International Journal on Emerging Technologies **10**(3): 444-453(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

An Authentication Method based on Visual Cryptography using LU Factorization for Cloud Environment

Anupama Jain[1] and R. K. Pateriya[2]
[1]Ph.D. Scholar, CSE Department, MANIT, Bhopal (Madhya Pradesh), India.
[2]Associate Professor, CSE Department, MANIT, Bhopal (Madhya Pradesh), India.

(Corresponding author: Anupama Jain)

(Received 16 June 2019, Revised 29 August 2019 Accepted 03 October 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In today's era, the significance of cloud computing and its advancements towards digitalization is getting close to every people in their day to day life. With its feature enhancement towards digitalization, cloud computing has also concerns about security, privacy, data integrity, authentication. From which, authentication to enable access control to only authorized end user plays a significant role towards service provider reliability, trust over data privacy, information security, etc. In this paper, numbers of existing authentication techniques such as Biometric-based authentication, Token-based authentication, Multi factor authentication and single sign-on authentication have been explored with its limitations. These authentication techniques are susceptible to attacks such as Identity Spoofing, Session Specific Temporary Information Attack, Weak Password attack, Dictionary Attack, Phishing etc. Hence in this paper based on the concise review of existing authentication techniques, a visual cryptography based authentication method is proposed to authenticate users in the cloud environment. It uses LU factorization method to decompose the image into slices. These factorized image slices are used to encrypt the image and as password for authentication. Finally, the result analysis has been carried out on four different standard datasets and performance evaluation matrices like F1-score, PR curve, ROC curve calculates. It shows the average accuracy of the proposed method is 98.24 percentages.

Keywords: Cloud Computing, Cloud Security, Authentication, Authentication Issues, Visual Cryptography.

I. INTRODUCTION

Since the face of the Internet is continually changing, as new services & novel applications appear and become globally noteworthy at an increasing pace. In same direction, execution of client processes is shifting toward the migration of computing resources to execute at remote server. Cloud computing is the solution to warehouse the computing resources, code and information centrally at the server, and retrieved anytime from anywhere through thin clients on the demand basis. It brings many advantages, including data ubiquity, flexibility of access, easy implementation, cost per usage and resilience.

"Cloud computing is defined as a model to provide the computing resources at on-demand basis that are scalable and rapidly provisioned or unbound by negligible configuration." Where, computing resources includes networks, servers, storage, applications, and services

From the point of view of centralized warehousing and accessing at remote side, cloud computing requires identification of thin client and fixing the access role, also may called authentication. Hence, various authentication techniques are useful to fix the access control issue to only authorized user. Authentication mechanism varies from set of credentials (login and password over secure channels) to strong authentication mechanism (based on digital signatures combined with secret password), etc. However, security and privacy issues have become an arising issue for the remote client and the cloud service provider.

In this paper, seven existing cloud authentication techniques has been discussed which are Password based user authentication, Challenge-response authentication protocol, Biometric-based authentication, Token-based authentication, Multi Factor Authentication (MFA), Single sign-on authentication and OAuth 2.0. Next possible attack vectors has been explored to know the process of attacking which helps to make batter solution.

Further, a concise review of existing cloud authentication techniques has been carried out and issues related to particular authentication techniques has been identified. The OAuth 2.0 protocol implementation for web environment is vulnerable to Man-in-Middle attack due to the existence of credentials in plain text format at third-party server. Password based authentication techniques are dependent on third party like CSP and bounded to share credentials with them. One of the main constraints of Visual Cryptography based authentication techniques is limited size of image due to mobile compatible cloud computing. Nevertheless, different authentication techniques are susceptible to different attack vectors such as replay attack, Denial of Service attack, dictionary attack, forgery attack, insider attack, etc.

Finally, to overcome the identified issues, a visual cryptography based authentication techniques has been proposed. The proposed visual cryptography based authentication technique is mobile compatible cloud computing use to its two level factorization.

It also overcome most of the authentication issues and prevents it from the attacks discussing in next sections.

The rest of paper is structured as follows. The existing cloud authentication mechanism has been explained in section II. The possible attacks on authentication techniques are illustrated in section III. The literature survey has been carried out in section IV. The proposed method has been described in section V. Results are analyzed and compared in section VI. The conclusion of this paper is explicated in section VII.

II. EXISTING CLOUD AUTHENTICATION TECHNIQUES

The purpose of authentication is to protect data accessing from unauthorized client. Authentication of end user in cloud computing has been done through different techniques as follows.

A. Password based user authentication

In this type of authentication, user sends their username and password to server to login to system and can access to information from cloud service provider [1].

B. Challenge-response authentication protocols

This protocol contains rules to authenticate the tenant through asking the response of the challenge from the tenant. So for the authentication, an authenticating system generates a challenge to tenant and tenant replies true response [2] as shown in Fig. 1.

For example, in Fig. 1 first client and server sends one-one unique challenge to each other. Further, Server calculates and replies the hash value of the client challenge and its secret key. Similarly, client calculates and replies the hash value of the server challenge and its secret key. Client and server both also predict the values and matched correctly for authentication.

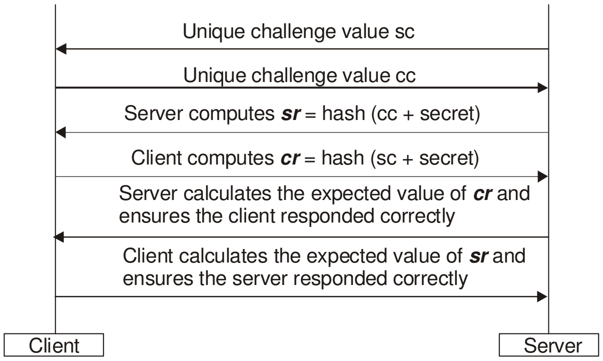
Unique challenge value sc
Unique challenge value cc
Server computes ***sr*** = hash (cc + secret)
Client computes ***cr*** = hash (sc + secret)
Server calculates the expected value of ***cr*** and ensures the client responded correctly
Client calculates the expected value of ***sr*** and ensures the server responded correctly
Client
Server

Fig. 1. Challenge-response authentication protocol.

