IMAGE ENCRYPTION USING PERSUASIVE CUED CLICK POINTS WITH MODIFIED EAES IN CLOUD STORAGE

¹G. PREETHI, ²N.P. GOPALAN

¹Research Scholar, Research and Development Centre, Bharathiar University, Coimbatore
²National Institute of Technology, Department of Computer Applications, Trichy
E-mail: ¹mgpreethi@gmail.com, ²npgopalan@nitt.edu

Abstract- The rapid growths of the technology, the user and organizations have stored their confidential data and private images in the cloud storage. This can be a new trend of outsourcing a database to authorized users. The authorized user is called a cloud service provider. Lots of service providers are available in now-a-days. The confidential data and private images need a security in the cloud storage. The double way of authentication scheme to protect the information such as data is embedding into the images these images are retrieved as original using Reversible Data Hiding techniques (RDH). The hidden data to be protected by using the persuasive cued click - points (CCPs) with Modified Efficient AES for providing a better security in the cloud database. The proposed method generates a random key is called SALT key for an image encryption. The SALT key increases the security of confidential data by the combination of data and images. The whole or partial confidential document hidden into the image, the cover image is split into a number of blocks. The user clicks an image randomly each clicks ahead of the next click until the third click to expand the image. Therefore, unauthorized user or untrusted service providers couldn’t gain the attempt of tracking the actual content which was stored by the data owner whether it may be an individual user or an organization. The proposed system is used to reduce the complexity of an algorithm and has civilized the performance result of an image encryption.

Keywords- Image Encryption, Persuasive Cued Click-Points, AES, Data Security, RDH.

I. INTRODUCTION

The emerging field of cloud computing is a significant process of storing information instead of traditional storing systems. The database outsourcing is a measurable environment of large-scale data and progression that work on various applications and services mean by on-demand self-services. The new aspects of storing and distributing files in-and-around of an organization are utilizing the outsourcing services. The healthcare, IT organization, school and universities are broadly utilizing this facility to comparably low-cost, less processing time and platform independent on the client side. In recently, many organizations are relieved from the burden of storage management; maintain a huge database and distribution of database to the clients. The vast and tedious processes have been increased the processing timing of an organization.

The stored information and a large database handling are not suitable for the traditional method. There are many cyber security problems arises in various ways. The cloud infrastructure as a service (IaaS) has more potential energy and reliable than their own laptop or personal computers of user. The data must have a protection in many ways such as data encryption, image encryption and data hiding into the image. The most powerful protection scheme is data embedding into an image; these images are encrypting by split into a number of matrix forms. Each block has confidential information in the form of encrypted images. These blocks are differentiated by compressing and uncompressing of images used by revisable data hiding techniques. The encrypted key is randomly generated by the SALT key with Efficient advanced encryption standard. These images lead three clicks on login phase; each clicks ahead a next click of the image until to getting a decrypted data. The summarization of our contributions is described as follows:

1. The best of our work to concentrate and show the results of adding SALT Key of 16 bits for data hiding into the image, to protect the large-scale database in a cloud storage.
2. In this paper presents the security of framework in the images are split into a number of blocks and each block may contain a confidential data, the authenticated user can extract the data from an image otherwise that has shown the cover image.
3. We systematically analyzed the security system and make experimental through the outsourced database in cloud service provider. We examine the cloud service provider is also a trusted or untrusted of data owners.

In this paper organized as follow. Section 2 the existing works which is associated to PCCP authentication system, Section 3 methodologies of click based authentication CCP and PCCP’s overview of secure authentication discussed in detailed. Section 4 presents the Persuasive Cued Click with Modified Efficient AES formulates the problem and gave solution to improved efficiency. Section 5 analyzes the performance of security system in the cloud database. Section 6 concludes this paper work and exposes the future direction of this research area.
II. RELATED WORK

