Science & Engineering, Haridwar University, Roorkee 249404, India*

[5] *Department of Computer Science & Engineering-Data Science, Swami Vivekananda Institute of Technology, Hyderabad, Telangana 500003, India*

[6] *Department of Computer Science & Engineering, University of Lucknow, Uttar Pradesh 226007, India*

[7] *Department of Internet of Things, K L Deemed to be University, Vaddeswaram, Guntur 522302, India*

*** Corresponding author:** Sumit Kumar, dr.sumitcse@huroorkee.ac.in

ABSTRACT

Cloud computing is an important aspect for cloud security using digital watermarking. Digital watermarking is a technique used to embed information into digital content such as images, audio, or video, for various purposes including copyright protection, authentication, and tamper detection. While digital watermarking itself is not a direct solution for cloud security, it can be used as a component of a broader security strategy. Conveying information concentrated work processes in the cloud carries new factors to be considered during detail and planning. The cloud planning work process under asset distribution is essentially difficult because of the computational power of the work process, the reliance among assignments, and the heterogeneity of cloud assets. Phishing is a sort of friendly designing attack routinely used to take individual information, alongside login qualifications and FICO rating card numbers. Acknowledge potential challenges associated with the implementation of digital watermarking in the cloud, such as algorithm strength, scalability, and evolving security threats. Emphasize the importance of regular updates and assessments to maintain the effectiveness of watermarking techniques. The proposed ODWS Algorithm (Optimized digital watermarking Security system) performs higher in compression to the previously developed based algorithms for securing the cloud services. Watermarking can be integrated with encryption key management systems. Watermarks may contain information about the encryption keys used to protect the data. This can add an extra layer of security, as unauthorized access attempts without the correct keys would be evident through the absence of incorrect watermark information. The need for encryption for cloud services using the internet. It's important to note that while digital watermarking can enhance security, it should be used in conjunction with other security measures such as encryption, access controls, and regular security audits. Additionally, the effectiveness of digital watermarking depends on the specific implementation and the strength of the watermarking algorithm used. Regular updates and assessments of the watermarking technique are essential to adapt to evolving security threats.

Keywords: cloud service attacks; cloud security system; digital security of services; system security; resource security; digital security; end users; watermarking security tools

ARTICLE INFO

Received: 28 July 2023
Accepted: 20 December 2023
Available online: 5 August 2024

1. Introduction

Cloud computing has revolutionized the way organizations handle data, offering unprecedented flexibility and scalability. However, this shift to the cloud also brings forth new challenges, particularly in ensuring the security and integrity of sensitive information. This introduction explores the integration of digital watermarking as a strategic component in cloud security measures. Digital watermarking, traditionally used for copyright protection, is now emerging as a robust tool for enhancing data integrity, authentication, and tamper detection in cloud environments. In the scenario the place phishing assaults on the cloud are enhancing step via step, associations ought to put together for the most pessimistic situation circumstances. This planning needs to be viable by means of splendid records reinforcement methodologies as hostile to moderating anticipated harm. The public levels warranty those providers facts is continuously scrambled on the cloud and upheld. Encryption of reinforcement files in the cloud attaches a more safety layer in opposition to undesirable backyard substances. Each year bunches round the world lose countless bucks to phishing assaults. The overwhelming reason toward the rear of the misfortune is the absence of acknowledgment among representatives. Today, phishing assaults, moreover, perceived as friendly designing attacks continue to play a predominant capability in the digital opportunity scene[1]. The recurrence and refinement phase of these attacks are going up each spending year. Notwithstanding, the assortment can be extensively diminished by utilizing understanding what these attacks are, how they work, and how they are conveyed. There are various types of phishing done in cloud computing resources like email, spear, whaling, smishing and vishing. These attacks are varied dangerous for cloud resources. An e mail that includes malicious hyperlinks and attachments to steal the user's data, such as login credentials and credit score card numbers, is regarded as electronic mail phishing[2]. The e-mail templates may additionally range based totally on the attacker and the target. However, the rationale is the same, that is to steal your touchy statistics or supply malware. Often cyber criminals impersonate anyone the person will have confidence so that the person can fall for the assault easily. They will body the e-mail in such a way that will tempt the person to click on the malicious hyperlink or download the attachment that comes with the email. Most of the time the malicious actors create urgency so that the consumer doesn't take time questioning about clicking or downloading the hyperlink or attachment. Noticeable and imperceptible are the two crucial sorts of advanced watermarking, and each computerized watermark can be viewed as both seen and undetectable[3]. Recognizable computerized watermarking is a method by which any individual can see the contents of the developed sign. The contents are typically a symbol that identifies the computerized flag's owner. The creators make it clear that cloud security is complicated[4]. Cloud customers are responsible for accurately arranging cloud assurance and safeguarding their capacities and workloads, whereas cloud companies take responsibility for the security of the foundation they oversee. Malware defilement in your cloud computing environment is one of the most extreme security issues that can result from misconfiguration and the need for software security. Although the presence of malware in the cloud may appear to be a strikingly recent development, cybercriminals have since discovered that cloud structures serve as a distribution platform for malware. These are cloud-based structures: typically, accessible via the Internet[5]. Standard and useful for locating an aggressor. composed of a vast array of materials, including capacity buckets, machines, and holders, each of which can serve as an unprotected link for abusers. As businesses increasingly migrate their operations to the cloud, concerns about the security of sensitive data have become paramount. Digital watermarking, a technique that embeds imperceptible information into digital content, provides a unique and versatile approach to fortifying cloud security. This introduction delves into the key applications of digital watermarking and its role in addressing security challenges in the cloud. Explore the integration of digital watermarking with access control policies and encryption key management[6]. **Figure 1** defines the block diagram of digital water marking system. Discuss how watermarks can contain information about user permissions, access times, and encryption keys, adding an additional layer of security to cloud environments.