C. Biometric-based authentication

This method uses a person’s physical characteristics such as fingerprint, voice, face, keyboard timing, etc. to authenticate the end user. It cannot be disclosed, lost, forgotten. Sharma and Balasubramanian [3] brings in focus few limitations of the biometric based authentication technique including expensive, complex installation & maintenance, more false positive and false negatives, privacy leakage etc.

D. Token-based authentication

This method carries conversation with a card reader having inbuilt CPU and memory. It may be in various forms such as PIN protected memory card, Enter PIN to get the password, cryptographic challenge/ response cards, device generates a random challenge, provide an identification number to encrypt or decrypt the challenge with the help of card, etc.

E. Multi Factor Authentication (MFA)

It provides an extra layer of security for sign-in credentials through providing the second-level authentication for the accounts [4]. When a user signs-in with the system working on MFA, the system firstly asked the client to enter their credentials such as user ID and password. Secondly, it requires an authentication code from their MFA enabled device. Two example of MFA device in the form of Smartphone application are Gmail to hardware MFA device and Virtual MFA device.

F. Single sign-on authentication

In Single sign-on method (SSO), a user may access multiple system and application after signing in only once for first time. Firstly, the end user’s identity has verified and there is no need to sign again to access related system and applications [5], e.g., Gmail and its services like Google drive, G+, sites, etc. Another example is to login at slide share from social media accounts such as Facebook or Linked in account.

In such scheme end user may just login through single credential. Yet, decentralized SSO schemes like Open ID, involve third party services to participate in each user authentication session and manage the shared identities. Adopting the traditional SSO schemes for distributed mobile cloud environments are inappropriate [6].

G. OAuth 2.0

OAuth is an open standard, published in RFC 6749 [7]. Commonly, it is employed as an authentication of end users to grant their account access to third party clients. It validates user through releasing the access tokens to third party client using the authorization server. OAuth 2.0 does not provide encryption, signature, channel binding, or client verification [8]. It partially depends on confidentiality mechanism of Transport Layer Security. Hence, OAuth 2.0 protocol is vulnerable to take advantages of small to medium size of web servers [8]. These servers may exploit through flooding the storage spaces of the web server to busy its web applications and unavailable to access.

III. POSSIBLE ATTACKES ON AUTHENTICATION TECHNIQUES

Cloud computing is susceptible for different vulnerabilities such as data privacy, data leakage, network attacks and infrastructure threats, etc [9]. Privacy of information and sharing credentials with third party without client’s agreement is one of the most important concerns of big data and cloud computing environment [10-11]. Common authentication vulnerabilities and attacks in cloud environment are explored as follows.

A. Identity Spoofing

It refers to the action of assuming and setting the identity of other accounts to accomplish their session. Approximate the pattern value of S_{ID} from the historical packet information intercepted from the open channel or form the identity dictionary D_{id}. Compute the new S_{ID} in proportion with captured patterns.

B. Session Specific Temporary Information Attack

It is the concern of reusing the ID based session of the active tenant due to the leakage or stealing of credentials such as session ID S_{ID}. Advisory A_d may establish the same session of authorized tenant through the compromised S_{ID}.

C. Weak Password & Dictionary Attack

It tries to authenticate the victim with the common password strings stored as dictionary. If, advisory A_d guess one of the short-term exponent r_u from the identity dictionary D_{id}. A can calculate long-term key. The complexity of it is [12]

$$O(|D_{id}| * (T_P + T_H))$$

where

T_P = the running time for point multiplication

T_H = the running time for the Hash function.

$|D_{id}|$ = Size of identity dictionary

D. Phishing

It is a fake user interface F_{ui} which is similar in look and feel as genuine interface G_{ui}. Advisory A sends multiple fake packets P_f encompass the fake user interface F_{ui} in order to induce the credentials of tenant T_i. F_{ui} redirects the credentials to the A's database. Repeats the process until the authentic session is found [13].

IV. BACKGROUND AND LITERATURE REVIEW

Researchers have proposed numerous approaches to resolve the authentication issues. Yassin *et al.*, [14] introduced an authentication mechanism to prevent from the replay vulnerability. Nevertheless, it is susceptible to Denial of Service attack.

Darwish and Ouda [8] evaluate the Google's OAuth 2.0 implementation for web applications that indicates it leads to security flaws. Author, introduced the first security flaw that the access data consists of the credentials in plain text form and stored by the third-party client. If the authentication credentials are available in plain text format then any third-party can access available resources, as well.

The second vulnerability introduced is that the web server authentication mechanism uses only password for authenticating the user. The third vulnerability is that the admin has not the control the access threshold and session of the third-party users. Hence, unstable and unsafe execution of the OAuth protocol is risky and increases the possibility of the DoS attack.

Number of authentication techniques in cloud computing are vulnerable to DoS vulnerability due to the complex validation methods and clever attackers' requests from genuine end user [14].

Hence, Darwish *et al.*, [15] introduced a protocol suite for authenticating client in cloud environment to defend from internal in addition with external Denial of Service (DoS) attack. It also has some dependencies, like it simply relies on basic software and hardware constraints of both the cloud systems and cloud users. It requires support of dynamic coding to solve the required difficulty levels of the puzzle.

Babaeizadeh *et al.*, [1] carried out a survey cloud authentication mechanism such as username/password, multifactor, MTM, PKI, biometric authentication, etc. With the intension to verify the identity of the tenant in cloud, authentication becomes more important issue. But, it requires some prevention mechanism to safe critical and sensitive data at the end of Cloud Service Provider (CSP).

Ledesma-Carrillo *et al.*, [16] proposed an online encryption method for images derived from the concept of FPGS and orthogonal functions. The proposed image encryption technique is derived from N-order Hadamard matrices. The Hadamard matrix contains only +1 or -1 values; hence, the calculation may be simplified as simple additions and subtractions of row pixels from the original image.

Yang *et al.*, developed an authentication technique derived from the concept of Visual Cryptography Scheme (VCS) for Smartphone. Author designed different authentication techniques using VCS. Due to the, small size of Smartphone screen, the high quality of Image in VCS is an unavoidable problem. It only prevents from the MITM attack. Authentication of client of different devices with the help of Visual Cryptography Scheme may have a vast impression in future [17].

Tsai and Lo [6] has introduced an authentication mechanism for the services of distributed m-cloud. It is derived from the dynamic nonce generation and bilinear pairing cryptosystem. The scheme trusts on third party SCG to issues the smart card to each registered tenant during the registration phase.

