Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

A secure mutual authentication protocol for Cloud computing using secret sharing and Image steganography

Sagar Khatal[1], Akshay Kadhane[2], Ravi Moon[3] , Prof. Imran Tamboli[4]

[1,2,3,4] *Computer Engineering, Dr.D.Y Patil College of Engineering, Ambi*

Abstract — *Cloud computing is a collection of virtually massive distributed large scale computers to handle enormous Enterprise computing, hardware, storage needs. An exponential advancement of communication and information technologies results in substantial traffic for accessing of cloud resources wired and mobile, through various communication devices like desktop, laptop, tabs, etc. via Internet. Significance of enterprise data and increased access rates from low-resource terminal devices demands for reliable and low cost authentication techniques. Lots of researchers have proposed authentication schemes based on password, biometric, steganography etc. with varied efficiencies. In 2014, Nimmy et al proposed a steganography based mutual authentication protocol for cloud computing and claimed that their scheme resists major cryptographic attacks. Unfortunately, in this paper we will show that Nimmy et al is vulnerable to offline password guessing attack and Denial of Service attack. As a part of our contribution, we propose a low cost steganography based authentication scheme which is strongly secure and best suited for asymmetric cloud computing environment.*

Keywords- *Steganography, Mutual Authentication, Cloud security, Mobile cloud*

I. INTRODUCTION

Cloud computing is a distribution of standard computing services where dynamically accessible and virtualized resources are delivered as a service across the internet. The Cloud services deliver lot of advantages especially in ubiquitous services, in which everybody can access computing services provided over Internet. Besides many assistances that the cloud computing has presented, the information security is the major barrier which makes the user worried of. According to the NIST definition, cloud computing is a delivery model that enables convenient instant network access to a pool of shared configurable computing resources that can be quickly provisioned and released. Cloud model supports availability of resources and has many characteristics such as on-demand self-service distributed network access, resource pooling measured service and rapid elasticity.

II. RELATED WORK

Authors introduced a handwriting authentication system. This process allows users to access restricted data in the Cloud using a mobile phone with security. It is composed of pre-processing, feature extraction, classification and Authentication process. The classification method is predicated on three completely different classification techniques: ANN, KNN, and Euclidean Distance classifier. The classifier algorithmic program employs parallel combination of Classifiers so as to attain satisfactory accuracy on each recognition and error rate.

The combination of the cloud computing and mobile computing creates mobile cloud computing and additionally Introduce security threats appreciate unauthorized users access. The authors focus during this analysis is on the Mobile cloud and protective mobile cloud resources from illegitimate access. Biometric recognition are going to be Employed in the close to future in mobile devices. The projected solution by authors for authenticating mobile cloud users' exploitation the present mobile device camera as a fingerprint sensing element to get a fingerprint image, then process it and recognize it. Results show that the proposed solution has supplementary value to stay performance at an accepted level.

