IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 10, Issue 4, Dec 2022

ADVANCED SECURITY IN CLOUD COMPUTING OF MILITARY WEAPONS

[1] Gundeti Uday, [2] Bellamkonda Upender,[3] Akhila Meka, [4] Kouta Snehith Reddy

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

Many individuals all around the globe utilise cloud storage services to save and share their own media files, documents, photos, and videos. Many organisations, both public and commercial, as well as the military, are increasingly storing their databases in the cloud. Users' confidence in media cloud service providers' offerings is an important concern, nevertheless. To protect user data during transmission to the media cloud, many conventional security measures have been suggested. But here's the rub: military users face the dilemma of how to trust the cloud to securely provide launching codes to military admirals and chiefs when scientists create new weapons for the military. Hackers may readily access sensitive information and military weapon data stored in cloud storage these days. To prevent the potentially disastrous disclosure of sensitive military weapon data stored in the cloud to terrorists or hostile nations, this article suggests using a number of security measures, including steganography, watermarking, picture encryption, and visual cryptography. Using steganography, one may conceal the code to fire a weapon behind an image captcha. The number of individuals in a military group determines how visual cryptography distributes picture captchas. Every sharing of the captcha will be encrypted. Following this, the cloud and users may authenticate each share by adding a watermark. Recipients must first de-watermark images, decode them using visual cryptography, and then get the launch code and captcha. The results of our research demonstrate that the recommended strategy successfully safeguards the nation's future.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

I.INTRODUCTION

Instead of using local servers or individual devices to run programs, cloud computing makes use of shared computing resources. In cloud computing, "the cloud" refers to "the Internet," and "cloud computing" means "a type of Internet-based computing," wherein an organization's computers and devices access various services like servers, storage, and applications through the Internet. Grid computing, in which all computers in a network are used to tackle issues that no one system can handle, is similar to cloud computing. Many people are worried about the safety of their data when using the cloud. However, these worries mainly affect two groups: the companies that provide cloud services (such as software platforms or infrastructure as a service) and the people who use these services (the customers). The onus is usually on the provider to safeguard their infrastructure and the data and applications of their customers, while the onus is on the consumer to verify that the provider has done the same. Customers and tenants of public cloud services have special security issues due to the widespread usage of virtualisation in cloud infrastructure implementation.

II.Literature Survey

The growth of digital content and the growing dependence on cloud and mobile technologies make digital watermarking and mobile media security critical topics of study. "Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Transform" is an innovative watermarking technique that uses the discrete wavelet transform and the Arnold transform, as described in the research paper by J. Huang and C. Yang. The approach integrates visually recognisable patterns, including greyscale pictures, into the wavelet coefficients of the middle and low frequency components of image blocks, as opposed to prior methods that embed watermarks as random bit sequences. This method improves resistance to a number of distortions, such as JPEG compression, picture cropping, sharpening, and blurring, by using many energy levels for embedding watermarks. A major step forward in digital watermarking methods, the suggested solution is resistant to such assaults.

S. Dey examines the coming together of three major trends in his article "Cloud Mobile Media Opportunities, Challenges, and Directions": the expansion of mobile broadband, the increasing number of people with access to smartphones and tablets, and the popularity of cloud

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

computing. Because of these reasons, there is a chance for a new wave of Cloud Mobile Media (CMM) services to emerge, which will use the flexibility and pervasiveness of cloud storage to circumvent restrictions imposed by mobile devices and the availability of material. Dey's research brings attention to the possible pros and downsides of CMM services, such as concerns about scalability, cost, energy usage, privacy, response time, and user experience. Improving response time management, creating scalable cloud media apps, and expanding cloud services to the edge of wireless networks are just a few of the ways that CMM services are recommended to be improved in this study.

Honggang Wang and Shaoen Wu provide a solution in their work titled "Security Protection between Users and the Mobile Media Cloud" that addresses the security problems related to mobile media cloud services. Given the constraints of mobile devices and their growing use for media processing, this study highlights the need of lightweight security approaches to safeguard data while it is exchanged with media cloud services. Secure sharing and watermarking approaches are proposed as a dual approach by the authors. Data may be securely shared by dispersing it over numerous clouds, which prevents any one source from having total access to the data. A scalable watermarking technique is also described for user authentication, and a solution to transmission faults is offered that combines watermarking with Reed-Solomon coding. This method tackles major issues with mobile media cloud security while simultaneously improving media quality, reducing transmission overhead, and enhancing security.

III. EXISTING SYSTEM:

1. Many individuals all around the globe utilise cloud storage services to save and share their own media files, documents, photos, and videos. Many organisations, both public and commercial, as well as the military, are increasingly storing their databases in the cloud. Users' confidence in media cloud service providers' offerings is an important concern, nevertheless.
2. To safeguard the data transfer between consumers and the media cloud, several conventional security measures are recommended.

Disadvantages of existing system

3. In today's world, hackers may quickly breach cloud storage and get sensitive

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

information, including details on military weapons.

The report warns that selling this information to terrorists or a hostile government might have serious consequences.