Wang *et al.*, identified that traditional authentication schemes coupled with identity based cryptosystem are suffered from the bottlenecks of public-key infrastructure [13]. Author identified that the existing authentication schemes [18-20] are vulnerable to new attacking scenarios such as known session-specific temporary information attack, key compromise impersonation attack, replay attack and collusion attack.

Tsai [21] identified that certificate-less short signature (CLSS) mechanism derived from the map to point, a probabilistic hash function. It is hard to implement with complex computations rather than bilinear pairings. Hence, author proposed CLSS mechanism derived from the bilinear pairings. Pairing does not require random number hence; it is used to prepare the short signature scheme having the length half of the DSA. A bilinear pairing is map/ function

$$e: G_1 \times G_2 \rightarrow G_T$$

where, G_1, G_2 and G_T are additive and multiplicative groups of the same prime order q. If $G_1 = G_2$, the pairing is called to be symmetric. If $G_1 \neq G_2$ the pairing is called to be asymmetric. A bilinear pairing has the following properties

$$\forall\ a, b \in Z_p^* \text{ and } \forall\ S,R \in G_1,$$

$$e(aP, bP) = e(P, P)^{ab} \text{ and } e(S + R, P) = e(S, P)e(R, P)$$

Where, P is the generator of G_1, a & b are the prime numbers, S & R are the private key and corresponding public key.

Chen *et al.*, (2014) [22] presented a client authentication mechanism base on password. It works on four phases including registration, login, authentication and password change.

Li *et al.*, [23] introduces an enhancement over authentication mechanism with similar four phases. It is based on smart card pre-authentication which affected by attacks such as guessing of the password at off-line mode, dictionary attack, replay attack, insider attack, impersonation attack and duplicity of smart card.

Mishra *et al.,* (2015) [24] presented a remote authentication method which is based on smart card and secure channel. It requires the computation of public key, hash function and XOR computation. It is a light-weighted, user friendly mechanism which may detect incorrect input. The proposed scheme supports smart card revocation, efficient login and password change phases. Authentication schemes based on smart card services requires trust on third party like smart card generators which are also responsible for secure key distribution. Thus, privacy preservation of end user's credentials is a rising issue due to the common attacks such as identity tracing and identity masquerade.

Chaturvedi *et al.*, (2016) [25] proposed a secure biometric-based mutual authentication scheme for multi server environment by means of smart card. Multi-server system felicitates numerous registrations with distinct authorities. The authentication method is derived from the theory of two prime numbers (p, q). Further, to enhance its security proposed authentication method is analyzed by Burrows–Abadi–Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. BAN logic defines the set of rules to determine the flaws of the authentication logic between a legal end user Ui and the server S. Whereas, AVISPA tool substantiates the security against replay and MITM attacks only.

End user U_i enters his/her identity UID'_i and password PW'_i after inserting the Smart Card SC_i in card reader and biometrics B'_i at the sensor. Subsequently, smart card SC_i creates the session as follows:

Step S_1: SC_i validates the injected credentials through the condition

$V = h(UID_i' \oplus PW_i' \oplus H\ (B_i'))$

Where,

$H(\cdot)$ = Secure bio hashing function

$\oplus$ = Bitwise XOR operation

If credentials are wrong, SC_i aborts the session.

Step S_2: SCi computes

$X_{ij} = Y_{ij} \oplus h(UID_i \mid\mid PW'_i \mid\mid H(B'_i))$

Where-

X_{ij} = U_i's secret key

$Y_{ij} = X_{ij} \oplus RPW_i$

RPW_i = masked password

$= h(UID_i \mid\mid PW_i \mid\mid H(B_i))$

$h(\cdot)$ = Collision-resistant one-way cryptographic hash function

$\mid\mid$ = String concatenation operation

Step S_3: Afterward, SC_i produces a random number $\alpha \in Z_q^*$, and D_i, D_i' and R_i as follows-

$D_i' = g^{\alpha}(\text{mod } p) = B_i \oplus h(ID_i \mid\mid A_i)$

$D_i' = D_i \oplus X_{ij}$

$R_i = h(UID_i \mid\mid D_i \mid\mid X_{ij} \mid\mid T_i)$

where, T_i represents the current timestamp.

Finally, SC_i sends the login message $\{UID_i, D'_i, R_i, T_i\}$ to S_j via a public channel. It may be captured in the middle of communication by the attacker to recovers the identity UID_i of the end User U_i and may establish the unauthorized session next time.

The strong authentication in the cloud can be achieved by using Image-based authentication techniques it is based on the order of selected images. There are many authentication methods proposed in which image is used in the authentication process.

Tomar *et al.*, (2014) [26] have proposed image-based secure key exchange mechanism of authentication, in which image-based authentication method has combined together with a secure exchange of key between user and CSP. CSP authorized the cloud user (CU_i) through the sequence of images (S_{img}) selected by the CU_i. Where, S_{img} is a subset of image database, $D_{img} = \sum_{i=0}^{n} Img_i$) stored at CSP. Thus, from n number of images if user is has selected the r number of images then total possible distinct combinations are C(n, r). Hence, the probability to identify the correct combination is P = 1/ C(n, r). This probability is sufficient for today's high speed systems to identify the correct sequence in seconds, because to reduce the complexity and easy authentication process, CSP tries to send not more images to CU_i. It increases the possibility of sequence identification.

Another authentication method based on the encryption of digital images uses the concept of edge detection, which is proposed by Yassin *et al.*, (2015) [27]. Author proposed a cloud authentication technique uses the encryption of digital Image using Canny's edge detection scheme. In this method, cloud user CU_i submits his/her credentials (Username U_{Ni} and Password P_{wi}) to the third party. Then it generates the public key PU = $\{U_{ni}, P_{wi}, Img_i, sh\}$ and private key PK = $\{Img_i, sh, n\}$ for service provider and CU_i respectively. Here, stream cipher is used to encrypt the edge pixels of a digital image (Img_i) as it contains majority of the image's data $D_{Img} = \sum_{i=0}^{n} Img_i$. The proposed method is dependent on third party which point out the privacy issue. End user submits his/her personnel credentials (username, password and digital image) to third parity.

