International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

ADVANCE SECURITY IN CLOUD COMPUTING FOR MILITARY WEAPONS

Akash Bagul[1], Puja Sonawane[2], Laxmi Sawant [3], Rohit Doshi[4]

Department of Computer Engineering

AISSMS College of Engineering

Shivajinagar, Pune 01

Guide: Professor Amol Jagtap

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.

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.

1.1 Problem Statement

Leaking of personal information, secret government document, confidential secrets about our country defense, military secret is now a day big serious problem facing today. Uploading an information on cloud can now easily hacked by hackers. Several methods have been proposed in order to combat this. Providing more techniques in security could solve the problem that we facing today.

1.2 Purpose

The aim of the project is to provide high security in cloud for Military including multiple organizations for their confidential information. It also

provides high security for Militaries Confidential work or project from Terrorists and Enemy hackers.

2. Literature Survey

Now a day security in private and public cloud is main issue. Now a day almost all the small scale to large scale companies, government, military are now uploading their data on cloud. But their data is not safe on cloud either until there is some security majors. But there is lack of security in cloud storage. Some security is not up to mark to stop hackers from stealing information and data. There are some algorithms and methodologies are used to provide security but those aren't enough. Only one or two algorithms won't help to provide security. There has to be at least more than 3 or 4 algorithms which will work together to provide maximum security for data for Military and other Organizations.

3. Proposed System

As our application is for Providing security in cloud for militaries weapons code so we added three methodologies and algorithms to maximize security level on cloud.

Our Application comprises of modules which are as follows:

- **Admin: -**

  In our application admin is tier with cloud server, and his job is to add and manage accounts of higher authorities.

- **Scientist: -**

  In our application, Scientist job is

  1.Sign in

  2.Add/Manage Weapons

  3.Send activation codes to higher authorities

- **Cloud Server: -**

  All the methodologies and algorithms are applying in this module for providing security to text weapon code. Following are the operations which is applying in this module.

  1.Recieve activation code.

  2.Create Captcha of Activation code.

  3.Perform Visual cryptography on captcha(M:M)

  4.Apply LSB For Watermarking on each share

  5.Apply Image Encryption(AES)

  6.Send share to each owner via Email.

- **User Group: -**

  In this module, we getting actual code. for getting this code following operations take place.

  1.Sign-in

  2.Provide individual shares.

  3.Decrypt shares

  4.Authenticate shares using LSB

  5.If Verified

  6.Perfrom Visual Cryptography

  7.View Original Image

  8.Put Activation Code & Launch Weapon

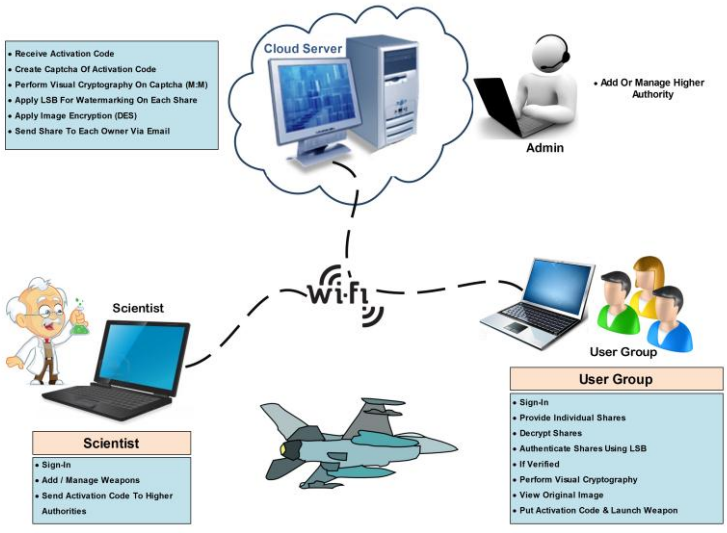

Fig.1:- Propose System Architecture

4. Results & Discussions

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 De-watermarking 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.

5.Future scope

This application currently for military use but this application or techniques we used in this application can be used for Government, Banking Corporation, Medical Research also.
This application is focused on private cloud storage but it can be used for public cloud also for that we need to make some changes in code and methodology.
This application is for windows platform but for future it can come in android and iOS.

6. 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.

7.Acknowledgement

We would like to thank the publishers, researchers and teachers for their guidance. We would also thank the college authority for providing the required infrastructure and support. Last but not the least we would like to extend a heartfelt gratitude to friends and family members for their support.

8.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.