Akshat Agrawal el al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 3, September 2015, pp. 130-138

Detection of Object using coloring scheme

Akshat Agrawal

Department of CSE, Amity School of Engineering & Technology, Amity University. Manesar, Haryana

Abstract— **Obstacle detection is a main key of independent systems. In the case when communicating with huge robots in unstructured background, resilient obstacle detection is required. The methods aremainly suited for background in which the ground is comparatively flat and of roughly the same color. The procedure uses a submissive monocular camera, performs in real-time, and produces a binary obstacle image at high resolutions. We use the technique like the homography between two frames captured from the succession and after that develop a systematic algorithm for the calculation so that the centeroid of the detected object is triangulated so as to estimatethe distance. Weexamine a difficultyintrinsic to any homography-based outlook to the provided task, and show how the discussed way can locate this difficulty to a huge level. An obstacle system based on visual particular attribute and stereo vision is expressed.**

Keywords- **Image Segmentation, Centroid, Thresholding, Fundamental Matrix calculate and Triangulation).**

I. INTRODUCTION

As the technology increases day by day difficulties also increases with respect to safety in any path between object and obstacle, so obstacle detection is the methodology that refers to ability to detect the obstacle that appears in between the desired destination or any other object. Obstacle detection is a methodology that helps to human-being, vehicles; robots etc. to take decision so that they can be save when there is any obstacle in their path. Generally an obstacle is a thing, condition that creates barrier. Any impediment is planned to stop, halt, and turn the movement of an opposing force. An obstacle can be natural or it can be made by any man or it may be that it is combination of both. So there are many type of obstacle such as physical, political, economic. Before sometimes, generally when use hardware and white cane to detect any obstacle so there occur some problem with these methods. Because hardware uses sensors to detect obstacle and sensors are very costly i.e. economically problem and other problem of sensor requires computationally very high to detect. The problem of second one is that it cannot detect overhanging obstacle so this is not also feasible. So color based technique is a solution to above problems. The main objective of this work is to detect the obstacle on the basis of color cue. Any obstacle is detected by its color and position from monocular camera. Position can be calculated by distance. Other proposed algorithm has developed on the basis of color only. Triangulation method in this work will help detect the orientation of two frames of same image so that distance can be detected .So distance between one of the frame and camera can be evaluated. Take two images from camera and segment it into Taking Centroid for two consecutive frames so that can be detect the orientation of camera or some changes that can be held due to noise. This work describes an obstacle detection algorithm for use in relatively flat areas where there is similarity in color. In computer vision triangulation refers to the process of determining a point in 3D space given its projections onto two, or more, images. This point is an interested point of two frames of same image. Triangulationis a MATLAB library which computes a triangulation of a set of points in 2D, and computes any other operation in the form of sparse matrix on triangulations of order 3.The mesh is the collection of triangles. Each triangle in this mesh is known as elements. This model typically calculates the position of obstacles according to a monocular camera by using range information. If the obstacle is in range then unnamed vehicle or human-being can take decision to turnRange information may be collected from sensors or vision based techniques. We prefer vision based techniques. Vision based has advantages over other technique:

1. Vision based techniques has low cost compare to others.
2. It has low power consumption so that it requires less computational as compare to laser.
3. It has highest point of accuracy.

There is image segmentation, help to segment the image from background. Thresholding is a way in which can convert an image into grey scale image. So this will give background information to detect obstacle.

In this paper, Section 2 describes related work or Literature study. Section 3 describes motivation. Section 4 describes problem statement. Section 5 describes innovative content. Section 6describes assumption of obstacle detection. Section 7 describes methodology.

II. RELATED WORK

This section gives an overview of the related research that has been done in respect of obstacle detection based on color cue till now. Basically the domain of literature survey is the approach used for obstacle detection in computer vision. Following is the existing work done by the researcher in context of their interest:

[1] Tells about the fast color image segmentation for robots. It describes vision systems employing region segmentation by color are crucial in real-time mobile robot applications. Generally systems involving priority wise color-based segmentation are either executed in hardware, or extremely important software systems that retrieve the gain of domain information to achieve the betterefficiency. However; we have found that with careful achieve to algorithm efficiency, obstacle

detection can be done using image capture and CPU hardware [1].