From the literature review author find out that the encryption of data and authentication of client are important for protecting the communication channel in cloud environment. It is equally important to authenticate the end user's identity at remote end of the connection. But, an encrypted channel is worthless if the remote end happens to be an attacker, or an imposter relaying the connection to the intended recipient. We have to fix the user authentication issues by a technology which is secure enough.

A. Literature on Visual Cryptography Mechanisem

Jena and Jena [28] introduces an approach for (2, 2) visual cryptography in 2009. In this approach one pixel may generates either two sub-pixels or four sub-pixels in each shares to decompose the image into 2 layers. Image decomposition has been done through decomposing the each pixel into 2*2 matrixes which contains the 4 values. If the pixel is black then first layer of it contains the $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ matrix value and second layer contains the $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ matrix value or vice versa. If the pixel value is white then both the layers contains the similar value matrix. First layer contains $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ and second layer contains the $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ or vice versa.

Mulliner, [29] proposed a novel idea of the hierarchal visual cryptography scheme. It encrypts the original image in two different levels. The encryption is carried out as it generates the four share in which any three shares are sufficient to superimpose the original image.

Chavan *et al.*, [30] proposed a system to enhance the security of the hidden data through Multi-pixel Visual Cryptography for color images. Author a mathematical proof that proposed system enhanced the security of hidden data successfully which is independent from the robustness, capacity and embedding induced distortion.

Abboud *et al.*, [31] mingles the concept of visual cryptography with Stegenography to communicate the messages in hidden form. It is a novel idea however it increased the computational complexity to decompose and superimposed the shares.

Chen *et al.*, (2012) [32] proposed a novel secret sharing scheme with reduced mathematical computations for authentication. In this scheme pixel expansion ratio is 1:1 hence the original image may be superimposed without distortion. However, the difficulty identified in this scheme is that the author utilizes the Boolean operations for encrypting the image which is impracticable through half shares in signature based authentication.

The existing authentication and key agreement schemes for cloud computing lacking in functionality and features. These have various security weaknesses such as MitM Attack, DoS Attack, etc. These authentication mechanisms suffer from privacy preservation issue due to sharing of original contents. And few of them do not work on all cloud environments (SaaS, PaaS, IaaS, NaaS, CaaS, etc) [33].

Authentication and encryption are important for protecting the communication channel in cloud environment. It is equally important to authenticate the identity of the remote end of the connection. An encrypted channel is worthless if the remote end happens to be an attacker, or an imposter relaying the connection to the intended recipient. We have to fix the user authentication issues by a technology which is secure enough.

V. PROPOSED WORK

Proposed work is based on the visual cryptography scheme used for authentication in cloud environment. It is based on the decomposition of an image. Block diagram of the proposed model to authenticate the end user in cloud environment is shown in Fig. 2.

A. Registration Process

Registration procedure for a new tenant T_i has the following steps:

- T_i sends a registration request to the targeted server.
- On receiving the registration request, server S_t sends a set of images I_n from the existing database of images I_m where, $I_m > I_n$.
- Upon receiving I_n, T_i selects an image I_{t1} and submits $\{I_{t1}\}$ to the S_t via secure channel. Finally, S_t store I_{t1} in relation with T_i.

where

I_m = Set of Images stored at server
= $(I_{t1}, I_{t2}, I_{t3}, \ldots\ldots\, I_{tp}, I_1, I_2, I_3, \ldots\ldots\ldots I_n)$

I_{tp} = Registered Image related with tenant T.

p = represents the number of tenants

I_n = Set of random Images send by server to tenant

I_n must contain Image related with communicating tenant $I_m > I_n$

I_{t1} = Image selected by the tenant and server during registration

Proposed registration process for the server side and client side is shown in Fig. 2.

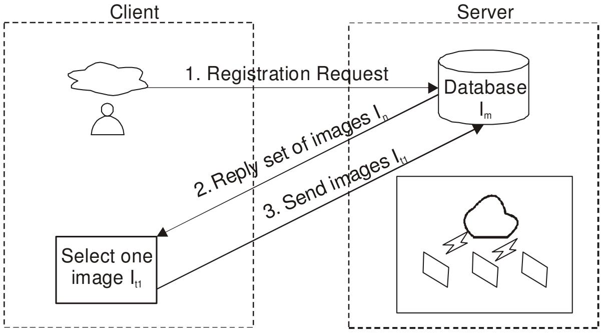

Fig. 2. Proposed Registration Process for Authentication Mechanism.

B. Authentication Mechanism

The registered tenant T_i may set up an authorized connection with the targeted server S_t. Block diagram of proposed authentication scheme in cloud computing environment is shown in Fig. 3. The authentication procedure for the registered tenant T_i has the following steps:

- T_i sends an authentication request to the targeted server S_t.
- On receiving the authentication request, S_t sends a set of images I_n from the existing database of images I_m where, $I_m > I_n$ and I_n must contains registered image I_{t1}.
- T_i selects the I_{t1} and encrypts it using proposed visual cryptography technique for authentication and submits it to the S_t through secure channel.

The detailed visual cryptographic process applied in this work is shown in Fig. 4. On receiving the registered image I_{t1} is decomposed into n parts in context of the size of the key image. And then each part is encrypted through altering the pixel value. If pixel value of K(x, y) in the key image is 0 then the corresponding pixel value of the original image I(x, y) is used as pixel value of E(x, y) in encrypted image.

If pixel value of K(x, y) in the key image is 1 then the corresponding pixel value of I(x, y) in the original image is flipped and used as pixel value of E(x, y) in the encrypted image.