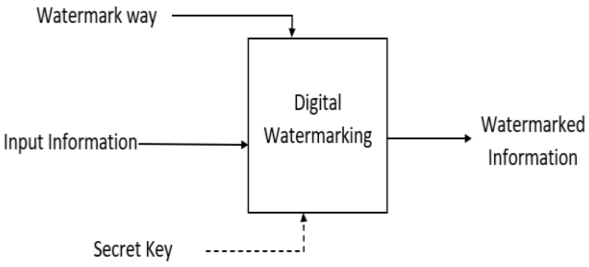

Figure 1. Basic cloud digital watermarking.

A distributed denial of service (DDoS) attack on your company or any of your neighbors in the public cloud can affect the entire neighborhood as well as the cloud system that is hidden. Likewise, there's an obvious bet that unattended VMs or compartments will be undermined by aggressors, and your passed-on dealing with resources will be used for bad behavior[7]. A hyper-jacking assault is an attempt by an attacker to install a rootkit on a virtual machine and take control of the hypervisor. If the attacker is successful, they will gain access to the entire system, alter the behavior of virtual machines, harm currently running VMs, and, shockingly, create inactive VMs with the intention of exacting retribution. Directors and chairmen should be aware of the possibility of being held responsible for numerous cloud malware incidents. A comprehensive plan can show proper behavior and make people more aware of common security risks. Representatives who are aware of cloud systems are required to regularly complete preparation courses on cloud security, organize security, and submit applications to the board[8]. Cloud Bits of Information help you quickly identify issues that recently have an impact on your business. Increase utilization in such a way that it is easier to reduce uses, accomplish more with limited resources, identify ransomware attacks that have recently reached the point of no return, and successfully report on data access for security consistency review. NetApp Cloud Bits of knowledge prevents malicious or compromised clients from mishandling various levels of data by utilizing cutting-edge AI and out-of-the-ordinary recognition[9].

2. Background

The survey explores the role of digital watermarking in securing data stored in the cloud. It analyzes different watermarking techniques, their strengths, and limitations, and discusses practical implementations for ensuring data integrity and preventing unauthorized access. It explores the combined use of digital watermarking and encryption for bolstering cloud security. It discusses how these two techniques can complement each other, providing a multi-layered approach to safeguarding data in cloud environments. This paper provides a comprehensive review of the use of digital watermarking techniques in enhancing cloud security. It covers various applications, challenges, and recent advancements in the field, offering insights into the integration of watermarking for data integrity, authentication, and traceability in cloud environments[8]. A parodied e-mail curiously from myuniversity.edu is mass-circulated to something wide variety personnel as should moderately be expected. Unlike other phishing assaults, skewer phishing doesn't depend on the shower and ask procedures. In stick phishing, digital lawbreakers make more customized layouts. This makes this assault vector more successful and riskier than other phishing assaults, for example, email phishing[10]. In stick phishing, digital crooks tweak the email layout in view of the client's situation or organization. This helps the aggressors in deceiving the client to accept that they have an association. Figure 2 defines the way of phishing used by most of the attackers[11]. Cybercriminals send off the mission using lance phishing strategies to pursue profiles. Like lance phishing assaults, in whaling assaults, cybercriminals alter the assault format considering the clients' situation and company. Individual data is accumulated from sources like web-based entertainment. Then, at that point, they are customized so that they will incorporate the client's name, position, and fundamental data that will make the assault layout look authentic Once a cybercriminal correctly infects and good points get entry to one pc on your network, it is possibly they will be capable to hack others if they are the usage of the identical cloud-based system[12]. A literature survey on cloud security using digital watermarking involves reviewing relevant research articles, papers, and publications to understand the current state of knowledge, challenges, and advancements in this area. Here is a concise literature survey highlighting key findings from existing works on cloud security with a focus on digital watermarking. Investigates the role of digital watermarking in ensuring the integrity of data stored in the cloud. Explores how watermarking techniques can provide a robust mechanism for detecting unauthorized modifications to cloud-hosted files performance is shown in **Figure 2.** Discusses the impact of different watermarking algorithms on data integrity and proposes improvements. Examines the use of digital watermarking as a means of authentication in cloud environments. Evaluates the effectiveness of watermarking in verifying the legitimacy of files during access or download from the cloud.

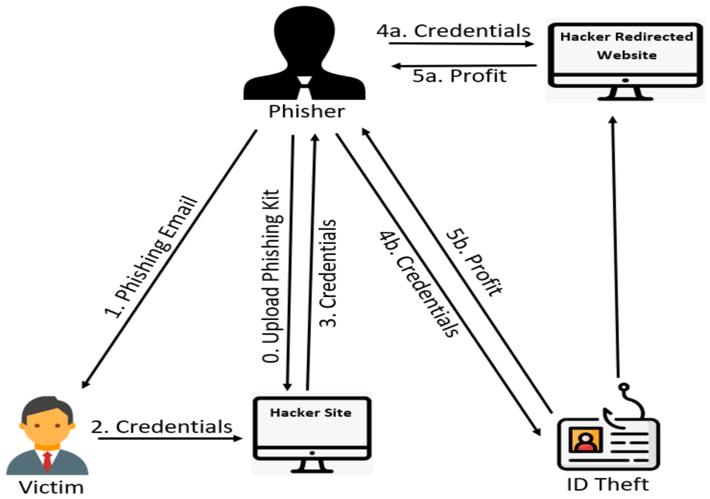

Figure 2. Ways to do phishing attack in cloud system.