The important step in [1] used approach is to classify each pixel in an image into one of an individual number of color classes. This approach to complete the obstacle detection includes four tasks. These tasks are linear color thresholding, nearest neighbor classification, color space thresholding and probabilistic method [1].

The technology in this system is as following:

1. An implementation of a threshold identifier.
2. Grouping system to form regions through connected components.
3. Segregation and sorting system that collects many region features, and a top down merging heuristic to approximate perceptual grouping.

[1] Showed results about image segmentation that first execution was a rules which are set of autonomous robots on the behalf of ProboticsCyeplatform. And it depends on Uclass [11], Vclass [11] and Yclass[1].In its present model the system can process 320x240 images at 30 Hz with 25% utilization of the 375 MHz CPU.

[1] Approach includes the use of thresholds in a three dimensional color space. Various color spaces are in mostly use, including Hue Saturation Intensity (HSI), YUV and Red Green Blue (RGB).

[1] Purposed figure 2.1 **a 3**-D region of the color space for classification is represented as a grouping of three binary functions. These three functions are

Pixel-in-class = YClass[Y]

AND UClass [U]

AND VClass [V];

[2] Proposed a technique for appearance based obstacle detection. Wan has developed a new *appearance-based* obstacle detection system that is based on passive monocular color vision. The main point of this technique is to segregate from the ground on the basis of appearance and then denoting them as obstacles. Range sensors are also unable to differentiate between various forms of ground surfaces. This is a problem with sensors so [2] gave solution hence obstacle detection system is purely based on the appearance of individual pixels.

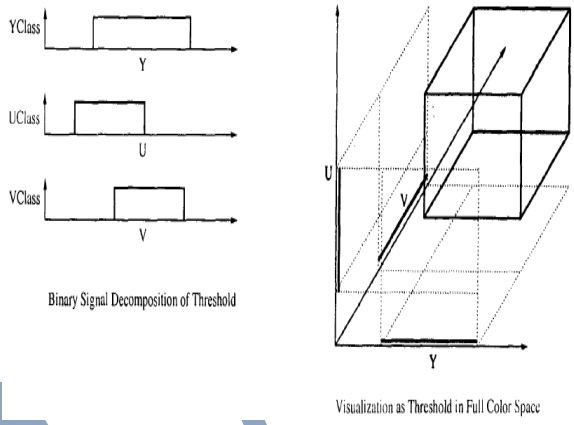

Figure 2.1

The approach used in [2] has number of assumption so that it can handle the problem with indoor and outdoor environments as well.

1. Obstacles differ in appearance from the ground.
2. There should not be any over-hanging obstacle.
3. The ground must be flat.

The simplified technology of appearance-based obstacle detection method [2]consists of the following four steps:

1. Filter the given input binary image.
2. Transform the color input image into HIS color space.
3. Histogram the reference area.
4. Compare this histogram with other reference histogram.

Iwan gave experimental result in which give Input color image with trapezoidal reference area and give output as Binary obstacle image in fig 2.2.

Figure 2.2: 1. Input color image with reference trapezoidal area 2. Binary obstacle output image

Parag H. Batavia and Sanjiv Singh [3] purposed Obstacle Detection Using Adaptive Color Segmentation and Color Stereo homography. The view of author behind color segmentation for obstacle detection is that pixels in an image are notified as obstacle or free space on the basis of color.

The idea of homography is that general stereo cameras are used to find range to images and It requires high

computationally cost. So there is another way to find obstacle i.e. homography. It is linear in the number of pixel because it does not require any computationally cost.

