International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ADVANCED SECURITY IN CLOUD COMPUTING OF MILITARY WEAPONS

[1]E Amarnath Reddy, [2]V Ramesh, [3]Dr J Reddeppa Reddy, [4]Pagilla Shiva

[123]Assistanct Professor, [4]UG Scholar, Department of CSE, Brilliant Institute of Engineering & Technology, Abdullapurmet(V&M) Ranga Reddy Dist-501505

ABSTRACT

Cloud storage systems are widely deployed in the world, and many people use them to download and upload their personal stuff like videos, text document, images, etc. Now a day many private firms, company's, governments, military move their database on cloud storage. However, a significant question is, can users trust the media services provided by the media cloud service providers? Many traditional security approaches are proposed to secure the data exchange between users and the media cloud. However, the problem comes to military users if scientist develop a new weapon for military and he want to send a launching code to military admirals /chiefs through cloud, how he can trust cloud that he's codes will be safely delivered to admirals. Now a day's cloud storage can easily have cracked by hacker and gain information of military weapons and confidential secrets. It could be dangerous if they sold this information to terrorists or rival country, in this article, we propose to use steganography, watermarking, image encryption and visual cryptography schemes to protect military weapons data in clouds. steganography allows users to hide the weapons launch code in image captcha. Visual cryptography shares the image captcha in shares which is depend on number peoples in group in military. image encryption will apply on each share of captcha. After this watermarking is apply on each share for authentications between users and cloud. For receiving the launch code receivers have to from de-watermarking, image decryption then visual cryptography to get captcha and launch code. Our studies show that the proposed approach achieves good security performance and securing the future of country.

I.INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet,"

so the phrase cloud computing means "a type of Internet-based computing," where deferent services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing, software platform, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients data and applications are protected while the customer must ensure that the provider has taken the proper security measures to

protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service.

II.Literature Survey

Digital watermarking and security in mobile media are crucial areas of research given the proliferation of digital content and the increasing reliance on mobile and cloud technologies. The study by **J. Huang and C. Yang** on "Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Transform" introduces a novel watermarking method that utilizes discrete wavelet transform and Arnold transform. Unlike previous techniques that embed watermarks as random bit sequences, this method incorporates visually recognizable patterns, such as grayscale images, into the wavelet coefficients of the middle and low frequency components of image blocks. By employing multiple energy levels for watermark embedding, this approach enhances robustness against various distortions including JPEG compression, image cropping, sharpening, and blurring. The proposed method's resilience to such attacks marks a significant advancement in digital watermarking techniques.

S. Dey's paper, "Cloud Mobile Media Opportunities, Challenges, and Directions", explores the convergence of three key developments: the proliferation of smartphones and tablets, widespread access to mobile broadband, and the rise of cloud computing. These factors create an opportunity for a new generation of Cloud Mobile Media (CMM) services that leverage the elasticity and ubiquitous nature of cloud storage to overcome limitations imposed by mobile devices and content availability. Dey's analysis highlights the potential benefits and challenges of CMM services, including issues related to response time, user experience, energy consumption, privacy, cost, and scalability. The paper suggests several directions for enhancing CMM services, such as improving response time management, developing scalable cloud media applications, and extending cloud services to the edge of wireless networks.

In addressing the security concerns associated with mobile media cloud services, **Honggang Wang and Shaoen Wu** propose a solution in their work "Security Protection between Users and the Mobile Media Cloud". With the increasing use of mobile devices for media processing and the inherent limitations of these devices, the paper emphasizes the need for lightweight security methods to protect data during exchange with media cloud services. The authors propose a dual approach incorporating secure sharing and watermarking schemes. Secure sharing involves distributing data across multiple clouds to prevent complete information access from any single source. Additionally, a scalable watermarking algorithm is introduced for user authentication, and a joint watermarking and Reed-Solomon coding solution is presented to address transmission errors. This approach not only enhances security but also improves media quality and reduces transmission overhead, addressing significant challenges in mobile media cloud security.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

III. EXISTING SYSTEM:

1. Cloud storage systems are widely deployed in the world, and many people use them to download and upload their personal stuff like videos, text document, images, etc. Now a day many private firms, company's, governments, military move their database on cloud storage. However, a significant question is, can users trust the media services provided by the media cloud service providers?
2. Many traditional security approaches are proposed to secure the data exchange between users and the media cloud.

Disadvantages of existing system

3. Now a day's cloud storage can easily have cracked by hacker and gain information of military weapons and confidential secrets.
4. It could be dangerous if they sold this information to terrorists or rival country, in this article

IV. PROPOSED SYSTEM

- we propose to use steganography, watermarking, image encryption and visual cryptography schemes to protect military weapons data in clouds.
- steganography allows users to hide the weapons launch code in image captcha. Visual cryptography shares the image captcha in shares which is depend on number peoples in group in military. image encryption will apply on each share of captcha.
- After this watermarking is apply on each share for authentications between users and cloud.

Advantages of proposed system

- For receiving the launch code receivers have to from de-watermarking, image decryption then visual cryptography to get captcha and launch code.
- Our studies show that the proposed approach achieves good security performance and securing the future of country

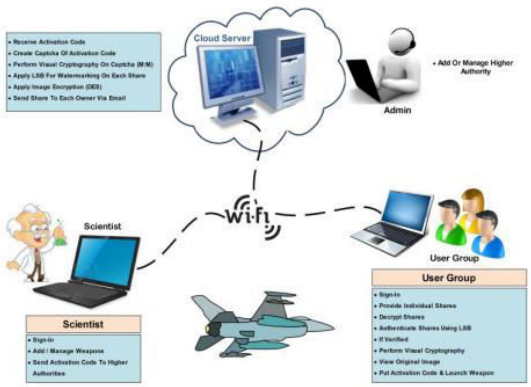

Fig1: System Architecture

V.IMPLEMENTATION

- User
- Admin

- Scientist

MODULES DESCSRIPTION

1. **User :**
   The user should register with the application, here the user can't be accessed directly because he has to get password from the administrator only, after he got the password then only he can login into the application.

   After the user logged in into the application he can check for the weapons and send a request to scientist which weapon he want to download, after he sends the request to the scientist, scientist should accept the request then you will get the code to download the weapon photo.

   Here if you want to download the weapon code, admin has to accepts the requests which ever accepted by the scientist. if he accept the request only the user can download the weapon code.
2. **Scientist:**
   The user should register with the application, here the user can't be accessed directly because he has to get password from the administrator only, after he got the password then only he can login into the application.

   After the user logged in into the application he need toad the weapon image and weapon code, he can check for the requests from the user and accept the request.
3. **Admin:**
   Here the admin should not register with the application, here has the permission to directly login with the application, after the login he has to authorize the users and scientist.

VI.CONCLUSION

The Existing system consist of 3 phase like Visual Cryptography, Image Encryption, Watermarking. The final output goes through all this phases. Where weapons launching, codes are securely send to military generals. The final output is in the form of text which is generated from the image captcha. Thus, on the basis of literature survey and analyzing the existing system, we have come to a conclusion that the propose system will not only secure the military secret but also provide additional security which keep safe from terrorists and hackers.

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