3. Research challenges in cloud phishing security

Cloud phishing, or phishing attacks targeting cloud-based services, poses significant security challenges due to the evolving nature of cyber threats. Researchers and cybersecurity professionals are continuously addressing various challenges to enhance the security of cloud environments against phishing attacks[5]. The most important thing is to know what a cloud advanced attack is. A cloud advanced attack is any advanced attack that targets off-site business stages that offer capacity, figuring, or encouraging businesses through their cloud system. This could lead to attacks against business stages that use business movement models like SaaS, IaaS, and PaaS[7]. A greater number of organizations use cloud organizations to help them move to a different work environment and make it easier for colleagues around the world to work together. The cutting-edge technology of cloud computing provides a shared pool of computing resources over the internet at any time for very little to no cost. Numerous individuals and groups have reduced their IT costs while simultaneously speeding up their operations by utilizing cloud computing. While cloud computing designs have many advantages over on-site designs, they are vulnerable to both internal and external threats. As a result, cloud providers must implement security measures to protect sensitive user data from cyberattacks[13]. Virtualization and cloud coordination are two examples of shared connected sciences used in cloud computing. As a result, attackers could cause significant harm to a large number of cloud clients by exploiting vulnerabilities at any stage of these advancements. Programmers may be able to gain control over sophisticated machines or even the hypervisor itself thanks to its flaws. Programmers can gain unimpeded access to the host through shared assets in the event of a sophisticated computer evasion[14]. Therefore, the most important thing is to pay attention to the security of the cloud backer that you provide with your cloud arrangement. Although cloud providers use cryptographic calculations to protect data in storage, they typically mechanically generate arbitrary numbers for data encryption using restricted sources of entropy like time. For instance, advanced Linux-based machines only use a single millisecond to generate random keys[8]. In any case, attackers also use cutting-edge interpreting tools to hack data, so this may not be sufficient for strong encryption. As a result, cloud developers must assume how to secure facts before sending them to the cloud. A lot of people use weak passwords and reuse watchwords, making their secret word security extremely vulnerable. Because it allows a single stolen secret word to be used on a small number of unique accounts, this inconvenience increases the likelihood of phishing attacks and data breaches. As businesses become increasingly dependent on cloud-based foundation and capabilities for center endeavor capacities, account seizing is one of the additional real issues with cloud security[15]. An adversary who has access to an employee’s credentials can gain access to confidential information or usefulness, and compromised client credentials grant full control over an online account. In addition, businesses in the cloud frequently require the ability to recognize these risks and respond to them as effectively as they would for on-premises systems. The major challenges are phishers continually evolve their techniques to bypass traditional security measures. Phishing attackers often exploit newly discovered vulnerabilities or use novel attack vectors. Phishing attacks heavily rely on social engineering to trick users into divulging sensitive information. Phishers aim to harvest credentials to gain unauthorized access to cloud accounts. Attacks may originate from within an organization, involving compromised employee accounts. With the increasing use of mobile devices and Bring Your Own Device (BYOD) policies, phishing attacks targeting mobile users are on the rise. Enhancing the effectiveness of phishing detection and prevention using advanced technologies like artificial intelligence (AI) and machine learning (ML). Phishing attacks often exploit vulnerabilities in cloud service infrastructure. Users remain a critical element in the security chain and are susceptible to manipulation in phishing attacks. Meeting regulatory requirements and addressing privacy concerns while implementing effective phishing detection and prevention measures.

Research Focus is to develop strategies to ensure compliance with data protection regulations and address privacy implications when implementing security measures against cloud phishing. Investigate and develop human-centric security solutions, such as user-friendly education programs, to empower individuals to recognize and avoid phishing threats. Foster collaboration between researchers, cybersecurity professionals, and cloud service providers to share threat intelligence and develop collective defense mechanisms against phishing attacks. Develop and refine machine learning models that can analyze patterns, behaviors, and anomalies to identify phishing attempts in real-time. Explore mobile-specific anti-phishing solutions and secure BYOD practices to protect cloud services accessed through mobile devices. Investigate methods for early detection of insider threats, emphasizing anomaly detection and user behavior analytics to identify suspicious activities. Develop advanced authentication mechanisms, including multi-factor authentication, and investigate ways to detect and prevent unauthorized access even with compromised credentials. Develop proactive defense mechanisms that can detect and mitigate zero-day phishing attacks and novel threats before they become widespread. Investigate and develop detection mechanisms that can adapt to dynamic phishing tactics, including polymorphic phishing websites and evasion techniques. As reception increments, so do the weaknesses. By understanding cloud security rudiments and probably the most widely recognized weaknesses that happen in that, we can restrict our gamble of turning into an objective of cloud digital assaults. Smishing is a kind of phishing assault, and it is additionally acknowledged as SMS phishing[16]. Unlike electronic mail phishing, in smishing attacks, the malicious hyperlinks are embedded in SMS/text messages that are delivered through cellular phones. **Figure 3** shows the level of cloud security system. The cause in the back of the assault is the equal as different phishing attacks. In a smishing attack, malicious actors supply textual content messages to customers urging them to reply to the message or click on the hyperlink that is embedded in it. A consumer who falls for the lure and clicks the hyperlink ends up downloading the hazardous code or submitting private information. The messages are designed primarily based on the targets. However, it can rely on the attacker[17]. Addressing these challenges requires a multidisciplinary approach that combines technical innovations, user education, and collaboration between the cybersecurity community and cloud service providers. Researchers play a crucial role in advancing the field and staying ahead of the evolving landscape of cloud phishing threats.