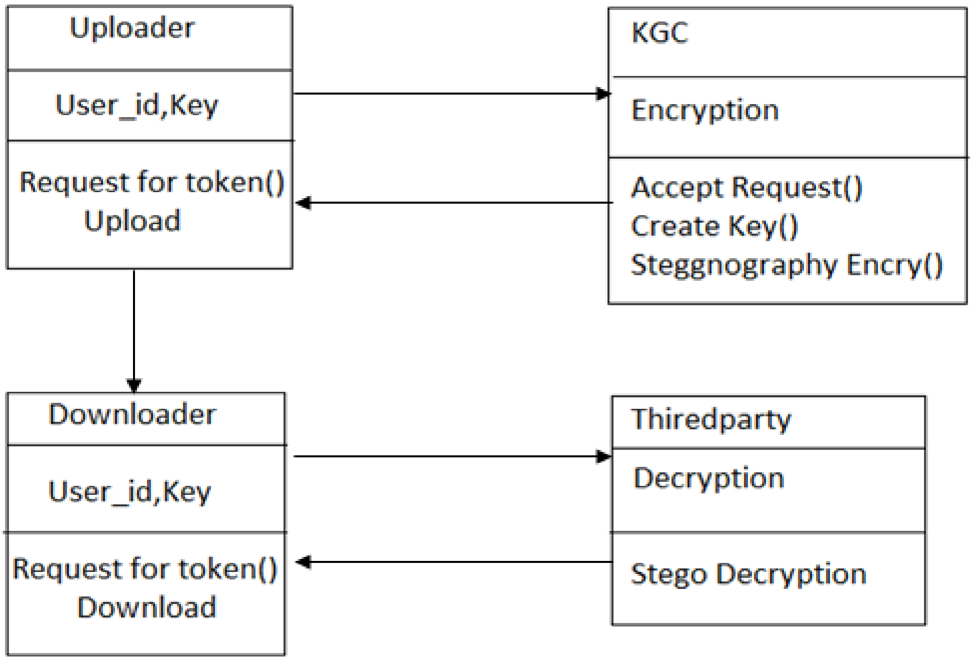
In this paper , authors propose an easy and effective on-line signature verification system that's appropriate for user authentication on a mobile device. The advantages of the proposed algorithm are as follows. First, a histogram based mostly feature set for representing an online signature are often derived in linear time and also the system needs a little and fixed-size area to store the signature model. Additionally, since the feature set represents solely statistics concerning distribution of original on-line signature attributes, the transformation is non-invertible. As a result, the privacy of the first biometric information is well-protected. Second, a user-specific classifier comprising of a user specific quantization step size vector and its associated measure feature vector are often trained victimization only enrollment samples from that user while not requiring a training set from an outsized variety of users. Many experiments performed on MCYT and SUSIG datasets express effectiveness of the proposed technique in terms of verification performance as compared to existing algorithms.

Security analysis of on-line signature verification system as compared to it of 4-digits PIN and two usability metrics is additionally given. additional investigation includes the utilization of alternative biometric key binding approaches, like fuzzy commitment, so as to strengthen security of the system, even once stored templates, helper information etc., are compromised, whereas protective verification performance. Lastly, it's possible to derive a fusion approach by combining the proposed technique with alternative existing approaches, e.g., DTW, HMM-based, etc., in order to enhance verification performance, particularly for applications wherever privacy of the signature traits is a smaller amount crucial.
In this paper , authors examine whether or not people could guess the hand-drawn images which were used as the graphical password of others, if they know some cultural information about the users, such as their religion or even their hopes or where they came from. The analysis also aims to contribute evidence of a bias in the user choice of images and considers the impact this could have on guess ability. However, the results analysis shows that there is no dissimilarity between males and females and between members of different cultures in their ability to guess images.
One clear result of this work is that it is apparently extremely potential to guess other people's selected images if they contain cultural characteristics, especially religious marks, otherwise it is much more difficult to presume them. Also the authors provide Guidelines in this paper for drawing a secret password.
Authors proposed a completely unique mutual authentication protocol for cloud computing victimization secret sharing and steganography during this paper . The protocol is intended in such some way that it uses steganography as an extra encryption theme. The theme achieves authentication victimization secret sharing. Secret sharing permits a region of the secret to be unbroken in either side that once combined becomes the entire secret. The secret contains data concerning each parties concerned. Further, out of band authentication has been used that provides extra security.
According to the difficult problems throughout the user authentication and access management method in cloud-based environments, an efficient and scalable user authentication theme was proposed during this paper . It the advised model, numerous tools and techniques were introduced and employed by victimization the conception of agent.
Therefore, a client-based user authentication agent was introduced to verify identity of the user in client-side.
Moreover, a cloud-based software-as-a service application was wont to make sure the method of authentication for unregistered devices.
In this paper, authors knew a brand new privacy challenge during information accessing within the cloud computing to realize privacy-preserving entry level authority sharing. Authentication is confirmed to ensure information confidentiality and information integrity. Data obscurity is achieved since the wrapped data are changed throughout transmission.
User privacy is increased by unknown access requests to separately inform the cloud server concerning the users' access needs. Forward security is complete by the session identifiers to
stop the session correlation. It indicates that the proposed theme is probably applied for privacy preservation in cloud applications.
In this paper , authors present a survey of recent trends to automatic recognition of human facial behavior using soft computing. Soft computing is the most attractive field nowadays.
Soft computing proves effective techniques to the problem of classification, prediction, optimization, pattern recognition, image processing, etc. The facial behavior recognition processes in three steps in general. Face detection is the process of identifying face from images. Feature extraction is a process of highlighting the facial part that takes part in identification of expression and last a classifier is design that identifies the expression. There are a lot of effective methods are there to detect face expression, but no method performs best in all types of situation. Each method has their limitations. The future of human facial behavior recognition system is to make a robust system that will perform efficiently in any circumstances. Application developers may face with a adverse set of scenarios, each with its own identity solution without claim based identity. Claim-based identity helps in providing a consistent answer across a wide range of scenario of cloud services. By building and deploying claim-based applications besides existing application result in simpler migration. Claim-based identity is not for only Microsoft vendors-many vendors are involved. In this paper , authors show why claim-based identity solutions are required and how to use by the cloud service provider in cloud applications.

