INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

Password Embedding Through Audio Updation In Cloud

S.Santhana priya#1, Mr.S.Varadharajan*2,

*PG Scholar#1, Asst Professor*2.*

Surya group of Institution and Technology,

vikkaravandi

ABSTRACT

Integration of Cloud & Big Data is the most challenging task to handle. Virtualization was implemented for effective data Processing by which integration of Big Data & Cloud was achieved. Virtual Machines may be added or removed as per request. But when it comes under security the password could be hacked through tracing keys in keyboard.The proposed system is designed using audio based password system with an integration of Sound position. Many systems have been developed using the sound, but in the proposed system we used the positioning technique to integrate the sound track. The sound signature or tone can be recalled like images, text etc. Here we play an audio source for some duration, user have to click the audio clip at a particular time, a value is selected with will decide that the user is legitimate or an impostor. We use two kind of algorithm, in the first algorithm we use Audio Point Position for secure the key. In the second algorithm we use a reversible integer transform to obtain the transform domain coefficients.

Index Terms— authentication,, Pointing Running Position, Password Generation, Password Embedding, Password security.

I. INTRODUCTION:

Human factors are often considered the weakest link in a computer security system. There are three main areas where human computer interaction is important: authentication, security operations, and developing secure systems [3]. It is now beyond any doubt that user authentication is the most critical element in the field of Information Security. For the vast majority of computer systems, passwords are the method of choice for authenticating users. Authentication is the first step of information security. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during login time. Mostly user select password that is predictable. This happens with both graphical and text based passwords.

Users wants to select a memorable password, unfortunately it means that the passwords tend to follow predictable patterns that is easy for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords.

The primary goal of improving the current user authentication technology is to make the method secure yet easier for the user. Graphical password authentication systems (GPAS), which consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based password system. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated particularly by the fact that humans can recall pictures better than text [2]. Psychological studies have shown that people can remember pictures better than text. Pictures are generally easy to be remember than text, especially photos,

ISSN : 2454-9924

which are even easier to be remembered than random pictures. It has also been suggested that graphical passwords may be hard to guess or broken by brute force search. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks.

Because of these advantages, interest will improve in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

This project supports both usability and security. Cued click points (CCP tries to propose an authentication mechanism which) is a click-based graphical password scheme, a cued-recall graphical password technique. In addition user wants to select a sound signature during registration process.
Various GPAS have been proposed as alternatives to text based passwords. It can be used as password for folder lock, web-driven applications, desktop lock etc.

The objective of this project is to provide the security for any folders in a computer system by using graphical passwords with view port, sound signature and persuasive cued click-points. Here a graphical password system with a supportive sound signature to increase the remembrance of the password is developed. Here a click-based graphical password scheme called Cued Click Points is presented. In this system, a password consists of sequence of some images in which user can select one click-point per image.

The next image is based on the previous click-point. During login phase, if the selected click-point is not the appropriate one then the system will load an image which is not a part of the password image-sequence. In addition user wants to select a sound signature during registration phase. This sound signature will be used to help the user in recalling the click point on an image during login phase. That is, during login phase, if the user clicks the appropriate point on the image then the sound that the user selected during registration phase will be played. Persuasion is used to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. It can be used as password for folder lock, hard disk locking, web-driven applications, desktop lock etc.

II. LITERATURE SURVEY:

A. **Authentication Using Graphical Password Effect of Tolerance and Image Choice System Concept:**

This Paper using Authentication when user click on the image to authenticate by own rather than alphanumeric string by using pass points Our paper have proposed the concept of using pass point in audio authentication by clicks.

B. CAPTCHA-Using Hard AI Problem for security
System Concept:

The paper uses CAPTCHA based authentication technique used only by the human. System based authentication must have Hard AI Based problem resolution. This was more complex and so the proposed system uses classical unitary transforms with quantization reversible integer transform.

C.Securing passwords Against Dictionary Attacks
System Concept:

This paper defines about the Dictionary Attack that attacks the user authentication and also protect against Denail of Service attack. The same technique has been used in Authentication password for the audio.

D.On User Choice in Graphical Password Schemes
Darren Davis Fabian Monrose, Michael K.Reiter

ISSN : 2454-9924

This paper was based on consideration of posture password authentication for graphical passwords. This includes stylus and mouse input only. Our password authentication will include both the Keyboard and stylus input for graphical input password.