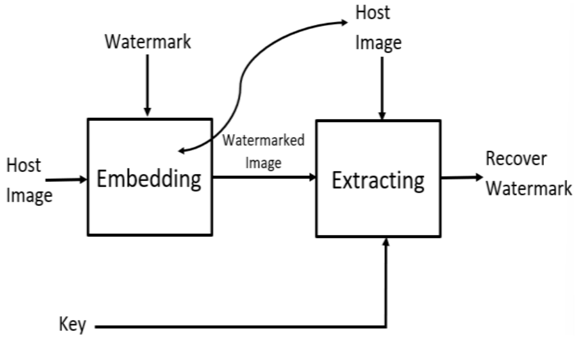

Figure 3. Levels of cloud watermarking-based security.

It is essential to bring our copyright proprietorship and use privileges regardless of we are global media organizations or impartial photographic artists. Computerized content material is voyaging faster and farther than at any different time because the mixture of get right of entry to and new instruments. Computerized has grew to become into a fundamental approach for articulation and correspondence. We can implant watermarks which include indistinct computerized statistics that can include possession data, contact subtleties, utilization freedoms and something we pick. Prior to choosing to move your own or proficient information to the cloud, doing your research is significant[18].

4. Attack vectors for cloud computing

Cloud computing introduces a paradigm shift in how computing resources are provisioned, deployed, and managed. While cloud platforms offer numerous benefits, they also introduce new attack vectors that malicious actors can exploit. Securing cloud environments requires a comprehensive approach, including a strong emphasis on proper configuration, access management, encryption, and ongoing monitoring. Storing or processing data in ways that contravene legal and compliance standards, leading to legal consequences and reputational damage[19]. Malicious insiders abusing their privileges to steal or manipulate sensitive data, disrupt services, or conduct other harmful activities. Conducting malicious activities unnoticed by exploiting the lack of real-time monitoring, making it difficult to detect and respond to security incidents. Leveraging weaknesses in hypervisors, virtual machines, or other shared resources to compromise the security of multiple tenants within the same cloud environment. Password attacks, credential stuffing, or bypassing weak authentication measures to gain unauthorized access to cloud resources. Exploiting vulnerabilities in cloud storage or databases to access, steal, or manipulate confidential information[20]. To mitigate these attack vectors, organizations should implement a comprehensive security strategy that includes robust access controls, encryption, regular security audits, employee training, and collaboration with cloud service providers to address shared responsibility in securing the cloud environment. **Figure 4** elaborates the attack vectors in cloud computing. Exploiting misconfigured access controls, weak authentication, or vulnerabilities in cloud services. Credential theft, unauthorized privilege escalation, or exploiting weaknesses in the ICAM systems[21].

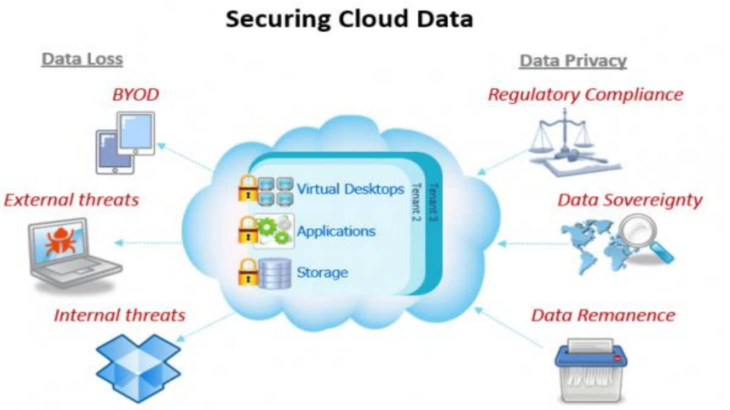

Figure 4. Attack vectors in cloud computing.

5. The security of cloud-based solutions

The conventional security system that is used for on-location programming is disrupted by the capable idea of cloud organizations. Clearly, a cloud-friendly organization cannot guarantee all cloud security. Additionally, cloud clients bear a significant portion of the responsibility. While providing a layered security approach is the most effective method for protecting client data in the cloud, cloud master cooperatives must implement best practices to ensure the highest possible level of cloud security. **Figure 5** defines the flow chart of digital watermarking. The security of cloud-based solutions is a critical aspect that involves safeguarding data, applications, and infrastructure hosted in cloud environments. Cloud security is a shared responsibility between cloud service providers (CSPs) and their customers[22]. Here are key considerations and measures to ensure the security of cloud-based solutions:

- Data encryption: In Transit: Use secure communication protocols (e.g., TLS/SSL) to encrypt data transmitted between users and cloud services. At Rest: Implement encryption mechanisms to protect data stored in the cloud, ensuring that even if unauthorized access occurs, the data remains unreadable without proper decryption keys[23].
- Identity and access management (IAM): Implement robust IAM policies to control user access, privileges, and permissions. Enforce the principle of least privilege to ensure that users have the minimum access required to perform their tasks. Utilize multi-factor authentication (MFA) to enhance user authentication[24].
- Authentication protocols: Deploy strong authentication protocols to ensure the secure identification of users and devices. Regularly update passwords and credentials and educate users about secure authentication practices[25].
- Network security: Implement network security controls, such as firewalls and intrusion detection/prevention systems, to monitor and filter traffic. Segment networks to isolate sensitive data and applications from potential threats[26].