III. PROPOSED SYSTEM

We propose a simple and elective approach for Image Steganography and Mutual authentication. The Image Steganography is being used for hiding the data and keeping the privacy of that File/document. The privacy is generated by applying differential Evolution algorithm. The algorithm is being used to generate the document as image and again retrieve it as document. The future plan is to generate the image steganography by providing key generation. This device can be used to share documents. Private detectives Security, Digital information security. We can achieve the goals. like Correctness: Data can be stored correctly within images, Availability: An authorized user can retrieve the information from an image when required. 3. Protection: It is fully protected from unauthorized user because, perceiving an image does not provide any idea of the original information.

IV. SYSTEM ARCHITECTURE



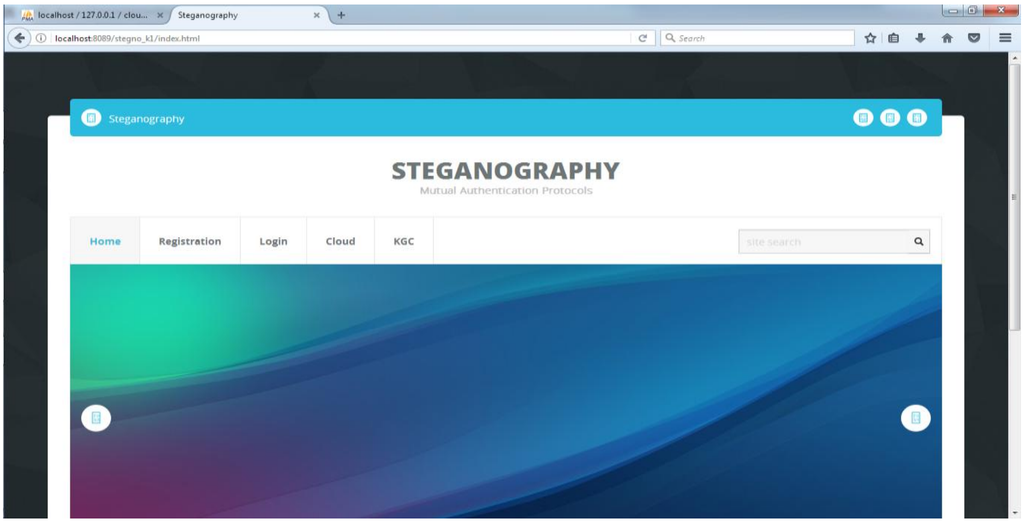
Flow of the Project:

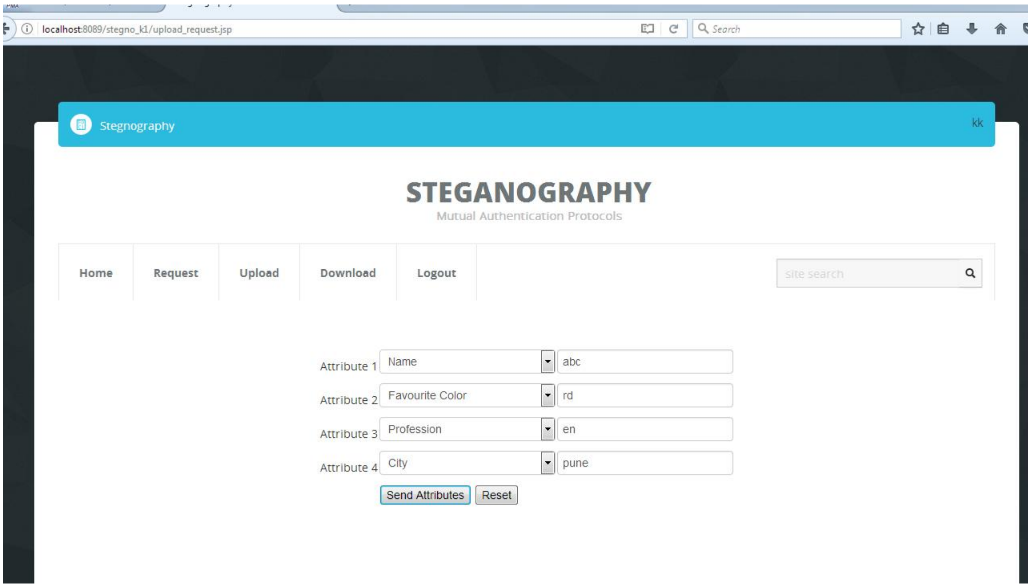
The complete work flow of the method is as follow:
Step 1: Get the data or information which is going to be on cloud infrastructure.
Step 2: Now choose any image, and apply differential evolution algorithm.
This will perform an intelligent segmentation process and will differentiate
Between objects and background of the image.
Step 3: Now the encryption key will be generate by using segmented objects
Of the image.
Step 4: Encryption will be process using the generate key.
Step 5: System will use KDC for third party authentication.
Step 6: Cloud computing infrastructure will communicate with both KDC
And PKI for the secure transaction of data and information over the network.

V. Database Description

Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity. The term database design can be used to describe many different parts of the design of an overall database system. Principally, and most correctly, it can be thought of as the logical design of the base data structures used to store the data. In the relational model these are the tables and views. In an object database the entities and relationships map directly to object classes and named relationships. However, the term database design could also be used to apply to the overall process of designing, not just the base data structures, but also the forms and queries used as part of the overall Database application within the DBMS

VI. Snapshots


localhost / 127.0.0.1 / clou...
Steganography
localhost:8089/stegno_k1/index.html
Search
Steganography
STEGANOGRAPHY
Mutual Authentication Protocols
Home
Registration
Login
Cloud
KGC
site search