E.Exploiting Predictability in Click based Graphical Password

The paper tells about the prediction of the click between the regular common intervals which give ways to the exploitation of password. Our password input may include the Irregular interval of click between them. This technique was difficult for exploiting the password.

III.PROPOSED COMMUNITY STRUCTURE IN SOCIAL NETWORK:

The proposed system is designed using audio based password system with an integration of Sound position. Many systems have been developed using the sound, but in the proposed system we are using positioning technique to integrate the sound track. The sound signature or tone can be recalled like images, text etc. Here we play an audio source for some duration, user have to click the audio clip at a particular time, a value is selected with will decide that the user is legitimate or an impostor.

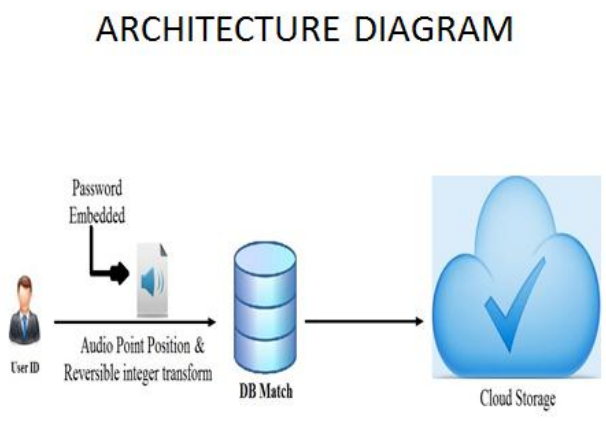


Fig. 1. Architecture for authentication

IV. ALGORITHM STEPS

Step 1: The first step is to specify user name.

Step 2: In this step, the relevant audio file is displayed to the user and he/she selects maximum of four clicks from the audio file set. This is done by specific digits selections, which are stored in the database with the specific username. The user needs to select same number of digits based specific location during the file play.

Step 3: During authentication phase, the user recalls pre-selected location and makes the click. If the click matches the specific position then the user is authenticated else user is rejected.

A) AUDIO POINT POSITION

if host sample a>0
if bit 0 is to be embedded
if a$i-1$=0 then
a$i-1$a$i-2$...a0=11...1
if a$i-1$=1 then
a$i-1$a$i-2$...a0=00...0 and
if ai+1=0 then
ai+1=1
else if ai+2=0 then
ai+2=1...
else if a15=0 then
a15=1
else if bit 1 is to be embedded
if a$i-1$=1 then
a$i-1$a$i-2$...a0=00...0
if a$i-1$=0 then
a$i-1$a$i-2$...a0=11...1 and
if ai+1=1 then ai+1=0
else if ai+2=1 then
ai+2=0...
else if a15=1 then a15=0
if host sample a<0
if bit 0 is to be embedded
if a$i-1$=0 then
a$i-1$a$i-2$...a0=11...1
if a$i-1$=1 then
a$i-1$a$i-2$...a0=00...0 and

ISSN : 2454-9924

if a*i*+1=1 then
a*i*+1=0
else if a*i*+2=1 then
a*i*+2=0...
else if a15=1 then a15=0
else if bit 1 is to be embedded

if a*i*−1=1 then
a*i*−1a*i*−2...a0=00...0
if a*i*−1=0 then
a*i*−1a*i*−2...a0=11...1 and
if a*i*+1=1 then
a*i*+1=0
else if a*i*+2=1 then
a*i*+2=0...
else if a15=1 then
a15=0

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use.

For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage: As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased.

Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable.

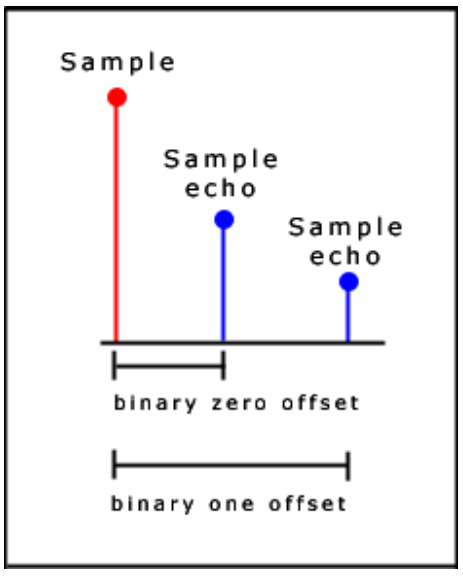
B) REVERSIBLE INTEGER TRANSFORM

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of this artificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude.