- Incident response and monitoring: Establish an incident response plan to address and mitigate security incidents promptly. Implement robust monitoring and logging capabilities to detect and respond to security events in real-time[27].
- Data residency and compliance: Understand data residency requirements and choose cloud providers that comply with relevant data protection regulations. Regularly audit and assess compliance with industry-specific and regional regulations.
- Regular security audits and assessments: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses. Collaborate with third-party security experts for independent assessments[28].
- Backup and disaster recovery: Implement robust backup and disaster recovery strategies to ensure data availability in case of accidental deletion, data corruption, or other disasters. Test and validate the effectiveness of backup and recovery procedures[29].
- Secure development practices: Adhere to secure coding practices when developing and deploying applications in the cloud. Conduct thorough security reviews during the development of the lifecycle.
- Cloud provider security collaboration: Understand the shared responsibility model and collaborate with cloud providers to ensure security across the entire stack. Regularly review and update service-level agreements (SLAs) to align with security requirements[30].
- Employee training and awareness: Train employees on security best practices, the risks associated with cloud usage, and how to recognize and avoid phishing attacks. Foster a culture of security awareness and responsibility among employees[31].
- Threat intelligence integration: Integrate threat intelligence feeds to stay informed about emerging threats and vulnerabilities. Use threat intelligence to enhance security controls and incident response.
- Container security: If utilizing containerized applications, implement container security practices, including image scanning, runtime security, and secure orchestration. Ensuring the security of cloud-based solutions requires a holistic and proactive approach[32].

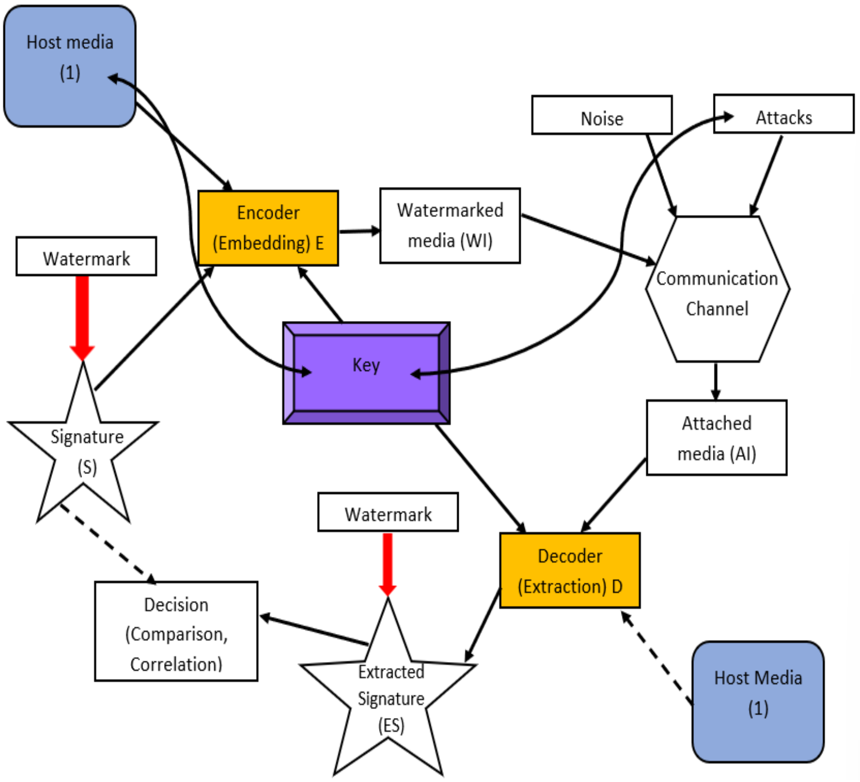

Figure 5. Flowchart for digital watermarking.

6. Proposed methodological structure

The proposed ODWS (Optimized digital watermarking Security system) performs better in compression to the methodology. Duplicate assault is possibly of the most customary assault on superior watermarking. We can reflect on consideration on the watermark as commotion in the first superior signal, the aggressor can some way or some other gauge the first computerized signal. As a count of fact, there are exclusive investigates are about how to channel the introduced substance clamor from computerized signal, this implies the assailants can make use of these new excessive stage exploration result to gauge or get rid of the watermarks. Evacuation assault is one extra standard assault on computerized watermarking. Expulsion assault is performing by using casting off the watermark from the first sign. It contains a ton of strategies, such as denoising, lossy pressure, quantization, demodulation, averaging assaults, and plot are described with the help of **Figure 6**. In the proposed ODWS performs best in the scheduler receives n no of talks for the on-hand property to the quit clients.

1) Step 1: Select the noise and attacks present in the system.
2) Step 2: Do the encoding so that the value of digital may change.
3) Step 3: Set the digital Id and its index value.
4) Step 4: Select the key for the encryption.
5) Step 5: The watermarked key is applied.
6) Step 6: Do the total processing of the digital signed data.
7) Step 7: Applying decoding in the user side to get secure data.
8) Step 8: Repeat the steps 1 to 7 until all the users gets the secure resources.