The CCP techniques used to protecting a data in the cloud storage with help of phases of GPA is suggested [1]. The encryption and decryption may not support a full control over the stored data; they give better idea of integrity management and access control mechanism. This has security in login phase but not over all stored data in the cloud. In the author Ashok use another method called password cued click points recognition for password verification. This consists ten sets of key offering from 0 to 9 [2], the key set assign twelve digit alpha numeric characters to user for remembrance. This key process makes more complexity for hackers to access the content. The one-time data division uses a concept of Divide and Nest to gets a password encryption. The limitation of this system was having combination of 4 passwords and three keys to make a length and tedious process on the emergency period [3]. The authenticate system has a strong security code for user memorable [11] [8]. The paper concentrates only alphanumeric security system not a combination of alphanumeric and special cases. This was the limitation on this paper. The author suggest graphical password [13] [22] and recall based techniques. In paper [5] used the method circular tolerance by avoiding a drawbacks of cued click point, which is based on the knowledge based alpha numeric password and graphical password. The recall based security system and recognition based techniques with DAS are used widely [12]. The suggested methods proved theoretical space comparison not for the storage capability. The main consideration of memory capability is not discussed on the paper. They were lots of people have a same guessing points on the images for visual attention research [18]. This is easy to predict the security code by click-based images. The authors Davis et al [20] recommend the user choice of 1D graphical password code but it was not acceptable for all kind of users because it’s predictable. The systems were generating a password in random wise based on their user preference. The preference may be a safe path from the least node (or split block) of an image. The knowledge based security system having many different types of recall based techniques. The author suggests pure recall based method behind of Draw-A-Secret technique [21]. This technique is used to draw a password in the two-dimensional grid with the help of stylus or mouse. The user draw a diagram on the grid which consist one continuous fondle or use too many fondles on the security system to make a new password. The same strokes are matched on the grid then user is allowed to access the content. The limitation of this method is frequently not possible to draw a diagram with the same stroke on login phase. The suggested method is having examples of Passdoodle [20], Grid Selection [16]. Similarly the author J. Thorpe et al [17] discuss the method of hotspots with predefined pattern based attacks. This attacks is cued recall based techniques which identify the authorized user or not in the entry level. These all drawbacks are overcome by the method of PCCP [4], the PCCP method is used to avoid the pattern effect and hotspots clicking by the more familiar areas of an images. The results of PCCP is comparably good and having advantages of users in the point of security system. The performance of PCCP is good but the result of image quality is not acceptable in the modern world. The above mentioned authors are concentrating only on entry level of security system. The implementation of PCCP with SHA algorithm [9][21] for securing a folder because the user stored their confidential documents are keep it their own folder on the local disk is prescribed by authors Shilpa and Dhapade [10]. The combination of PCCP and AES [7] has been proved in the graphical authentication system but the limitation of this method is using only one image for all the click points. The graphical notations or symbols are not includes on the extraction. Although, upgrading a new image is not possible on the hotspots region. The attackers have an easy guess of click point’s area on the images and proved theoretically. Suggestion given by smita et al [6] increases more security in the ways of text and image password using persuasive CCP with IAES. They add Salt key of 8 bits for expanding of next click images. The advantage of this method is dictionary attack take away from the database. The proposed method is slightly having a difference of the above mention technology. The Salt key size is increased as well as iterations improved highly. The memory capacity is decreased by using a same image to be extracted for next click points. The performance of this method is increased rather than the existing methods. The author plan to extend the security system has highly sensitive using the homomorphic encryption [14] on the untrusted service provider.

III. CLICK BASED GRAPHICAL AUTHENTICATION

This is a knowledge-based authentications provides the control of human memory in the form of visualization of a graphical security system. In the visualization of images to give user able to identify the goal of previously point-out the locations surrounded by one or more images. The image split into the number of cubes with includes a PassPoints of an image. The authenticated user has been remembering the locations in-order of the click points on the images. The user tries to attempt the click points on the images which the pattern is stored, the user allows to access the database otherwise the user may be treat as unauthenticated. The PassPoints are comparatively utilizable thus security weakness makes password very easy to guess everyone. The PassPoints are required large number of memory
capacity to store their images because the user may have a guess at anywhere in the image.

3.1 CUED CLICK-POINTS
The Cued Click - Points (CCP) of encryption design is reducing the predefined patterns and also reduces the hotspots in support of assailant. The CCP has single click point rather than the five clicks on the images. This is used a single click on the five different images which is shown as consequently. The next images are exposed which is based on the previously determined the clicks of an image. This is generates a path on the stored images, shown in Figure 1. The new password is generated by a new click point of an image with the sequence of click. The advantage of CCP method is to know the user whether authenticate or not at the end of final click point, this is one of the protection against by the attackers. Every sequence of a click will create a new password in the CCP. This is the advantage as well as the drawback of the method. The user may not remember the sequence of the click is no longer for their memory. The system was generating the images for giving more security of one image at a time.

