ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

THE FUTURE OF MILITARY WEAPON SECURITY IN THE CLOUD

Ms.Manasu Madhavi[1], pooja[2], soumya [3], Shreya reddy[4]

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

[1]Assistant Professor, Department of CSE ,Malla Reddy Engineering College for Women,Hyderabad, manasumadhavi@gmail.com
[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, India.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

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.

PERFORMANCE ANALYSIS

This application will be able to connect to the Cloud database and take the input through Graphical User Interface. The Application will be able to generate weapons launching code which is in text format will hide in image captcha. after this image captcha, will breaks into shares. After making shares using visual cryptography. after this watermarking is applied on each pixel of image shares. image encryption is applied to encrypt image shares. after all this process shares are send through email. When it's come to receive mail, decryption is applied on each share then Dewater marking is applied after this visual cryptography is done to collect share and generate original image. Then stenography is used to get hidden weapons launching codes from image captcha. This are the expected result in our project.

PROBLEM DEFINATION

The unauthorized disclosure of personal information, secret government documents, and confidential details concerning our country's defense and military operations has emerged as a critical issue in today's digital age. With the prevalent use of cloud storage, the risk of hackers gaining access to sensitive data has escalated, posing a serious threat to national security. Various methods have been suggested to counteract this menace, emphasizing the urgent need for enhanced security measures. Introducing a multitude of advanced techniques in cybersecurity is pivotal to addressing the current challenges effectively. By implementing robust encryption protocols, multi-factor authentication, and regular security audits, we can fortify our defenses against cyber threats and safeguard critical information from unauthorized access. It is imperative to stay ahead of evolving cyber threats by continually innovating security strategies to protect our nation's confidential assets and uphold the integrity of our defense and military operations.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

II. LITERATURE SURVEY

1. Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Transform, J. Huang and C. Yang, Watermarking is a technique for labeling digital picture by hiding secret information in the images. This paper presents a method of watermark embedding and extracting based on discrete wavelet transform of blocks and Arnold transform. Different with most previous work, which uses a random number of a sequence of bits as a watermark, the proposed method embeds a watermark with visual recognizable patterns, such as gray image in images. In the proposed method, each pixel of watermark is embedded in the wavelet coefficient of the middle and low frequency of a block in the images. Unlike other watermarking techniques that use a single casting energy, this method casts watermarks in multi-energy level. The performance of the proposed watermarking is robust to variety of signal distortions, such a JPEG, image cropping, sharpening, and blurring attacks.

2. Cloud Mobile Media Opportunities, Challenges, and Directions, S. Dey.,Three recent developments - increasing adoption of smart phones and tablets as desired platforms for infotainment, increased access to mobile broadband networks globally, and availability of public Clouds - are aligning to possibly enable a new generation of truly ubiquitous multimedia services on mobile devices: Cloud Mobile Media (CMM) services. Such services will be able to avail of the elasticity of cloud computing and ubiquity of cloud storage, and thereby not constrained either by mobile device capabilities, or availability of content. In this paper, we look at early trends in CMM services, and opportunities and benefits for new CMM services in the near future. We analyze the possible impact of such services, and issues that need to be addressed to make CMM services viable, including response time, user experience, energy, privacy, cost and scalability. We provide several directions for possible solutions, which include developing response time management techniques, scalable cloud media application, and cloud user experience measurement techniques. We also propose extending the Cloud beyond the traditional Internet to the edge of the wireless networks.

3. Security Protection between Users and the Mobile Media Cloud ,Honggang Wang, University of Massachusetts, Shaoen Wu, Mobile