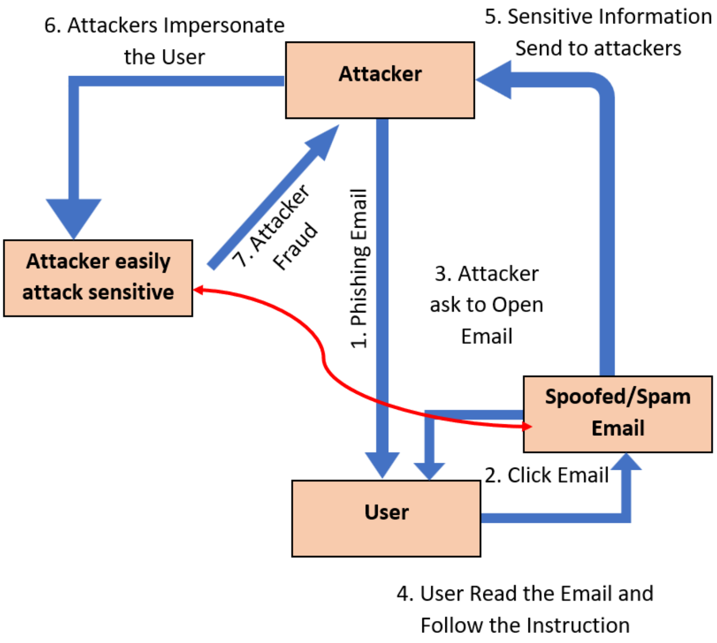
6. Attackers Impersonate the User
5. Sensitive Information Send to attackers
Attacker
7. Attacker Fraud
1. Phishing Email
Attacker easily attack sensitive
3. Attacker ask to Open Email
Spoofed/Spam Email
2. Click Email
User
4. User Read the Email and Follow the Instruction

Figure 6. Flowchart for applying digital watermarking in attacks.

7. Experiments and results

We have compared the proposed demonstrate to the foremost well-known calculations, such as the multi-objective calculation from prior models. DWT stands for Discrete Wavelet Transform, which is a mathematical technique used in signal processing and image compression. The DWT allows signals or images to be decomposed into different frequency components, providing a more compact representation of the data. The DWT is consistent with the bargain with framework that can be seen with ordinary eyes. DWT is based on the concept of Multiresolution Analysis. This means that the signal or image is analyzed at multiple levels of resolution. The decomposition is performed iteratively, resulting in a multilevel representation. In any case, each other flag coherent thought has as of late been utilized, and DWT can ruin the flag in spatiotemporal. The process starts with the original signal or image. The low-pass filter produces an approximation component, representing the overall trends or low-frequency information. The high-pass filter produces a detail component, capturing the high-frequency information or rapid changes. The coefficients obtained from the decomposition represent the contribution of each wavelet function at different scales and positions. These coefficients can be used to reconstruct the original signal or image or to compress the data by discarding less significant coefficients. DWT expansion is a process of decomposing a signal or image into its constituent wavelet components at multiple levels of resolution. This multiresolution analysis provides a powerful tool for various signal processing applications, offering a way to represent and analyze data in a more efficient and meaningful manner. The astounding picture is broken down into four sub-bunches, LL1, HL1, LH1, and HH1, which can be partitioned into littler rehash sub-gatherings and bigger full-size rehash sub-gatherings utilizing DWT. The Discrete Cosine Transform (DCT) is a mathematical transformation widely used in signal processing and image compression. It transforms a signal or image from the spatial domain to the frequency domain. The DCT is often associated with image and video compression standards, such as JPEG for still images and MPEG for video compression. It’s particularly effective in representing signal energy compaction, making it suitable for compression applications. A Fourier-related change, the DCT (Discrete Cosine Change) completely makes utilize of authorized numbers. It seems there might be a mix-up in terminology. The commonly used transform related to the Discrete Fourier Transform (DFT) family is the Discrete Hartley Transform (DHT), not the Discrete Hadamard Change. The DHT is an alternative to the DFT, and like the DFT, it transforms a signal or image into its frequency components. The DHT is particularly useful in applications where real-valued transforms are preferred over complex-valued transforms. DCT is about twice as enormous as DFT (discrete Fourier change), but it was works at a constrained number of authorized discrete insights centers. The Discrete Hadamard Transform is another type of mathematical transform used in signal processing. It is closely related to the Discrete Fourier Transform (DFT) and the Discrete Cosine Transform (DCT). Like the DCT and DFT, the DHT transforms a signal or image from the spatial domain to the frequency domain. It is used in various applications, including image compression and pattern recognition. The DHT (Discrete Hadamard Change) is an indeed alter that’s not sinusoidal. Hadamard capacities are made when a flag is broken up into a huge number of indeed rectangular waveforms. The trade is genuine and does not contain multipliers due to the reality that the wealth of Hadamard components comprises totally of two characteristics, +1 or −1. By keeping in intellect, a modern relationship of ventures for extension, the project’s standard length of time is chosen. Since the schedule is based on suspicions, it may be utilized in any case of whether the expansion is changed, or the ventures aren’t great sufficient.

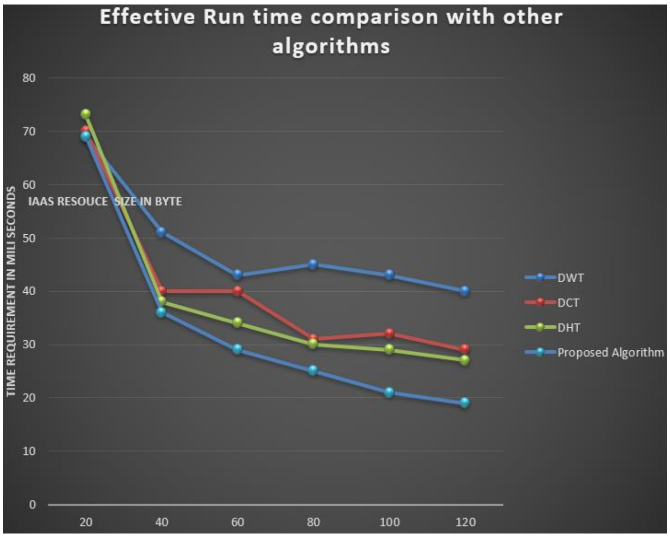

Figure 7. Effective run time comparison with other algorithms.