3.2 PERSUASIVE CUED – CLICK POINTS
The most popular technology of PCCP was introduced by E. Stobert [15]. This technology is used to create a strong password which is not able to support the password generating by the system. The user must have a strong memory capacity for remembering too many images on the PCCP security system unless the user generated a new password at every time. This will occupy the large memory area for storing a password for the security of hidden data in the cloud database. The PCCP security system reduces the hotspots in all way of attackers. The images are split into the number of blocks and user may select the randomly displayed positions of an image, that the selected blocks of an image are called the window port to viewport images. These images are called the screen coordinates in the displayed images. The coordinates are transformed from window to viewport each selected blocks as follows

$$\begin{align*}
X &= \frac{w_{max} - w_{min}}{w_{max} - w_{min}} x + \frac{w_{max} - w_{max}}{w_{max} - w_{min}} w_{max} + \frac{w_{max} - w_{min}}{w_{max} - w_{min}} w_{min} \\
Y &= \frac{v_{max} - v_{min}}{v_{max} - v_{min}} y + \frac{v_{max} - v_{max}}{v_{max} - v_{min}} v_{max} + \frac{v_{max} - v_{min}}{v_{max} - v_{min}} v_{min} \\
h &= 0.01
\end{align*}$$

The world coordinate points are transformed into the screen coordinate of x and y in XY plane. The authenticated user is allowed to extract the images and able to shuffle the images to create a new password for protecting the hidden data. The system guidance is not acceptable by the unauthorized users which may lead to click many times on the hotspots in the protected images. This may reduces the security system of hidden data. The proposed system of PCCP with Efficient encryption standard gives more security of hidden data on the cover images.

IV. PROPOSED SYSTEM
The outsource database has a security system in many ways. The data owner might choose any one of security system such as knowledge based, Token based and Biometric authentication system. The graphical representation is having more secured than the token based and biometric based system. The token based authentication is not suitable for large scale database. The device is a full responsibility of the authentication of biometric. The data are hiding into an image with the help of knowledge based authentication is provide better performance of cloud storage. There are three clicks of an image with a guess by the user this click has ahead a next move of the picture until the pattern is completed. The closed graph should be stored in the database. The partial portion is a pattern and the other partial portion has already stored a closed graph. If these two are getting similar to finish the end point of an image, the user has retrieved the information from the cloud storage. That the user may be authorized user otherwise access is denied.

4.1 PCCP WITH MODIFIED EFFICIENT ADVANCED ENCRYPTION STANDARD
The proposed encryption involves three stages of phases with an enhanced AES. These phases are namely setting data into an images, user registration, and authentication of CSP. The first phase of setting has the confidential data into the images using parameters of $T_{TP}$, $C_{SP}$, and $U_{R}$ which applying the EAES algorithm with SALT key for encryption. Here, the symmetric keys are used for encryption and decryption and it has the parameters $E_{Ci}$ and $D_{Ci}$. The symmetric keys size is different for all cryptography such as the 128 bits represents the iteration of 10, 192 bits represents the iteration of 12 and 256 represents the 14th iteration. Our proposed systems use the 192 bits instead of added the SALT key of 16 bits in the Enhanced Advanced Encryption Standard (EAES). The Trusted Third Party (TTP) has combinations of $E_{AES} = 2^{192} + 16$ bits are calculated which shows the results of 6.2771017457 and the another random value is generate for comparing the $E_{AES} = 2^{192} + 16$ bits has 9.0 e+40, send to the Cloud $\xi$ (2) Provider ($C_{SP}$), where $p \cdot q$ (SALT key value) is denoted the symmetric key and SALT $k_{i}$ encryption as well as decryption. The user server $E_{AES}$ values to the trusted third party to check the user is authenticate or not. If the user is authenticated allow to access the database from the cloud storage otherwise not. The trusted third party stores data into...
images and keep the public key parameters $P_k = (U_{id}, P_{wd}, C_{image}, S_{eq})$ and secret key $S_k = (C_{image}, S_{cell}, C_i)$ in the cloud service provider. The third party make a image into number of blocks and split blocks are contain partial portion of hidden data in the form of images. These images have a RGB color model into the gray-scale. The image is extracted from the cover image to compute the user id and password to be matched or not. The User has $U_{id}$ to encrypt their secret key as $S'_{K} = E_{ci}(S_k)$ and decrypt the stored hidden data from the image. The hidden data are stored in safe manner within the cover image.