$$V_E(x,y) = \begin{cases} V_I(x,y) & \text{if } V_K(x,y) = 0 \\ V_E(x,y) & \text{if } V_K(x,y) = 1 \end{cases}$$

where

$V_I(x, y)$ = value of pixel I(x, y) of original image

$V_K(x, y)$ = value of pixel K(x, y) of key image

$V_E(x, y)$ = value of pixel E(x, y) of encrypted image

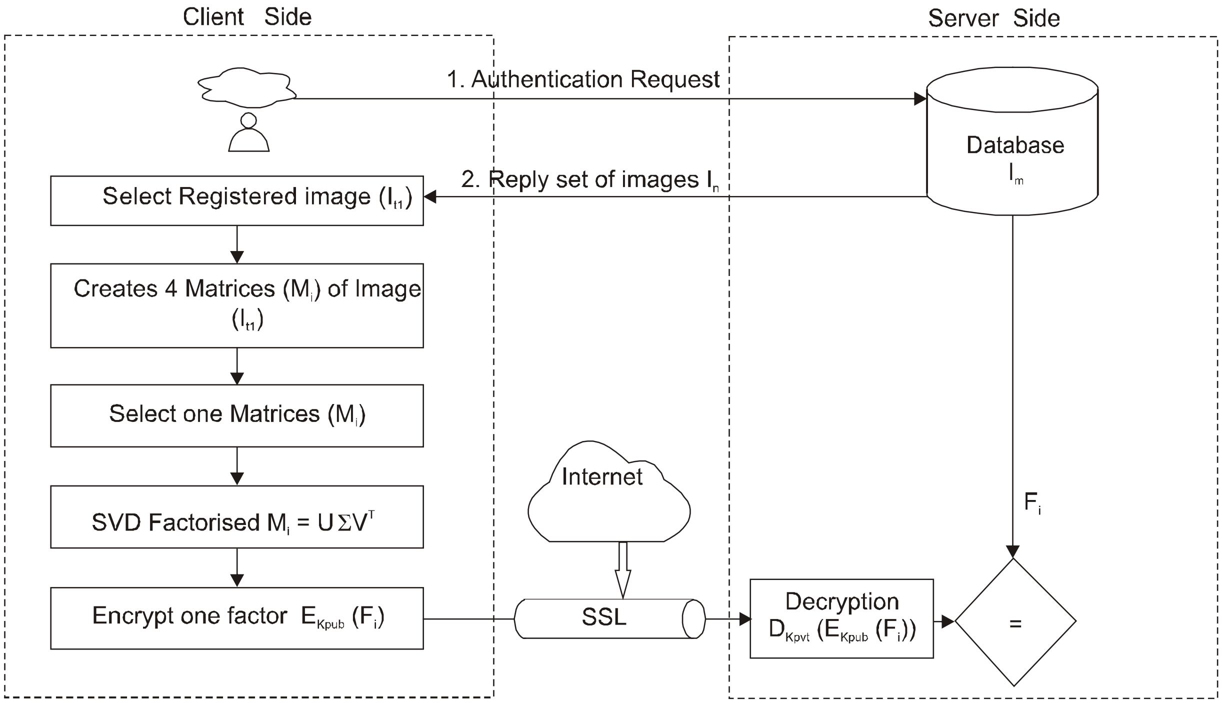
Client Side
Server Side
1. Authentication Request
Database
I_m
2. Reply set of images I_n
Select Registered image (I_{t1})
Creates 4 Matrices (M_i) of Image (I_{t1})
Select one Matrices (M_i)
SVD Factorised $M_i = U\Sigma V^T$
Encrypt one factor E_{Kpub} (F_i)
Internet
SSL
F_i
Decryption D_{Kpvt} (E_{Kpub} (F_i))
=

Fig. 3. Proposed Authentication Mechanism for Registered Tenant.

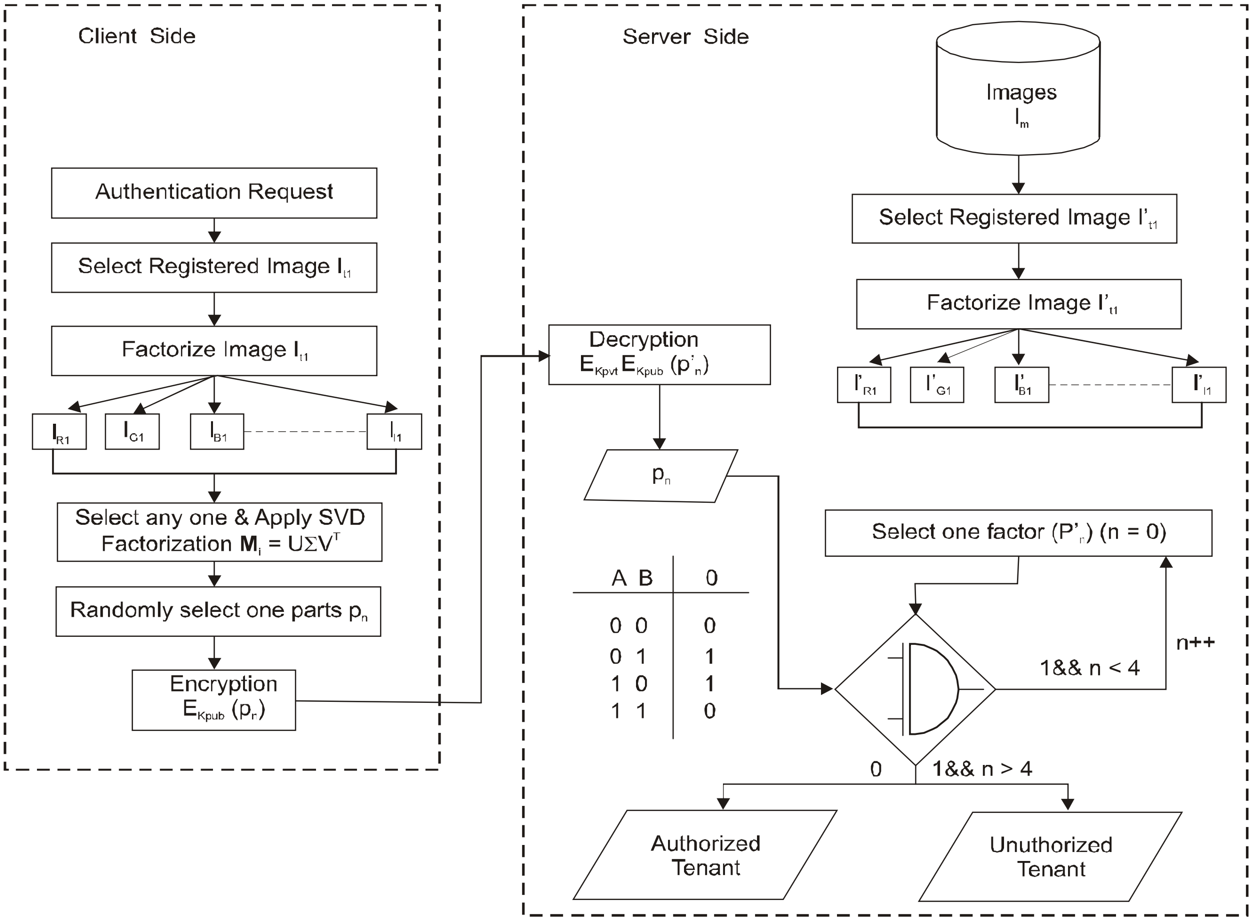
Client Side
Server Side
Images
I_m
Authentication Request
Select Registered Image I_{t1}
Factorize Image I_{t1}
I_{R1}
I_{G1}
I_{B1}
I_{I1}
Select any one & Apply SVD Factorization $M_i = U\Sigma V^T$
Randomly select one parts p_n
Encryption E_{Kpub} (p_r)
Select Registered Image I'_{t1}
Factorize Image I'_{t1}
I'_{R1}
I'_{G1}
I'_{B1}
I'_{I1}
Decryption $E_{Kpvt} E_{Kpub}$ (p'_n)
p_n
Select one factor (P'_r) (n = 0)
A B 0
0 0 0
0 1 1
1 0 1
1 1 0
1&& n < 4
n++
0
1&& n > 4
Authorized Tenant
Unuthorized Tenant