[3] Discussed an approach for obstacle detection using color segmentation. Each pixel in image is denoted by 3-tuples i.e. Red, Green, Blue. In this model, several protocols would be used to classify pixels, for instance "If blue is between 125 and 170 and red is less than 20 and blue is more than 75, then termed as ground i.e. it is not obstacle

Parag has discussed training set which is represented by 2-D histogram. The bins in histogram are located on the basis of H and S values in the pixels of image. The values of the bin show the number of occurrences of that specific H and S pair in the training set. For each pixel in the training image, the value of that histogram bin is increased. After training, the system is ready to recognize pixels as obstacle or free space. For each pixel, p, in a test image.We look up the bin value of the respectively color of p. It gives a probabilistic measure, P, of that image. If P is larger than threshold then it is assumed as free space else it is considered as an obstacle.

Parag [3] purposed a figure in which discuss the result of purposed algorithm.

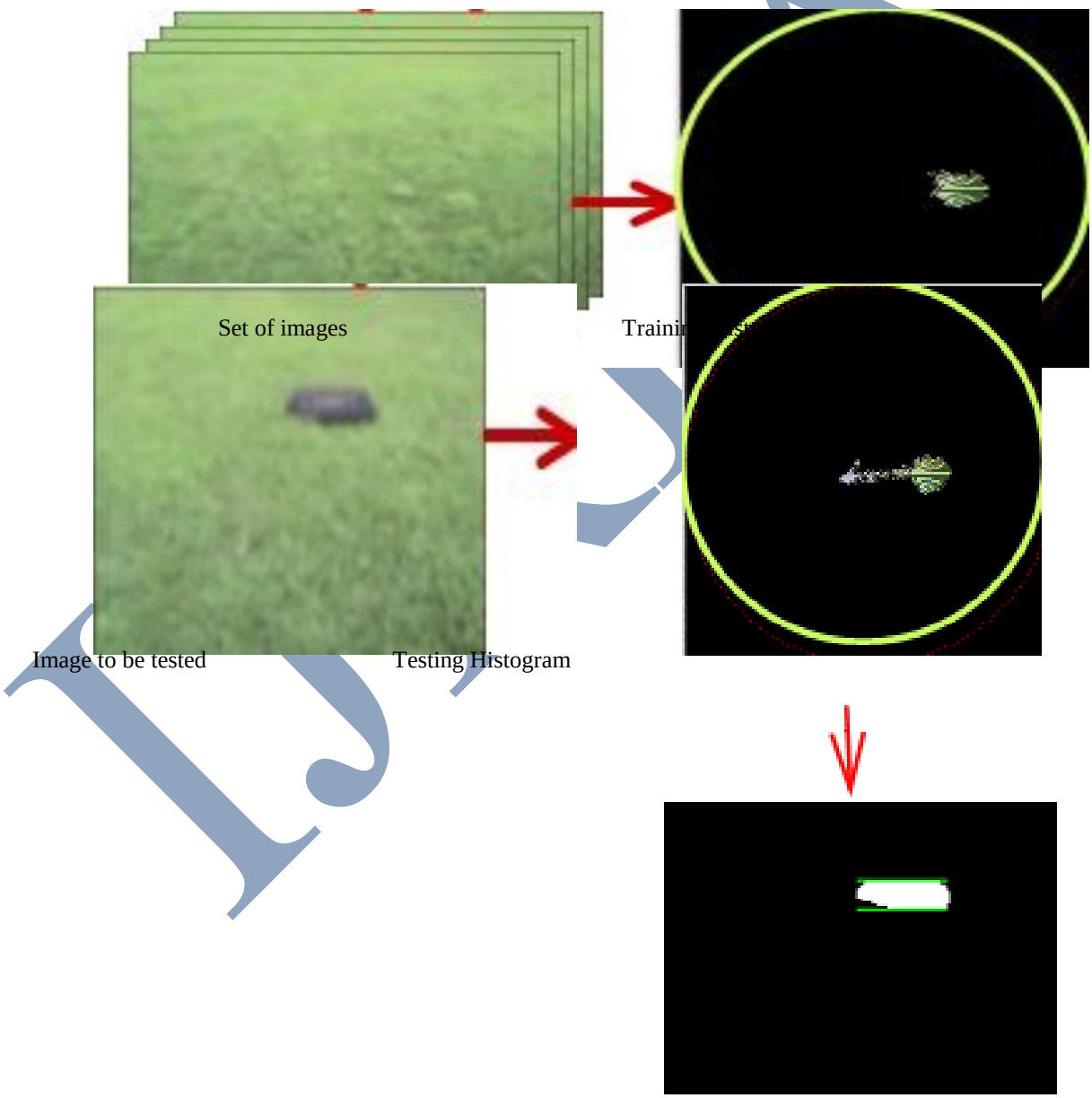

Figure 2.3

Another way is to use nearest neighbor classification. To classify a new pixel, a list of the *K* nearest essence is found, and then the pixel is classified according to the largest ratio of categorizing of the neighbors [4].

- Another approach [5] is to use a set of constant thresholds defining a color class as a rectangular block in the color space. This technique provides well performance, but is not able to retrieve gain of prospects dependencies between the color space dimensions.
- H.R. Everett [6] purposed a technique in which it can be detect the position of autonomous system and sensor. While a huge part of work exists for range-based obstacle detection, little work has been done in appearance based obstacle detection.