<table>
<thead>
<tr>
<th>SYMBOLS</th>
<th>DEFINITION OF SYMBOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_k$</td>
<td>Public key</td>
</tr>
<tr>
<td>$S_k$</td>
<td>Secret key</td>
</tr>
<tr>
<td>EAES</td>
<td>Efficient Advance Encryption Standard</td>
</tr>
<tr>
<td>$P$</td>
<td>Symmetric key</td>
</tr>
<tr>
<td>$C_{id}$</td>
<td>SALT key in bits</td>
</tr>
<tr>
<td>$U_{id}$</td>
<td>User Id</td>
</tr>
<tr>
<td>$P_{wd}$</td>
<td>Password</td>
</tr>
<tr>
<td>$C_{image}$</td>
<td>Cover image on the hidden data</td>
</tr>
<tr>
<td>$S_{eq}$</td>
<td>Image split into number of cells</td>
</tr>
<tr>
<td>$R_{pi}$</td>
<td>Random pixels are select from the split image</td>
</tr>
<tr>
<td>$T_{TP}$</td>
<td>Trusted Third Party</td>
</tr>
<tr>
<td>$C_{SP}$</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>$E_{eq}$</td>
<td>Encryption and Decryption of Cover Image (ci)</td>
</tr>
<tr>
<td>$E(x)$</td>
<td>Encryption of a variable</td>
</tr>
<tr>
<td>$D(x)$</td>
<td>Decryption of a variable</td>
</tr>
</tbody>
</table>

Table 1: Notations for Proposed Work

V. PROPOSED ALGORITHM

1. $U_{id} \rightarrow$ Submit ($C_{SP}: U'_{id}, P'_{wd}, \alpha, U_{id}$) to perform the generating random value, decryption as following steps:
   - To decrypt the hidden data from cover image using their password $S_i = D_i(S'_{i})$.
   - To generating a random value $r_i \in Z_n$, and compute the user name $U_{id} = h(user id)$, password $P'_{wd} = h(h(sec_id)) \parallel s_n \parallel r_i$, OneTimeCode = $h(\alpha)$. 
   - These parameters $U'_{id}, P'_{wd}, \alpha$ are send to validations

2. $C_{SP} \rightarrow User'_{id}$: $(x_{cor}, y_{cor}), R_{pi}$. The $C_{SP}$ validate the user identifications factors as follows:
   - The new password $P'_{wd} = h(P_{wd} || s_n || r_i)$ to compare the already stored password in the cloud database, $P'_{wd}$, whether both are equal or not. The authentication is matched, user have a permission to access the next level otherwise the Cloud Service Provider ($C_{SP}$) terminate the process.

3. The authenticator of user verify $U_{id} \rightarrow C_{SP} : E'_{ci}$ and $C_{image}$ is extract by $R_{pi}$. The image is split into number of cubes and the $E(E_{ci} \in R_{pi}(n))$ to identify the next cubes in the images until last block on the image.

4. $C_{SP}$ receiving the authentication key and allow to downloading the confidential data for decryption.

5. $D_{ci}$ ($R_{ci} = D_{ci}(E_{ci}(C_{SP})))$ authenticate user can download the image wants to decrypt using SALT key and get the hidden data.

V.1 HOTSPOTS ON PCCP IMAGES

The image has a high possibility of click on the selected portion is called hotspots, which are used for a security system of the login phase on the cloud storage. This may generate patterns using the solid line, dash and dotted line, and straight lines; it can be demoralized by unauthorized users without their knowledge of data owner and cover images. The authorized user must choose the position within the world coordinates to highlight the screen viewport otherwise click may lead shuffle the images again. In the security system, the image is split into a number of blocks which is based on the matrix of $3 \times 3$, $7 \times 7$, $9 \times 9$ [19] and so on. Each block have a click will show the next block of an extracted image until the third click of an original image. This will create a path for next move from the original image to final click on the image.

VI. EXPERIMENTAL RESULTS

In our experiments, we calculate the time taken by the CCP, PCCP, PCCP with AES, PCCP with IAES and PCCP with Modified EAES. The proposed systems have very less run time than the other existing system. The proposed system and existing system has a negligible difference but consider the point of security PCCP with modified EAES prove the good results. The other techniques have concentrated too many images to store in the cloud database for guessing of next click on the images.

Figure. 1 Original navigate image blocks extract using PCCP with modified EAES, first click ahead a next click image

This will occupy memory space on the cloud storage it will take too many processing time. Due to this problem, the system capacity and working interest
will go down. In our proposed method concentrate only three clicks on the image as well as the blocks are extracted with the same image and stored temporarily on the storage media and it will get refresh rate is 60 frames/sec. The refresh rate is equal to the time taken for refresh the raster scan display device. The extracted blocks are shown with enlarged images to identify the quality of our proposed method result.