In our proposed algorithm we have found that our proposed methodology of algorithm is giving better result in term of the complexity and run time as shown in **Figures 7** and **8**.

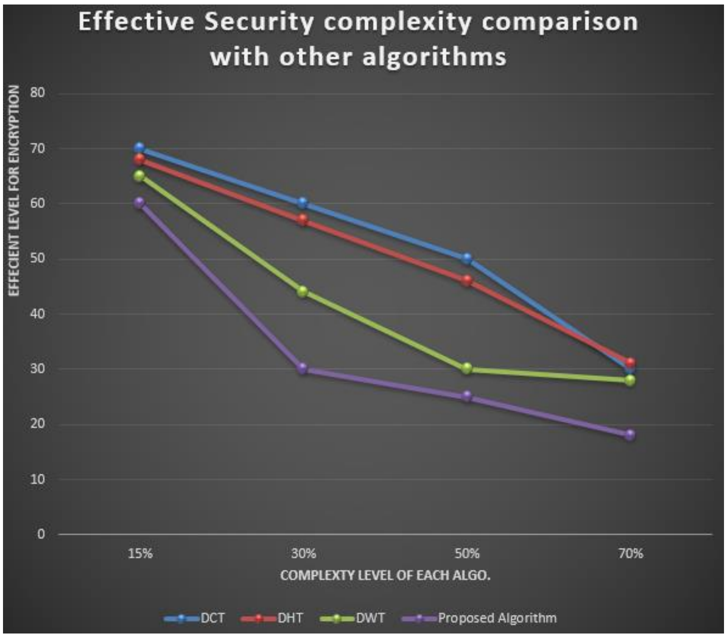

Figure 8. Effective security complexity comparison with other algorithms.

8. Conclusion

In conclusion, integrating digital watermarking into cloud security measures presents a multifaceted approach that enhances the protection, integrity, and traceability of digital assets stored in the cloud. The utilization of digital watermarking technology introduces several benefits and considerations for organizations seeking to bolster their cloud security posture. Most phishing methods are meant to deceive human administrators, and exclusive consumer debts are attractive focuses for cybercriminals. Limiting admittance to frameworks and statistics can aid with safeguarding refined statistics from spillage. Utilize the tenet of least honor and simply provide admittance to consumers who completely want it. The proposed ODWS (Optimized digital watermarking Security system) performs higher in compression to the methodologies like Educate your personnel and behavior education classes with mock phishing scenarios. Digital watermarking serves as a robust method for ensuring the integrity of data in the cloud. By embedding imperceptible watermarks, organizations can detect and respond to unauthorized modifications, providing an additional layer of data protection. With the speedy enhancement of superior innovation, men and women make use of computerized signal to convey, share information and store statistics all the extra regularly, computerized watermarking can supply protection assurance to the two human beings and organizations, and will proceed to foster speedy and anticipate a substantial section later network. In the rapidly evolving landscape of cloud security, the strategic adoption of digital watermarking underscores a commitment to proactive defense. As organizations navigate the complexities of securing their digital assets in the cloud, the combination of encryption, access controls, and digital watermarking emerges as a potent defense against unauthorized access, tampering, and data breaches. In summary, digital watermarking represents a valuable tool in the arsenal of cloud security measures, offering a nuanced and adaptive approach to safeguarding sensitive information in an increasingly interconnected and dynamic digital environment.

Author contributions

Conceptualization, JS and JK; methodology, B, JS and SA; software, MR, SA and JS; validation, JK, B and JS; formal analysis, RRB, SK and SA; investigation, JS and SA; resources, RRB and B; data curation, JS