- H.D.Cheng [7] purposed color image segmentation algorithm. Basically approaches are based on monochrome segmentation approaches operating in different color space. For example histogram Thresholding, edge detection, feature clustering, fuzzy technique etc.
- Richard I. Hartley [8] developed a technique for obstacle detection based on Triangulation. In this paper they consider the problem of finding the position of a point in space given its position in two images taken with cameras with known calibration and pose. This process requires the intersection of two known rays in space and is commonly known as triangulation.
  [8] Denotes triangulation method in which it defines a point in space which is intersection of two rays from two frames of same obstacle in following fig 2.4.

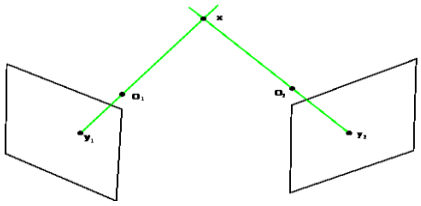

Figure 2.4

Active vision for the visually impaired, financed by the Portuguese Foundation for Science and Technology, combines several technologies, such as GPS, GIS, Wi-Fi and computer vision, to create a system which helps the visually impaired to move in- and outdoor [9].

- Cheng-Lung Lee [10] purposed an evaluation of a simple obstacle detection device for
  Blind people in which questionnaire survey for mobility needs was performed at the start of this study. After the detector was succeed, five blindfolded sighted and 15 blind peoples were invited to organize test under three terms: (1) using a white cane only, (2) using the obstacle detector only and (3) using both devices.
- Long CHEN, Bao-long GUO, Wei SUN [12] discussed obstacle detection system for blind people on the basis of stereo vision method. In this discussed approach, two cameras are installed simultaneously and by making map of those images he applied segmentation for feature extraction. And he detected region of the images so that microphone can detect there is an obstacle.

Long CHEN described a system model for obstacle detection in fig 2.5.

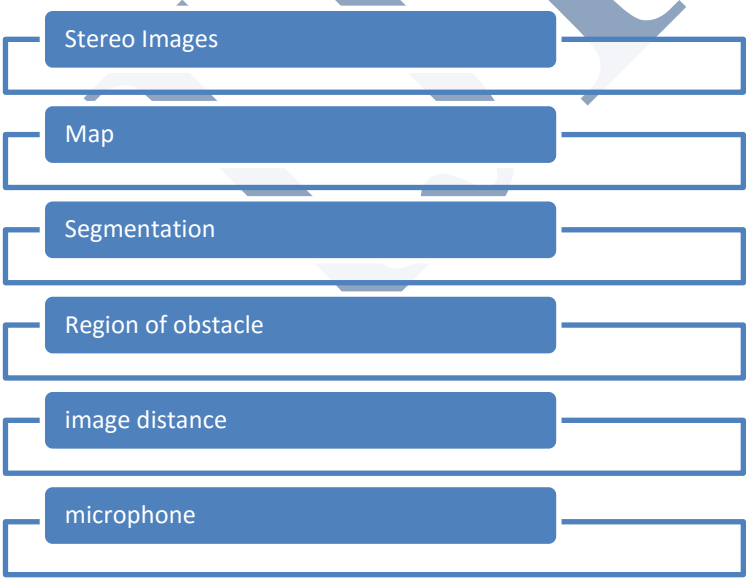

Figure 2.5

Table 1.