Figure 2. Navigation of image with confidential data hiding into each block

In the proposed scheme has Navigation of image with confidential data hiding into each block is shown in Figure 2. The experiments made by three client system and one system act as a server to predict the quality of the result. These systems are having different configuration and resolutions. The client 1 has Intel Core i5-6 processor, memory capacity 8 GB RAM, and 1 TB internal HDD and network adaptor is 802.11ac 2.4 /5 GHz wireless adaptor in windows 10 professional x64 SP1. Client 2 has Intel Core i3-3 processor, memory capacity 4 GB RAM and 500 GB processor, memory capacity 2.80 GHz, 1 GB RAM, Windows 7 Operating System internal hard drive, dual-band WIFI-certified 802.11 a/g compliant adapter. Client 3 has Intel® core™ i3 processor 3.00 GB RAM, Windows 7 ultimate operating system x32 bit and Client 4 has Intel P4 x32 bit. Our proposed system having various image sizes for attempting the click based experiments. The results rate shown in table 2 and mention various states of the attempt on images. The small image (1) indicates size is small, 1 click point in the first attempt; small image (4) indicates size is small, 4 click points; the size is large image and 3 click points; finally, the size is large image and have a 2 click points. The sizes of small images were 430 X 233 pixels and large images were 780 X 640 pixels with the resolution of image aspect ratio is 6:2. The state may be very short duration, little mistakes and success rate is high in our proposed system. The efficiency of existing and proposed scheme results has shown in Figure 3. This has a better quality of images and usability is shown in our results.

### 6.1 IMAGE AND HIDDEN DATA SECURITY EXTERNAL SOURCE

The confidential data are hidden into the image that is called cover image. The covering image has a security alert using the proposed method against the speculation attacks, CAPTCHA attacks.

### 6.2 SPECULATION ATTACKS

The speculation attack is mainly against of brute force attack as well as dictionary attack. The brute force attack is tried to get the security code or combination of code until the trial is successes. This is a one of the time taken process attack. However the most familiar hackers are using this attack. The complex combination of security code is possible in this type of attacks to identifying the security code for long process of brute force attack. The most similarity of trials is attempt by the attackers and guess by the nature of interest of data owners in the cloud. The next type of attack is called dictionary attack, attacker use all the dictionary words and common words to retrieving security code. This method is taking too many time for execution, our proposed system is not concentrate on this attack. We get the good quality of image and very high security system by using PCCP with modified efficient AES.

<table>
<thead>
<tr>
<th>Size &amp; Name of Cover Image</th>
<th>RDIF of Image on Security System (dB)</th>
<th>Capacity (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.jpg <em>(430 x 233)</em></td>
<td>43.62</td>
<td>0.7051</td>
</tr>
<tr>
<td>Zebra.jpg <em>(420 x 455)</em></td>
<td>53.20</td>
<td>0.0810</td>
</tr>
<tr>
<td>Baboon.tif <em>(760 x 620)</em></td>
<td>60.23</td>
<td>0.75</td>
</tr>
<tr>
<td>Palm.tif <em>(783 x 903)</em></td>
<td>48.01</td>
<td>0.78125</td>
</tr>
</tbody>
</table>

Table 3. Image Quality of Our Method

Figure 3. Run Time Computation using PCCP with Modified EAES
CONCLUSION AND FUTURE WORK

The most important security system of outsourcing database in the cloud computing has better results in our authentication systems. The technique of Modified Efficient Advanced Encryption Standard is one of the best authentications of graphical view password and confidential data embedded into the images for protecting from unauthorized or untrusted cloud service providers. The authenticated user can store their data hiding into the image in cloud storage. In existing PCCP design was implemented only for verification of entry level (login) not for hiding a data. In this paper proposes the design and implementation of hiding reversible manner of secret data into cover image. The PCCP with modified efficient AES is reduced the complexity by three click of image and increase the security system of cloud storage with SALT key encryption and decryption of confidential data. The experimental results are proved. The future work, will be adding a symmetric key within a 3D view of image encryption to give more secure cloud storage. Instead of retrieving images from a database the user capture a photo of their own face or natural scenes at the time of login in real time. This will be an interesting and unique way of protection is applied to all the users as an alternative of fingerprint security systems.

<table>
<thead>
<tr>
<th>State / No of Attempt</th>
<th>First Click</th>
<th>Within 3 Clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entry Level (%)</td>
<td>Shuf f le 1 (%)</td>
</tr>
<tr>
<td>Small Image (1)</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>Small Image (4)</td>
<td>95</td>
<td>90</td>
</tr>
<tr>
<td>Large Image (3)</td>
<td>92.36</td>
<td>91</td>
</tr>
<tr>
<td>Large Image (2)</td>
<td>99.1</td>
<td>93</td>
</tr>
</tbody>
</table>

Table 4: Success rate at the Modified Efficient AES

REFERENCES


***