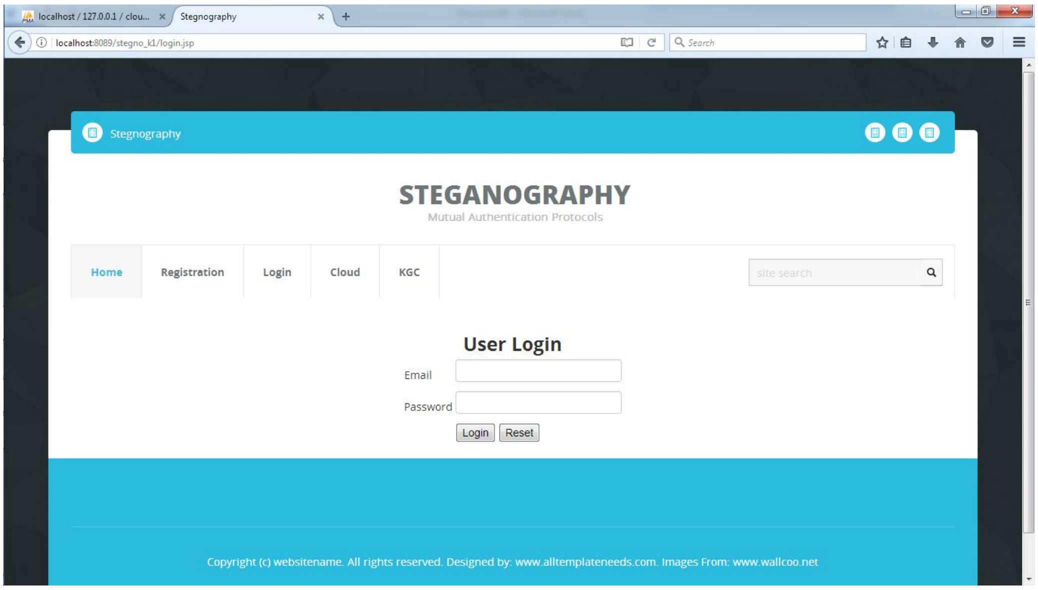


Attribute 1 Name abc

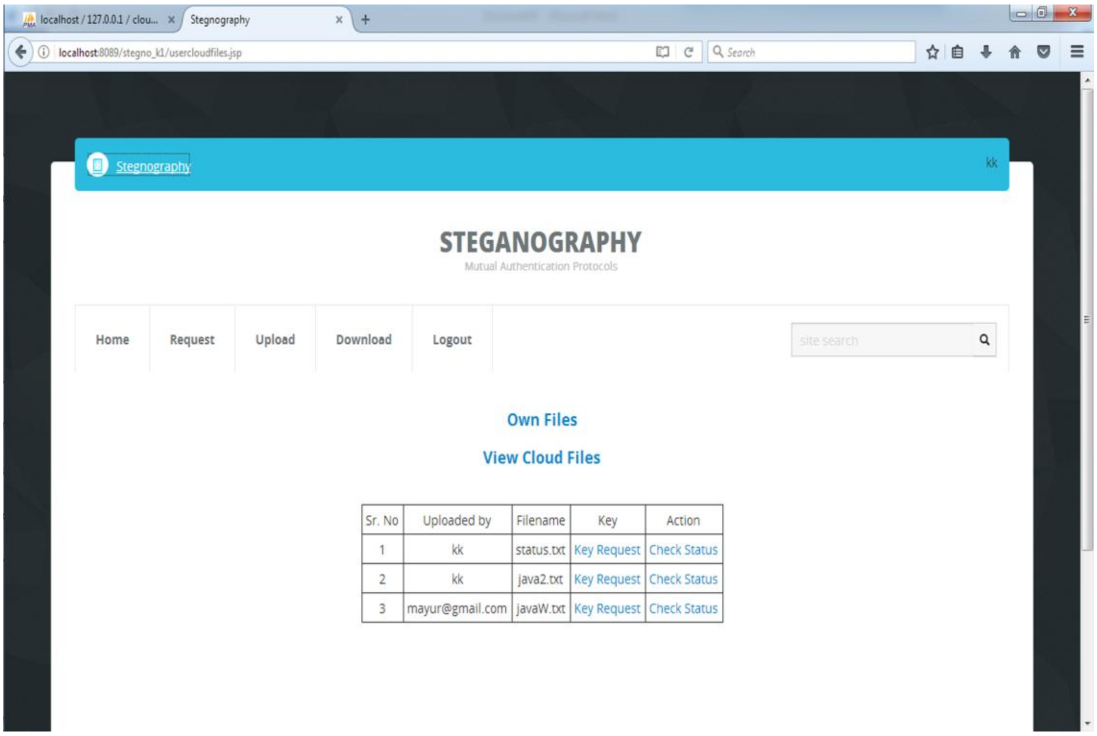
Attribute 2 Favourite Color rd

Attribute 3 Profession en

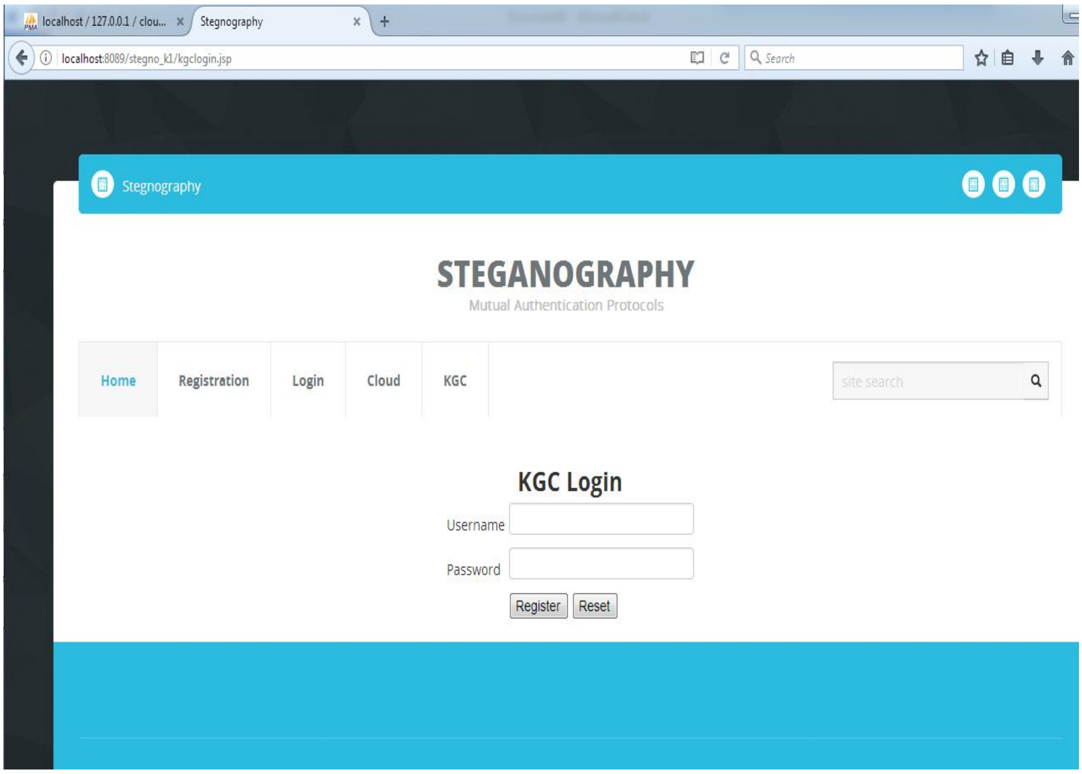