No.	Algorithm proposed by	Idea	Limitation
1.	James Bruce ,Tucker Balch and Manuela Veloso [1]	This paper describes a system which is able of following various number of regions of up to 32 color at 32 Hertz on common commodity hardware	This system operates on images only in color space and each pixel has been defined up to only 32 colors.
2.	Iwan Ulrich and IllahNourbakhsh [2]	The idea of this paper is to detect the obstacle based on appearance so that obstacle can be differing from free space.	This paper defines algorithm which is not relay on combination of all color space.
3.	Parag H. Batavia and Sanjiv [3]	The purpose of this paper is obstacle detection using color homography because it requires linear computational cost.	Homography approach is not limited to flat grounds. And it allows navigation system for small area only.

III. PROPOSED MODEL

In our proposed model we have worked with the following security algorithms:-

- RSA algorithm for secured communication [22, 23]
- AES for Secured file encryption [24, 25, 26]
- MD5 hashing for cover the tables from user [27]
- One time password for authentication [28, 29].

At present ensuring security in cloud computing platform has become one of the most significant concerns for the researchers. We have undertaken these problems in our research, to provide some solution correlated with security. We have proposed the following security model for cloud computing data storage shown in Figure 1. In this model, all the users irrespective of new or existing member, needs to pass through a secured channel which is connected to the main system computer. System server computer has relation with other data storage system. The data storage system can be servers or only storage devices. Here, each of the data storage devices can be thought as one or more servers in number. This means, there are no dedicated servers in cloud computing, rather all are independent servers and can be scaled as necessary.

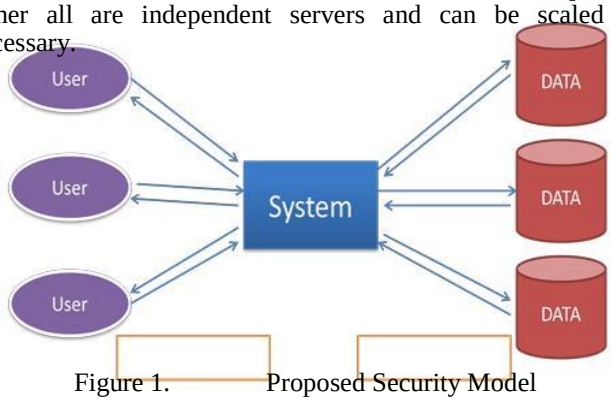

Figure 1. Proposed Security Model

In the proposed model RSA encryption algorithm is used for making the communication safe. Usually the users' requests are encrypted while sending to the cloud service provider system. RSA algorithm using the system's public key is used for the encryption. Whenever the user requests for a file the system sends it by encrypting it via RSA encryption algorithm using the user's public key. Same process is also applied about the user password requests, while logging in the system later. After receiving an encrypted file from the system the user's browser will decrypt it with RSA algorithm using the user's private key. Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result the communication becomes secured between the user and the system.

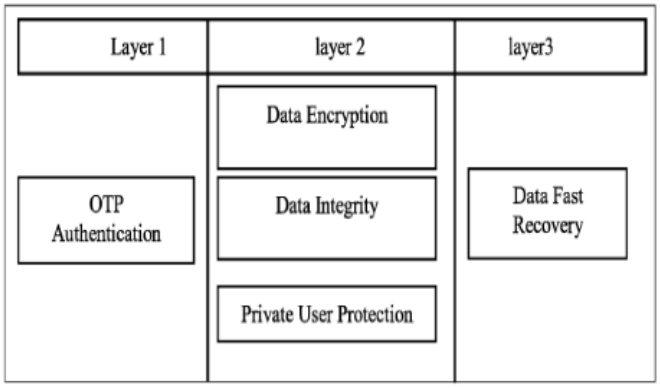

Fig.2 Proposed cloud data security model

In the proposed security model one time password has been used for authenticating the user. The password is used to keep the user account secure and secret from the unauthorized user. But the user defined password can be compromised. To overcome this difficulty one time password is used in the