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

devices such as smartphones are widely deployed in the world, and many people use them to download/upload media such as video and pictures to remote servers. On the other hand, a mobile device has limited resources, and some media processing tasks must be migrated to the media cloud for further processing. However, a significant question is, can mobile users trust the media services provided by the media cloud service providers? Many traditional security approaches are proposed to secure the data exchange between mobile users and the media cloud. However, first, because multimedia such as video is large-sized data, and mobile devices have limited capability to process media data, it is important to design a lightweight security method; second, uploading and downloading multi-resolution images/videos make it difficult for the traditional security methods to ensure security for users of the media cloud. Third, the error-prone wireless environment can cause failure of security protection such as authentication. To address the above challenges, in this article, we propose to use both secure sharing and watermarking schemes to protect user's data in the media cloud. The secure sharing scheme allows users to upload multiple data pieces to different clouds, making it impossible to derive the whole information from any one cloud. In addition, the proposed scalable watermarking algorithm can be used for authentications between personal mobile users and the media cloud. Furthermore, we introduce a new solution to resist multimedia transmission errors through a joint design of watermarking and Reed-Solomon codes. Our studies show that the proposed approach not only achieves good security performance, but also can enhance media quality and reduce transmission overhead.

III. EXISTING SYSTEM:

- 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?

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

- Many traditional security approaches are proposed to secure the data exchange between users and the media cloud.

Disadvantages of existing system:

- 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

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

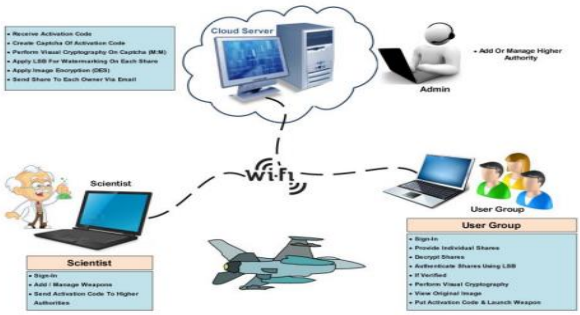


Fig1: System architecture

V. IMPLEMENTATION

MODULES:

- User
- Admin
- Scientist

MODULES DESCSRIPTION:

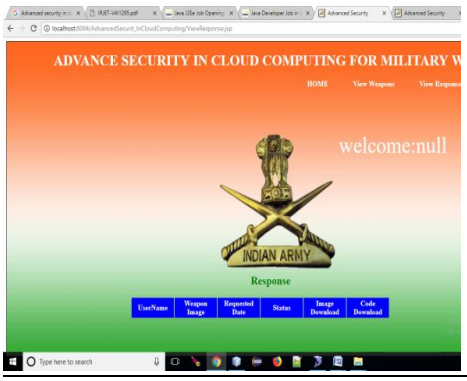
1.User :

The user should register with the application, here the user can't be accessed directly because he has to get

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issue 1 Jan 2024

password from the administrator only, after he got the password then only he can login into the application.

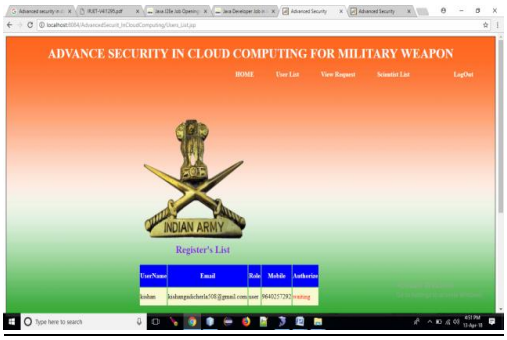
After the user logged in into the application he can check for the weapons and send a request to scientist which weapon he want to download, after he sends the request to the scientist, scientist should accept the request then you will get the code to download the weapon photo.



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.

1. **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.



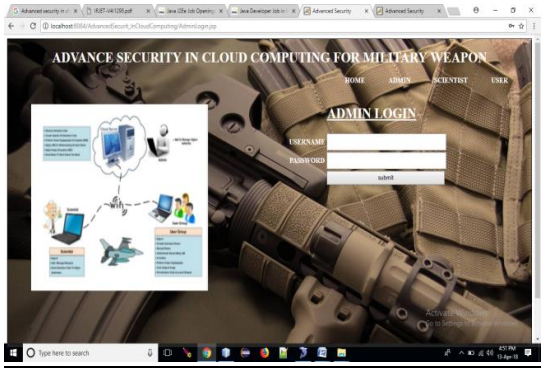
After the user logged in into the application he need toad the weapon image and weapon code, he can check for the requests from the user and accept the request.

2.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.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024



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