Attribute 4 City pune



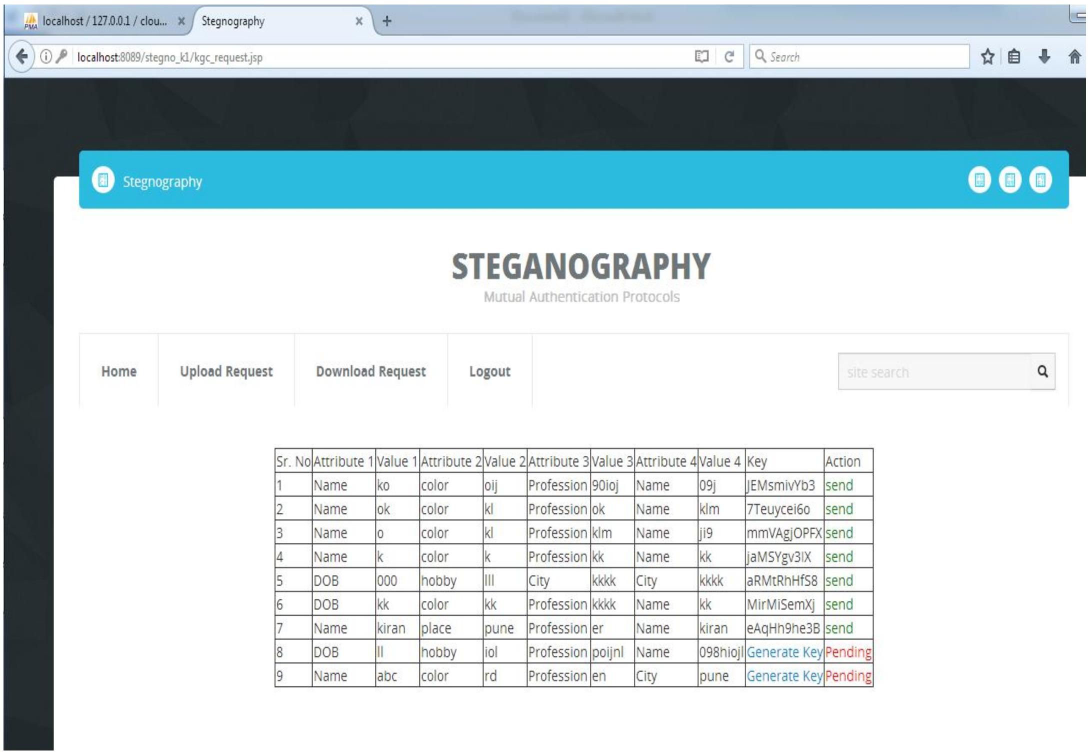
Copyright (c) websitename. All rights reserved. Designed by: www.alltemplateneeds.com. Images From: www.wallcoo.net