Fig. 4. Detailed Flow Process of Authentication Scheme.

VI. RESULT ANALYSIS

Result analysis of the proposed system has been carried out through implementing the idea in cloudsim using the Java. The implemented system has been

evaluated the performance through combining the four different standard image dataset such as CASIA v1.0, CASIA v2.0, Columbia & IFS-TC. Details of all four data sets are represented in Table 1.

In this paper these datasets has been applied on technique LU factorization used for image decomposition. LU factorization method decomposes the image into matrices according to the matrix values of different image parameters such as RGB, height, width and resolution as shown in Table 2.

Table 1: Dataset used in Analysis of Image Authentication.

S. No	Data Set	Size of Dataset	Image Size	Format
1.	CASIA v1.0	800 authentic images and 925 spliced color images	384x256 pixels	JPEG
2.	CASIA v2.0	7491 authentic images and 5123 tampered color images	Images sizes are different, range from 240 × 160 pixels to 900 × 600 pixels.	JPG, uncompressed image samples and JPEG images with different Q factors
3.	Columbia	933 authentic images and 912 spliced images	128 × 128 pixels	JPEG
4.	IFS-TC	It contains original images clicked from various digital cameras	Varying image size	JPEG and PNG Color Images

In this paper, performance analysis has been carried on four image attributes with varying matrix values represented as P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14} & P_{15}.

First, Precision and Recall of proposed system at all the fifteen parameters of image has been calculated and compared as shown in Fig. 5.

Further, F1-score has been calculated and compared to analyze the balance between the precession and recall of all considered parameters. F1-score for all considered image parameters has been identified and compared in Fig. 6. Further, the system has been evaluated by the Prevalence and Authentication rate which is compared and shown in Fig. 7.

Prevalence is defined as a fraction or a percentage or as the number of actually genuine user authenticated and malicious user rejected in dataset.

The authentication rate is defined as the number of times the system successfully authenticated the client (True Positive) divided by the total times it can be authenticated in the dataset.

Next, Sensitivity and Specificity has been identified which is shown in Fig. 8.

Table 2: Image Parameters used for generating the image factors and its Notations.

S. No	Notation	Image Attributes	Value	Matrix Value of Image
1.	P_1	RGB	Red color	Upper Triangular Matrix
2.	P_2	RGB	Red color	Lower Triangular Matrix
3.	P_3	RGB	Green Color	Upper Triangular Matrix
4.	P_4	RGB	Green Color	Lower Triangular Matrix
5.	P_5	RGB	Blue Color	Upper Triangular Matrix
6.	P_6	RGB	Blue Color	Lower Triangular Matrix
7.	P_7	RGB	Red & Green Color	Upper Triangular Matrix
8.	P_8	RGB	Red & Green Color	Lower Triangular Matrix
9.	P_9	RGB	Red & Blue Color	Upper Triangular Matrix
10.	P_{10}	RGB	Red & Blue Color	Lower Triangular Matrix
11.	P_{11}	RGB	Green & Blue Color	Upper Triangular Matrix
12.	P_{12}	RGB	Green & Blue Color	Lower Triangular Matrix
13	P_{13}	Height	Height	Full Matrix
14.	P_{14}	Width	Width	Full Matrix
15.	P_{15}	Resolution	Resolution	Full Matrix

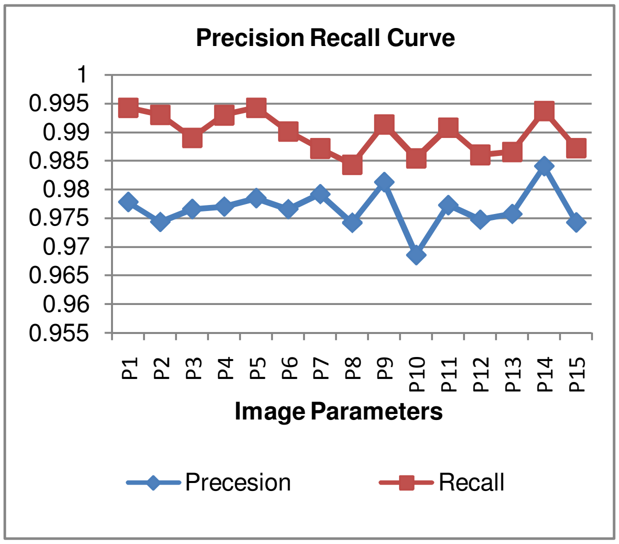

Fig. 5. Precision Recall Curve.

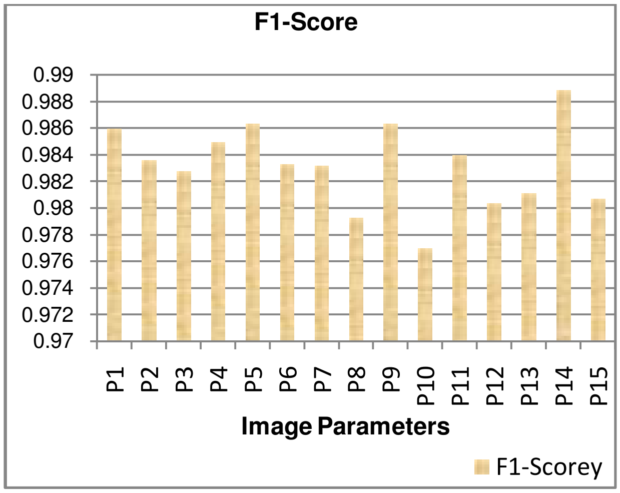

Fig. 6. F1-Score of proposed method at 15 parameters of image.