As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually a created carrier sound's echo is just heard as extra resonance.

In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.




```
init(Block blocks[])
{

 for (int i=0; i <blocks.length; i++)
 {

 if(blocks[i].echoValue()==0)
```

ISSN : 2454-9924

```
            blocks[i]    =    offset0(blocks[i]);
        else
            blocks[i]    =    offset1(blocks[i]);
      }
    }
     Block offset0(Block block)
     {
       return (block + (block - OFFSET_0));
    }

    Block offset1(Block block)

     {
     return (block + (block - OFFSET_1));
    }
```

The blocks are recombined to produce the final signal.

The "one" echo signal is then multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal. These two characteristics of the mixer signals produce smoother transitions between echoes.

V. BACKGROUND & RELATED WORKS:

A. Authentication Based on Audio Recording Conditions

Passive techniques are useful in detecting for- geries in audio recordings. Such techniques are based on properties extracted from the signal itself, such as frequency spectra introduced by the recording environment, the recording device, or the recording device's power source.

B. Environment-Based Techniques:

Reverberations are decaying echoes of incident sound, produced due to the reflection off walls, ceiling, and other surfaces in a room after the sound source is removed. The decay is modeled as an exponential in form of d(t) ¼ exp(t/t), where parameter t measures the ex- tent of reverberation. We estimate it by maximizing the log likelihood of the sound signal, assuming it to be Gaussian and independently and identically distributed (i.i.d.). Currently, this measure has been successfully applied to synthesized audio with assumptions that can- not be fulfilled by most real-world signals. Thus, it needs to be generalized for a wider range of applications. Although this method uses reverberation solely to differentiate one recording environment from another, another technique attempts to identify the recording environment by classifying it into one of several known categories.12

We can extract the audio-signal characteristics, such as its MFCCs and a few time-based features, and use them to classify different enclosures. Clustering algorithms were applied to these fea- tures to classify the rooms in which amateur audio recordings were made. The best result in classifying the recording environment into one of 10 possible rooms was 41.54 percent accuracy. This method offers a legitimate approach to environment classification, but its performance needs improvement.

C. Device-Based Techniques

The device used to make a recording often introduces other signals, or signatures, which helps us verify the location of recording and, eventually, determine the recording's owner- ship. For example, when analog audio was recorded on magnetic tapes, recording devices introduced flutter and other noise patterns that were characteristic of the device. For digi- tal audio, microphone classification is done using statistical features such as the empirical variance, mean, entropy, LSB flip rate, and MFCCs.

Christian Kraetzer and his colleagues showed, for example, that the recording environment and the microphone type can play a crucial role in successful classifications.12 Their results were

ISSN : 2454-9924

best in noisy environments and in those with high reverberations. The best result they achieved was 75.99 percent accuracy when classifying the recording device into one of five categories (four microphones and original data) was 75.99 percent, which allows room for further performance improvement.

In other work, Robert Buchholz, Christian Kraetzer, and Jana Dittmann proposed a different method that uses the histogram of Fourier coefficients to classify the microphone used to one of several known models.15 These coefficients are taken from near-silent frames to capture microphone properties, not from the signal itself. The researchers reported a test conducted with seven different microphones, and the classification accuracy in this case was 93.5 percent. These results differentiated be- tween microphones from different manufac- turers, but not between two microphones from the same manufacturer. Generally speaking, the reported results using these techniques are still preliminary. There are large differences in classification ac- curacy due to the adoption of different classi- fiers. Furthermore, the choice of thresholds was subjective, and the test sets were small.

- **List Of Modules**

The proposed system can be broadly divided into four modules, namely:

- Pointing Running Position
- Password Generation
- Password Embedding
- Authentication

MODULES DESCRIPTION

A. POINTING RUNNING POSITION

- A user is presented with a Audio and the user passes the authentication by recognizing and identifying the starting or ending part of voice, which he/she selected during the registration stage.
- Here the File running position is calculated.

B. PASSWORD GENERATION

- It encourages users to select passwords where all click-points are hotspots.
- Specifically, when user creates a password, user selects click-points while audio file is running.
- It marks the place in audio file running and takes it as a password during authentication.

