**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.

**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?
* 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

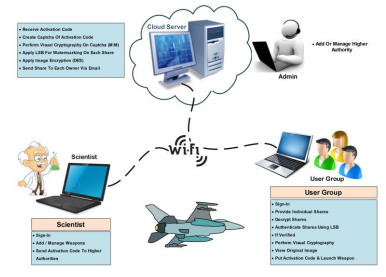
**PROPOSED SYSTEM:**

* 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

System Architecture:



**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.