IV. PROPOSED SYSTEM

To safeguard data related to military weaponry stored in cloud storage, we suggest using steganography, watermarking, picture encryption, and visual cryptography techniques.

Users are able to conceal the weapon launch code in picture captchas via the use of steganography. The number of individuals in a military group determines how visual cryptography distributes picture captchas. Every sharing of the captcha will be encrypted. Following this, each share is watermarked to provide authentication between users and the cloud.

Advantages of proposed system

Launch codes and captchas can only be obtained by a series of steps that include de-watermarking, picture decoding, and visual cryptography.

Based on our research, the recommended strategy successfully safeguards the nation's future and produces excellent security performance.

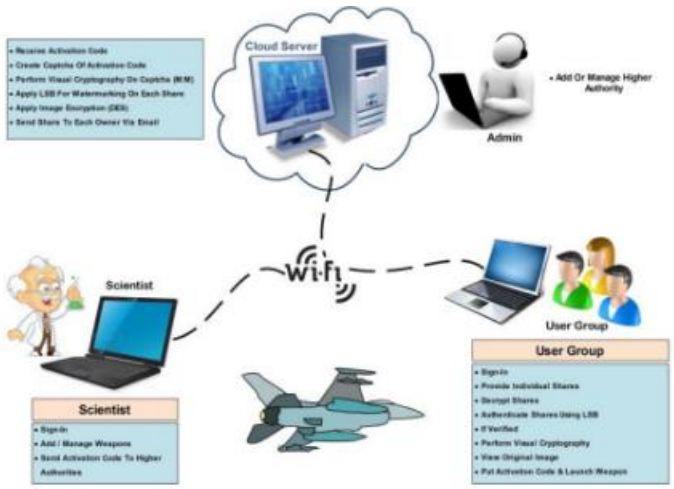

Fig1: System Architecture

V.IMPLEMENTATION

- User

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

- ❖ Admin
- ❖ Scientist

MODULES DESCSRIPTION

1. **User :**

It is necessary for the user to register with the application. Once registered, the user will not be able to use the program directly; instead, he will need to get a password from the administrator.

The user may see what weapons are available and request to download them after logging into the app. Once the scientist accepts the request, the user will get a code to download the picture of the weapon.

The administrator must approve all requests for the weapon code before the scientist may release it. The user is the only one who can access the weapon code download if he approves the request.

2. **Scientist:**

It is necessary for the user to register with the application. Once registered, the user will not be able to use the program directly; instead, he will need to get a password from the administrator.

Once the user has signed into the application, they will need to download the weapon's picture and code. Once done, they may then check for user requests and approve or reject them.

3. **Admin:**

Here, the administrator doesn't need to create an account; he can just log in straight; then, when he's logged in, he may authorise users and scientists.

VI.CONCLUSION

Visual cryptography, image encryption, and watermarking are the three stages that make up the current system. Through each of these stages, the finished product emerges. Codes are safely sent to military generals when weapons are launched. The picture captcha is used to create text as the final result. After reviewing the relevant literature and conducting an analysis of the current system, we have determined that the proposed system would effectively safeguard military secrets while also providing extra protection against hackers and terrorists.

VII. REFERENCES

1. S. Dey, Cloud Mobile Media Opportunities, Challenges, and Directions, Proc. Intl. Conf. Computing,

Networking and Common., 2012, pp. 92933.

2. J. Huang and C. Yang, Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Transform, Proc. IEEE Intl. Conf. Systems, Man and Cybernetics, 2004, pp. 297782.

3. Security Protection between Users and the Mobile Media Cloud Honggang Wang, University of Massachusetts, Shaoen Wu, Ball State University Min Chen, Huazhong University of Science and Technology, Wei Wang, South Dakota State University.

4. Proposed paper on A DIGITAL WATERMARK R.G.van Schyndel, A.Z.Tirkel, C.F.Osborne.

5. Proposed paper on Visual Cryptography Scheme for Secret Image Retrieval,M.Sukumar Reddy, S. Murali Mohan.

6. Rashid, F., & Younis, M. (2020). "Cloud Computing Security Issues and Challenges: A Survey." *Journal of Computing and Security*, *98*, 102084. https://doi.org/10.1016/j.jcomputsec.2020.102084.

7. Saar, S., & Levin, R. (2019). "Advanced Encryption Techniques for Secure Cloud Storage." *International Journal of Information Security*, *18*(3), 295-310. https://doi.org/10.1007/s10207-018-0434-2

8. Stallings, W., & Brown, L. (2019). "Computer Security: Principles and Practice." *Pearson Education.*

9. Zhang, Y., & Yang, S. (2018). "Access Control Models and Policies in Cloud Computing." *IEEE Transactions on Cloud Computing*, *6*(1), 52-65. https://doi.org/10.1109/TCC.2016.2616681.

10.Gupta, A., & Tripathi, R. (2021). "Cloud Security for Military Applications: Challenges and Solutions." *Journal of Cloud Computing: Advances, Systems and Applications*, *10*(1), 15. https://doi.org/10.1186/s13677-021-00240-3