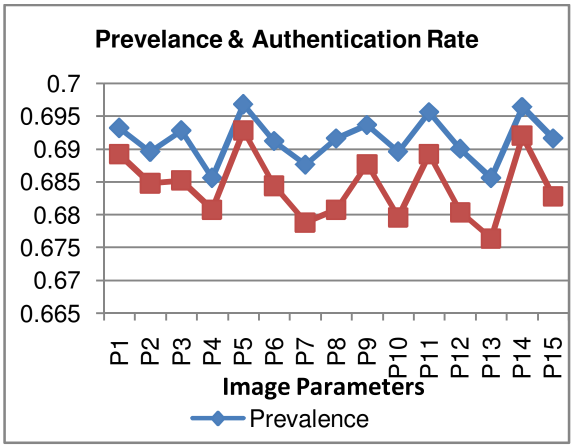

Fig. 7. Prevalence and authentication rate curve.

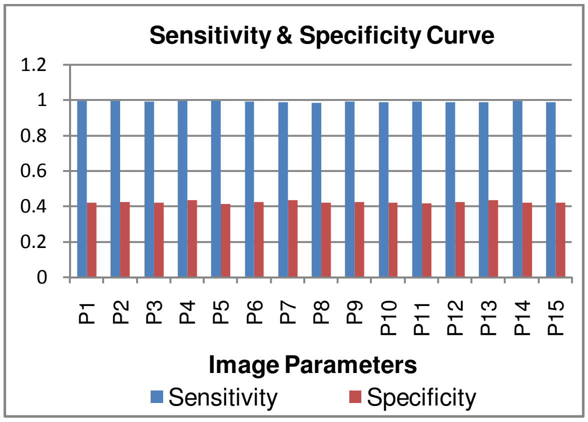

Fig. 8. Sensitivity and Specificity Curve.

Sensitivity is the measure for the true positive rate. It is also known as recall in some cases. The specificity is the measure for proportion of malicious users that are correctly authenticated. It is also known as True Negative Rate.

Finally, Accuracy of proposed system has been identified at 15 considered parameters which is compared and shown in Fig. 9.

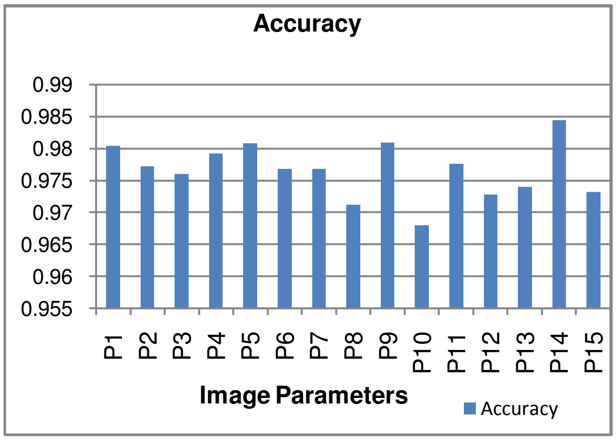

Fig. 9. Accuracy Curve of Proposed System at 15 parameters.

Accuracy is defined as the percentage of correctly classified results. In this work accuracy is defined by the correctly authentication of the user in their respective class i.e. authenticated and rejected. Finally, identified that the obtained results are providing the approx same for all parameters hence authentication through image in cloud environment can be carried out successfully.

VII. CONCLUSION AND FUTURE WORK

The survey carried out in this paper inspected different authentication technologies and methodologies of cloud environment. Survey section mainly described both strong and weak points of the discussed authentication techniques. To overcome the identified weaknesses, further a strong authentication technique for access control has been proposed.

In proposed work, an approach for achieving secure authentication based on image encryption has been presented. In which, there is no need to send original credentials to the cloud server during the authentication phase for authorizing the tenant. It prevents the tenant form the Information leakage, Man-in-Middle, type of attacks. Further, the image is factorized at two levels. At first level, image is factorized in four category according to respective color values such as Red, Green, Blue and Intensity. It may be factorized for any color combination. At second level, selected color has been further factorized through LU Factorization. Use of two level factorization, minimizes the probability to predict the factorized part of image used for authentication as credential. It also minimizes the size of factorized image part by selecting one of the features of image rather all features. Reduced size also makes it compatible with mobile friendly cloud computing.

Since the only encrypted part of image is sending to the server which increases the strength of security of authentication. Proposed method provides prevention from attacks such as dictionary attack, forgery attack, replay attack, insider attack, etc. The utility of this proposed system is its security mechanism that makes full secure authentication.

Result analysis shows that the proposed work providing the accurate results at all fifteen parameters of image considered in this work. Also, it provides prevention from attacks such as dictionary attack, forgery attack, replay attack, insider attack, etc. The utility of this proposed system is its security mechanism that makes full secure authentication. In future, planning to elaborate the same method more as next version and discussed on different parameters.

REFERENCES

[1]. Babaeizadeh, M., Bakhtiari, M. & Mohammed, A. M. (2015). Authentication Methods in Cloud Computing: A Survey. *Research Journal of Applied Sciences, Engineering and Technology, 9*(8): 655-664.

[2]. Zhao, G., Li, Y., Du, L., & Zhao, X. (2015, April). Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment. In *2015 2nd International Conference on Information Science and Control Engineering,* (pp. 156-159). IEEE.

[3]. Sharma, S. & Balasubramanian, V. (2014). A biometric based authentication and encryption framework for sensor health data in cloud. *IEEE, International Conference on Information Technology and Multimedia (ICIMU), Putrajaya, Malaysia, 2014*, pp. 49-54.

[4]. Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011). A strong user authentication framework for cloud computing. *IEEE Computer Society, Int. conf. on Asia- Pacific Services Computing*, 2011, pp. 110-115.

[5]. Odyurt, U. (2014). Evaluation of Single Sign-On Frameworks, as a Flexible Authorization Solution: OAuth 2.0 Authorization Framework.