proposed security model. Thus whenever a user login in the system, he/she will be provided with a new password for using it in the next login. This is usually provided by the system itself. This password will be generated randomly. Each time a new password is created for a user, the previous password for that user will be erased from the system. New password will be updated for that particular user. A single password will be used for login only once. The password will be sent to the users authorized mail account. Therefore at a same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account will be able to connect to the cloud system. By this system, existence of unauthorized user or a user with an invalid mail account will be pointed out. The newly generated password is restored in the system after md5 hashing. The main purpose of MD5 hashing is that this method is a one way system and unbreakable. Therefore it will be difficult for an unauthorized or unknown party for retrieving the password for a selected user even if gained access to the system database. After connecting with the system a user can upload or download the file(s). For the first time when connected with the system the user can only upload file(s). After that users can both upload and download their files. When a file is uploaded by an user the system server encrypts the file using AES encryption algorithm.

In the proposed security model 128 bit key is used for AES encryption. 192 bit or 256 bit can also be used for this purpose. Here the 128 bit key is generated randomly by the system server. A single key is used only once. That particular key is used for encrypting and decrypting a file of a user for that instance. This key is not further used in any instance later. The key is kept in the database table of the system server along with the user account name. Before inserting the user account name it is also hashed using md5 hashing. This insures that unauthorized person cannot retrieve the key to decrypt a particular file for a particular user by simply gaining access and observing the database table of the system server. As a result the key for a particular file becomes hidden and safe. Again when the encrypted file is uploaded for storing to the storage server, the path of the encrypted file along with the user account is kept and maintained in the database table on the storage server. Here user name is used for synchronization between the database tables of main system server and the storage server. The encrypted files on the storage server are inserted not serially. We have developed a hash table for determining where to insert a file into the database table. The algorithm for generating the hash table is described later in this section. Login into the main system is compulsory when a user wants to download a previously stored file. When the user selects a file to download, the system automatically retrieves the key for the requested file from the main system server. The system matches user account name saved in its database table with that saved in the storage server after hashing it using md5 hashing. The path of the encrypted file from the storage server is found by using the user account name and the hash table input for the requested file. In this model, the encryption key for a particular file of a particular user is only known to the main system server.

The path of the encrypted file is only known to the storage server which is only known to the main server. For this, the key as well as the encrypted file is hidden from the unauthorized persons. In this communication system when a file is sent from the main system server to the storage server it is already in its fully encrypted form. That's why there is no need to provide security in this communication channel. At last, we propose hardware encryption for making the databases fully secured from the attackers and other unauthorized persons. Figure 2 is the Pictorial representation of the proposed cloud security architecture. Here, single user and server represent n users and n servers. An algorithm is developed, which is used for inserting the file in the main server (System), and in the database table where the encrypted file is kept. This is saturated from the system server for the cloud computing platform. In the system server, the file is inserted by maintaining the sequence. In file saving server, the file is inserted in a random order which becomes the output of the algorithm. The relations between the system server table and database server tables can be thought as disjoint sets. The pseudo code of the algorithm used is described in table I.

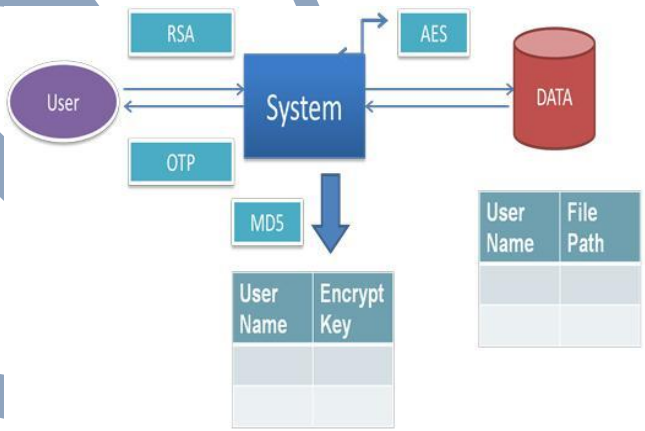

Figure3. Proposed Security Model/ Structure

IV. EXPERIMENTAL RESULTS

In the lab we have worked with about 100 users and also with their files for studying and prove the efficiency of the proposed model. We have tried to find out different execution results which helped us to demonstrate our model with better result. Different conditions and positions were observed during the working and execution time of this proposed model.