and JK; writing—original draft preparation, JS and SK; writing—review and editing, SK and RRB; visualization, JS, SK and B; supervision, JS; project administration, RRB and B; funding acquisition, SK. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Syed E. Final Report of Digital Watermarking. University of Texas at Arlington; 2011.
2. Zhou Y, Jin W. A novel image zero-watermarking scheme based on DWT-SVD. 2011 International Conference on Multimedia Technology. Published online July 2011. doi: 10.1109/icmt.2011.6002066
3. Sweeti NM. Similarity Based Technique and Text document classification. International Journal of Advance Engineering Research and Technology (IJAERT). 2016, 4(2): 23-30.
4. Tiwari A, Sharma RM. Potent Cloud Services Utilization with Efficient Revised Rough Set Optimization Service Parameters. Proceedings of the International Conference on Advances in Information Communication Technology & Computing - AICTC '16. Published online 2016. doi: 10.1145/2979779.2979869
5. Sun T, Shao X, Wang X. A Novel Binary Image Digital Watermarking Algorithm Based on DWT and Chaotic Encryption. Young Computer Scientists; 2008.
6. Franklin RV, Manekandan GRS, Santhi V. Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique. International Journal of Computer Applications; 2011.
7. Ramanjaneyulu1 K, Rajarajeswari K. An Oblivious and Robust Multiple Image Watermarking Scheme Using Genetic Algorithm. The International journal of Multimedia & Its Applications. 2010, 2(3): 19-38. doi: 10.5121/ijma.2010.2302
8. Yan Y, Rong H, Mintao X. A Novel Audio Watermarking Algorithm for Copyright Protection Based on DCT Domain. 2009 Second International Symposium on Electronic Commerce and Security. Published online 2009. doi: 10.1109/isecs.2009.141
9. Tiwari A, Sharma V, Mahrishi M. Service Adaptive Broking Mechanism Using MROSP Algorithm. Smart Innovation, Systems and Technologies. Published online 2014: 383-391. doi: 10.1007/978-3-319-07350-7_43
10. Chen L, Li M. An effective blind watermark algorithm based on DCT. 2008 7th World Congress on Intelligent Control and Automation. Published online 2008. doi: 10.1109/wcica.2008.4593967
11. Ameya KN, Raghunath SH. A Blind DCT Domain Digital Watermarking for Biometric Authentication. Intelligent Control and Automation. International Journal of Computer Applications. 2010.
12. Kim J, Won S, Zeng W, Park S. Copyright protection of vector map using digital watermarking in the spatial domain. In: Proceedings of the 2011 7th International Conference Digital Content, Multimedia Technology and its Applications (IDCTA).
13. Taherinia AH, Jamzad M. A new adaptive watermarking attack in wavelet domain. 2009 International Multimedia, Signal Processing and Communication Technologies. Published online March 2009. doi: 10.1109/mspct.2009.5164240
14. Bennour J, Dugelay JL, Matta F. Watermarking attack: BOWS contest. Security, Steganography, and Watermarking of Multimedia Contents IX. Published online February 26, 2007. doi: 10.1117/12.705561
15. Singh S, Chana I. A Survey on Resource Scheduling in Cloud Computing: Issues and Challenges. Journal of Grid Computing. 2016, 14(2): 217-264. doi: 10.1007/s10723-015-9359-2
16. Chang V, Wills G. A model to compare cloud and non-cloud storage of Big Data. Future Generation Computer Systems. 2016, 57: 56-76. doi: 10.1016/j.future.2015.10.003
17. Doja MN, Kumar N. Image authentication schemes against keylogger spyware. In: Proceedings of the 2008 Ninth ACIS International Conference on Software Engineering, Arti_cial Intelligence, Networking, and Parallel/Distributed Computing.
18. Tiwari A, Garg R. Orrs Orchestration of a Resource Reservation System Using Fuzzy Theory in High-Performance Computing. International Journal of Software Innovation. 2022, 10(1): 1-28. doi: 10.4018/ijsi.297923
19. Tiwari A, Garg R. Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems. International Journal on Semantic Web and Information Systems. 2022, 18(1): 1-18. doi: 10.4018/ijswis.306260
20. Tiwari A, Garg R. A Optimized Taxonomy on Spot Sale Services Using Mathematical Methodology. International Journal of Security and Privacy in Pervasive Computing. 2022, 14(1): 1-21. doi: 10.4018/ijsppc.313048
21. Tiwari A, Garg R. Reservation System for Cloud Computing Resources (RSCC). International Journal of Cloud Applications and Computing. 2022, 12(1): 1-22. doi: 10.4018/ijcac.311502
22. Tiwari A, Sharma RM. A Skywatch on the Challenging Gradual Progression of Scheduling in Cloud Computing. Applications of Computing, Automation and Wireless Systems in Electrical Engineering. Published online 2019: 531-541. doi: 10.1007/978-981-13-6772-4_46

23. Kumar Sharma A, Tiwari A, Bohra B, Khan S. A Vision towards Optimization of Ontological Datacenters Computing World. International Journal of Information Systems & Management Science. 2018, 1(2).
24. Tiwari A, Sharma RM. Rendering Form Ontology Methodology for IoT Services in Cloud Computing. International Journal of Advanced Studies of Scientific Research. 2018, 3(11).
25. Rangaiah YV, Sharma AK, Bhargavi T, et al. A Taxonomy towards Blockchain based Multimedia content Security. 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT). Published online December 23, 2022. doi: 10.1109/cisct55310.2022.10046548
26. Rohinidevi VV, Srivastava PK, Dubey N, et al. A Taxonomy towards fog computing Resource Allocation. 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT). Published online December 23, 2022. doi: 10.1109/cisct55310.2022.10046643
27. Singh NK, Jain A, Arya S, et al. Attack Detection Taxonomy System in cloud services. In: Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT).
28. Chouhan A, Tiwari A, Diwaker C, et al. Efficient Opportunities and Boundaries towards Internet of Things (IoT) Cost Adaptive Model. 2022 IEEE Delhi Section Conference (DELCON). Published online February 11, 2022. doi: 10.1109/delcon54057.2022.9753057
29. Theofanos MF, Pfleeger SL. Guest Editors’ Introduction: Shouldn’t All Security Be Usable? IEEE Security & Privacy Magazine. 2011, 9(2): 12-17. doi: 10.1109/msp.2011.30
30. Wiedenbeck S, Waters J, Birget JC, et al. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies. 2005, 63(1-2): 102-127. doi: 10.1016/j.ijhcs.2005.04.010
31. Jain AK, Gupta BB. A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems. 2021, 16(4): 527-565. doi: 10.1080/17517575.2021.1896786
32. Yu C, Li J, Li X, et al. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools and Applications. 2017, 77(4): 4585-4608. doi: 10.1007/s11042-017-4637-6