C.PASSWORD EMBEDDING

Least significant bit (LSB) coding is used embed password in a digital audio file.

- By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a of data to be encoded.
- This provides security by which password is no need to be stored in Data base.
- By which password is protected even though Data base is misused.

D. AUTHENTICATION

- During authentication, if the running positions are clicked correctly, then the user gets authenticated, else user is rejected.
- Here number of login attempts is limited to three since an extra protection is essential to our password protected system.
- Security is the main reason to restrict access.
- Login attempt-limit blocks a user from making further attempts after a specified limit on retries is reached.

VI. RESULT DISCUSSION:

We use two kind of algorithm, in the first algorithm we use Audio Point Position with quantization in the transform domain to point and to secure the key. The secure data is added in the transform domain coefficients. In the second algorithm we use a reversible integer transform to

ISSN : 2454-9924

obtain the transform domain coefficients. In the integer domain we look at the binary representation of the integer coefficients and join the secure key as an extra bit.

X. REFERENCE

1.Suo, X, Y. Zhu, and G.S. Owen. Graphical Passwords: A Survey. Annual Computer Security Applications Conference, 2005.

2.Tari, F., A.A. Ozok, and S.H. Holden. A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. ACM SOUPS,2006.

3.Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords.16th USENIX Security Symposium, 2007.

4.VanOorschot, P.C., S. Stubblebine. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. ACM Trans. Information and System Security 9(3), 235-258, 2006.

5. Weinshall, D. Cognitive Authentication Schemes Safe Against Spyware (Short Pa-per) IEEE Symposium on Security and Privacy, 2006.

6.Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.

7.Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 102-127, 2005.

8.ZongqingLu,YonggangWen and GuohongCao,"Community detection in weighted networks: algorithm and applications"IEEEjan 2013.

9.P.Hui,J.Crowcroft, and E.Yoneki, "Bubble rap:social based forwarding in delay tolerant networks":a social network perspective,in ACM Mobihoc 2008.

10.B.Chen, J.Xiang,K.Hu and Y.Tang ,Enhancing betwenness algorithm for detecting community in complex networks," modern physics letters B,Vol.28,no.09,2014.

11.F.D.Malliaros and M.Vazirgiannis,Clustring and community detection in directed networks:Asurvey:"physics report,Vol.533,no.4,pp.95-142,2013.

12. T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting Trust and Distrust in Social Networks", in Proc. of the 3rd IEEE Int. Conf. on Social Computing, 2011.

13. A. Ortigosa, J. M. Martín, and R. M. Carro, "Sentiment analysis in Facebook and its application to e-learning", in the Journal of Computers in Human Behavior, http://dx.doi.org/10.1016/j.cshb.2013.05.02, 2013

14. R. Zafarani, W. D. Cole, and H. Liu, Sentiment Propagation in Social Networks: A Case Study in LiveJournal, in Advances in Social Computing, Springer, 2010, pp. 413–420.

15. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and Stein. *Introduction to Algorithms*. MIT Press, 3rd edition, 2009

16. J. M. Pujol, G. Siganos, V. Erramilli, and P. Rodriguez. Scaling Online Social Networks without Pains. In *NetDB'09: 5th International Workshop onNetworking Meets Databases*, 2009.

17. U. Zwick. Exact and Approximate Distances in Graphs – A Survey. In *ESA'01: Procceding of the 9thAnnual European Symposium on Algorithms*, LectureNotes in Computer Science 2161/2001. Springer, 2001.

18. W. Gao, G. Cao, T. La Porta, and J. Han, "On exploiting transient social contact patterns for data forwarding in delay-tolerant networks," *MobileComputing, IEEE Transactions on*, vol. 12, no. 1, pp. 151 –165, jan.2013.

19. J. Leskovec, K. Lang, and M. Mahoney, "Empirical comparison of algorithms for network community detection," in *ACM WWW 2010*.

20. A. Scherrer, P. Borgnat, E. Fleury, J. L. Guillaume, and C. Robardet, "Description and simulation of dynamic mobility networks," Elsevier Computer Networks, vol. 52, no. 15, 2008

21. T. Spyropoulos, T. Turletti, and K. Obrazcka, "Routing in delay tolerant networks comprising heterogeneous populations of nodes," IEEE TMC, 2009

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924