A. Lab Setup

- Platform: Visual Studio 2010 (asp.net)
- Processor: Core 2 Duo (2.93 GHz),
- RAM: 2 GB

In this environment, the whole model took average of 5 seconds for executing all the steps. This hardware configuration takes highest 2 seconds to encrypt about a 10 KB file. This model is fast enough and can be applied to current cloud computing environments.

RSA is a public key algorithm invented in 1977 by 3 scientists Ron Rivest, Adi Shamir, Leonard Adleman (RSA). RSA is most widely used public key algorithm over internet RSA is

capable of supporting encryption and digital signatures. RSA gets its security by integer factorization problem. RSA is relatively very easy to understand and implement [10]. Today RSA is used worldwide to encrypt the data which is confidential and RSA gives best security policy that's why all the service providers such as Gmail, hotmail, media fire etc. are using RSA algorithm to ensure their users full of confidentiality. RSA is also used in some security protocols to ensure security and the protocols are [10]:

IPSEC/IKE: IP Data Security
TLS/SSL: Transport Layer Security
PGP: Email Security
SSH: Terminal Connection Security
SILC: Conferencing Service Security

Algorithm Steps of Authentication and Security Implementation

Step 1: Key Generation
Declare e as encryption exponent and d as decryption exponent.
p, q ← Integer numbers.
n←Modulus for keys.
Ø (n) ← Euler's Totient.
e ←Public key exponent.

Step 2: Compute Values
Choose two distinct large prime numbers p &q (Random prime no generation algorithm).
Compute n=p*q
Compute Ø(n)=(p-1)(q-1).
Choose e such that 1<e< Ø(n)
Compute d*e=1
Public key is (n, e), private key is (n, d)

Step 3: Digital Signing
Sender A create message digest of information using hash function (MD5).
Hash Function
Declare character, str' of unsigned long type.
Declare & initialize hash of unsigned integer type.
Unsigned int hash=0 int q. While (q = str + 1) Hash=hash + q.
Represent this digest as integer m& it is having value between 0 to n-1.
Uses private key (n, d) to compute the signature S=mD mod n
Send signature S to the recipients.

Step 4: Encryption
Sender A obtain receiver B's public key (n, e).
Plaintext message as integer m
Compute cipher text c=me mod n
Sends this message (cipher text) to B

Step 5: Decryption
Uses his private key (n, d) to compute m=cd mod n
Extract plain text.

Step 6:
Signature Verification
Receiver uses senders public key (n,e) to compute V=Se mod n
Extract message digest from integer V
Independently computes the message digest of the information that has been signed.
If both are identical the signature is valid

V. OTP (ONE TIME PASSWORD)

A onetime password (OTP) is generated without connecting the client to the server [3]. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client's mobile phone to generate the OTP [3]. In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments [3].

VI. PERFORMANCE EVALUATION

Models for delivering information technology services in which resources are retrieved from the internet through web based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web [18]. In cloud computing technology data and resources are shared; hence there is a threat of accessing of data by invalid users. Initially, the access to the cloud was not secure because credentials such as username and password were required to access. Any invalid user tries to make login to the system using other's account then he is able to access the data [14]. Security policies like 3 dimensional framework enables to categorize data into different security levels. Digital signature is very strong authentication scheme for verifying that only valid user who is liable to access can access the file. RSA is strongest public key encryption algorithm used over the internet now a day. RSA is one of the algorithms having asymmetric key encryption policy. Any invalid user accessing encrypted data then it is hard to interpret [10]. Security of cloud is enhanced by using 3 Dimensional Framework, Digital Signature, RSA Encryption Algorithm and Two Factor Authentication Schemes