Sr. No	Uploaded by	Filename	Key	Action
1	kk	status.txt	Key Request	Check Status
2	kk	java2.txt	Key Request	Check Status
3	mayur@gmail.com	javaW.txt	Key Request	Check Status



Username
Password


localhost / 127.0.0.1 / clou...
Stegnography
localhost:8089/stegno_k1/kgc_request.jsp
Search
Stegnography
STEGANOGRAPHY
Mutual Authentication Protocols
Home
Upload Request
Download Request
Logout
site search

Sr. No	Attribute 1	Value 1	Attribute 2	Value 2	Attribute 3	Value 3	Attribute 4	Value 4	Key	Action
1	Name	ko	color	oij	Profession	90ioj	Name	09j	JEMsmivYb3	send
2	Name	ok	color	kl	Profession	ok	Name	klm	7Teuycei6o	send
3	Name	o	color	kl	Profession	klm	Name	ji9	mmVAgjOPFX	send
4	Name	k	color	k	Profession	kk	Name	kk	jaMSYgv3IX	send
5	DOB	000	hobby	lll	City	kkkk	City	kkkk	aRMtRhHfS8	send
6	DOB	kk	color	kk	Profession	kkkk	Name	kk	MirMiSemXj	send
7	Name	kiran	place	pune	Profession	er	Name	kiran	eAqHh9he3B	send
8	DOB	ll	hobby	iol	Profession	poijnl	Name	098hiojl	Generate Key	Pending
9	Name	abc	color	rd	Profession	en	City	pune	Generate Key	Pending

VII. Conclusion

To ensure information and data privacy over the cloud, application is encrypting the user data before sending it over the cloud. Hackers and crypt analyst are capturing the data using various illegal practices over the communication network. In this paper we have proposed a method, where data is encrypted using image as encryption key and to generate this encryption key from image, we used differential evolution algorithm for multi-level segmentation. Results are compared with other nature inspired algorithms.

VIII. References

[1] V. K. Zadiraka and A. M. Kudin, "Cloud computing in cryptography and steganography", springer journal of Cybernetics and Systems Analysis, Volume 49, Issue 4, pp 584-588,July 2013.

[2] S. Subashini, and V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Elsevier Journal of Network and Computer Applications, vol 34, pp: 1–11, 2011.

[3] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M.Freire, and P. R.M. Inácio , "Security issues in cloud environments: a survey", springer international Journal of Information Security, Volume 13, Issue 2, pp 113-170, April 2014.

[4] E. Aguiar,Y.Zhang and M.Blanton, "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security", springer journal of High Performance Cloud Auditing and Applications pp 3-33, 2014.

[5] Q. Gu, and M. Guirguis. "Secure Mobile Cloud Computing and Security Issues", Springer: High Performance Cloud Auditing and Applications, pp 65-90, 2014.

[6] K.Murakami,K. Hanyu, R. Q. Zhao, and Y.Kaneda,"Improvement of security in cloud systems based on steganography", International Joint Conference on Awareness Science and Technology and Ubi Media Computing, pp:503 - 508, 2-4 Nov. 2013.

[7] A.B. Ramachandran, P.Pradeepan, and M.Saswati," Security as a Service using Data Steganography in Cloud", The International Conference on Cloud Security and Management , Washington University, Seattle, USA, Oct 17-18,October 2013.

[8] I.M.Khalil, A.Khreishah, M.Azeem, "Cloud Computing Security: A Survey", MDPI: Computers, vol 3, pp:1-35, 2014.