[6]. Tsai, J. L., & Lo, N. W. (2015). A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE systems journal*, *9*(3), 805-815.

[7]. Hardt D., (2012). Ed. "RFC:6749- The OAuth 2.0 Authorization Framework", 2012, [Online]. Available: https://tools.ietf.org/html/rfc6749

[8]. Darwish, M. & Ouda, A. (2015). Evaluation of an OAuth 2.0 protocol implementation for web server applications. in: IEEE, *International Conference and Workshop on Computing and Communication* (IEMCON).

[9]. Jabir, R. M., Khanji, S. I. R., Ahmad, L. A., Alfandi, O., & Said, H. (2016). Analysis of cloud computing attacks and countermeasures. In *2016 18th International Conference on Advanced Communication Technology (ICACT)* (pp. 117-123). IEEE.

[10]. Chahal D., Kharb L., Bhardwaj A., Singla D. (2018). A Comprehensive Study of Security in Cloud Computing. *International Journal of Engineering & Technology (IJET),* Vol. *7*, No. 4, pp. 3897-3901.

[11]. Aljunaedi, B., Z., & Younes, M. B. (2018). Big data in cloud computing and the related security issues. *International Journal of Engineering & Technology* (*IJET*), Vol. *7,* No. 4, pp. 4534-4538.

[12]. Sahu, D. R., & Tomar, D. (2017). Analysis of Web Application Code Vulnerabilities using Secure Coding Standards. Springer, *Arabian Journal for Science and Engineering*, Vol. *42*(2), pp. 885-895.

[13]. Wang, D., Cheng, H., He, D., & Wang, P. (2016). On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. *IEEE Systems Journal*, *12*(1), 916-925.

[14]. Yassin, A. A., Jin, H., Ibrahim, A., Qiang, W., & Zou, D. (2013). Cloud authentication based on anonymous one-time password. In *Ubiquitous Information Technologies and Applications* (pp. 423-431). Springer, Dordrecht.

[15]. Darwish M., Ouda A., & Fernando, L. C. (2015). A cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DoS) attacks. *Journal of Information Security and Applications*.

[16]. Babaeizadeh, M., Bakhtiari, M. & Muteb, A. Md. (2015). Authentication Methods in Cloud Computing: A Survey. *Research Journal of Applied Sciences, Engineering and Technology*, Vol. *9*(8), pp. 655-664.

[16]. Ledesma-Carrillo, L. M., Lopez-Ramirez, M., Cabal-Yepez, E., Ojeda-Castaneda, J., Rodriguez-Donate, C., & Lizarraga-Morales, R. A. (2016). FPGA-based reconfigurable unit for image encryption using orthogonal functions. In *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)* (pp. 168-173). IEEE.

[17]. Yang, C. N., Liao, J. K., Wu, F. H., & Yamaguchi, Y. (2016). Developing visual cryptography for authentication on smartphones. In *International Conference on Industrial IoT Technologies and Applications* (pp. 189-200). Springer, Cham.

[18]. Truong, T. T., Tran, M. T., & Duong, A. D. (2012). Improvement of the more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on ECC. *Proc. IEEE 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2012, pp. 698–703.

[19]. Li, X., Zhang, Y., Liu, X., Cao, J., & Zhao, Q. (2012). A lightweight roaming authentication protocol for anonymous wireless communication. In *2012 IEEE Global Communications Conference (GLOBECOM)* (pp. 1029-1034). IEEE.

[20]. Zhang, G., Fan, D., Zhang, Y., Li, X., & Liu, X. (2015). A privacy preserving authentication scheme for roaming services in global mobility networks. *Security and Communication Networks*, *8*(16), 2850-2859.

[21]. Tsai, J. L. (2015). A new efficient certificateless short signature scheme using bilinear pairings. *IEEE Systems Journal*, *11*(4), 2395-2402.

[22]. Chen, B. L., Kuo, W. C., & Wuu, L. C. (2014). Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems*, *27*(2), 377-389.

[23]. Li, X., Niu, J., Khan, M. K., & Liao, J. (2013). An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, *36*(5), 1365-1371.

[24]. Mishra, D., Chaturvedi, A., & Mukhopadhyay, S. (2015). Design of a lightweight two-factor authentication scheme with smart card revocation. *Journal of Information Security and Applications*, *23*, 44-53.

[25]. Chaturvedi, A., Das, A. K., Mishra, D., & Mukhopadhyay, S. (2016). Design of a secure smart card-based multi-server authentication scheme. *Journal of Information Security and Applications*, *30*, 64-80.

[26]. Tomar, A. S., Tak, G. K., & Chaudhary, R. (2014). Image based authentication with secure key exchange mechanism in cloud. In *2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom)* (pp. 428-431). IEEE.

[27]. Yassin, A. A., Hussain, A. A., & Mutlaq, K. A. A. (2015). Cloud authentication based on encryption of digital image using edge detection. In *2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP)* (pp. 1-6). IEEE.

[28]. Jena, D., & Jena, S. K. (2009). A novel visual cryptography scheme. In *2009 International Conference on Advanced Computer Control* (pp. 207-211). IEEE.

[29]. Mulliner, C. (2010). Privacy leaks in mobile phone internet access. In *2010 14th International Conference on Intelligence in Next Generation Networks* (pp. 1-6). IEEE.

[30]. Chavan, P. V., Atique, D., & Malik, D. (2014). Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares. *International Journal of Network Security & Its Applications (IJNSA),* Issue 1, Vol. *6*, pp. 91-102.

[31]. Abboud, G., Marean, J., & Yampolskiy, R. V. (2010). Steganography and visual cryptography in computer forensics. In *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 25-32). IEEE.

[32]. Chen, Y. H., & Lin, P. Y. (2012). Authentication mechanism for secret sharing using boolean operation. *Journal of Electronic Science and Technology*, *10*(3), 195-198.

[33]. Chaimaa, B., Najib, E., & Hilal, R. (2017). Authentication mechanisms in Cloud Computing environments. *International Journal on Information Technologies and Security*, *9*(3), 63-84.

How to cite this article: Jain A. and Pateriya R. K. (2019). An Authentication Method based on Visual Cryptography using LU Factorization for Cloud Environment. *International Journal on Emerging Technologies*, **10**(3): 444–453.