VII. CONCLUSION

cloud computing has bright prospects both for business and researchers certain challenging issues including security, performance, reliability, scalability, interoperability, virtualization etc. needs to be addressed carefully. We describe the security issues related to the cloud computing; help to better understand the protocols and the principles behind it thus make better integrity and authentication. So we have to improve security area of cloud to assure user about his privacy

regarding his data on the cloud. To achieve this we implement the technique of 3 dimensional frameworks along with Digital signature and RSA Encryption Algorithm to improve security one step ahead. In this paper we have projected a novel security formation for cloud computing environment which comprises AES, md5, OTP and RSA. The AES is used for file encryption system, RSA system is used for secure communication, Onetime password (OTP) is used to authenticate users in cloud environment and MD5 hashing method is used for hiding information. This model ensures authentication and security for complete cloud computing system.

In our proposed model we have used RSA encryption system which is deterministic. For this reason, it becomes brittle in long run process. But the other algorithms like AES, MD5 and OTP makes the model highly secured. In future we want to work with certifying protected communication system among users and systems and user to user. In future it can also possible that encryption algorithms will get weak, so we want to work with encryption algorithms to find out more secure encryption system for secured file information protected system.

REFERENCES

[1]. Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322

[2]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[3]. Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[4]. Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, "Resource Provisioning for Cloud Computing", IBM Canada Ltd., 2009

[5]. Daniele Catteddu, Giles Hogben, "Cloud Computing:- Benefits, risks and recommendations for information security", November, 2009

[6]. "Cloud Computing: Silver Lining or Storm Ahead?", Volume 13 Number 2, Spring 2010

[7]. NGONGANG GUY MOLLET, "CLOUD COMPUTING SECURITY" , Thesis Paper, April 11, 2011

[8]. Gunasekar Kumar, Anirudh Chelikani, "Analysis of security issues in cloud based e-learning", Master's thesis, 2011

[9]. Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang "Recent Advances in Cloud Security", JOURNAL OF COMPUTERS, VOL. 6, NO. 10, OCTOBER 2011

[10]. Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "Token - Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency", TRUST 2010, LNCS6101, pp . 417–429, 2010.

[11]. Trusted Computing Group, "Solving the Data Security Dilemma with Self-Encrypting Drives", May 2010

[12]. Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", CloudCom 2009, LNCS 5931, pp. 157–166, 2009

[13]. Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency", CASED, Germany, 2011

[14]. Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency"- Extended Abstract, CASED, Germany, 2011

[15]. Luis M. Vaquero, Luis Rodero-Merino, Daniel Morán, "Locking the sky: a survey on IaaS cloud security", Computing (2011) 91:93–118

[16]. Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion", 2010

[17]. Thuy D. Nguyen, Mark A. Gondree, David J. Shifflett, Jean Khosalim, Timothy E. Levin, Cynthia E. Irvine, "A Cloud-Oriented Cross-Domain Security Architecture", The 2010 Military Communications Conference, U.S. Govt.

[18]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", US National Science Foundation under grant CNS-0831963, CNS-0626601, CNS-0716306, and CNS-0831628, 2009

[19]. Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Secure Data Storage and Retrieval in the Cloud", University of Texas, 2011

[20]. John Harauz, Lori M. Kaufman, Bruce Potter, "data Security in the World of Cloud Computing", The IEEE Computer SOCIETIES, August, 2009

[21]. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for cloud computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[22]. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, 1977

[23]. Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories

[24]. Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", 1999

[25]. Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001

[26]. Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January 2010

[27]. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April 1992

[28]. Neil M.Haller, "THE S/KEY ONE-TIME PASSWORD SYSTEM", 1993

[29]. Neil Haller, "A One-Time Password System", October 23, 1995

[30]. "Securing Data at Rest: Developing a Database Encryption Strategy"- A White Paper for Developers, e-Business Managers and IT

[31]. Ulf T. Mattsson, "Database Encryption - How to Balance Security with Performance", 2004

