ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Improved Layered Approach for Securing Email Authentication

Shananda Dey, Miss Jharna Chopra

M.E, Dept. of CSE, Shankaracharya Group of Institutions, Bhilai (C.G.), India

Asst. Professor, Dept. of CSE, Shankaracharya Group of Institutions, Bhilai (C.G.), India

ABSTRACT: E-Mail security identifies the collective measures used to guarantee content and the accessibility of service or an electronic mail account. It enables an individual or organization to protect the entire accessibility. An email service provider implements e-mail security to procure information and subscriber e-mail accounts from hackers - and in transit. Email security is an extensive term that encompasses multiple techniques used to fasten an email service. Privacy of e-mail entails making sure it's shielded from unauthorized access. Integrity of e-mail includes a guarantee that an unauthorized person has not destroyed or altered it. Availability of e mail contains ensuring that mail servers remain online and able to service the user community. A layered approach is proposed by the current research for while accessing email info by combining handshaking protocol, routine security, voice recognition and facial recognition attributes for better level of security.

KEYWORDS: Handshaking Protocol, Grid Pattern, Voice recognition, Facial recognition

I. INTRODUCTION

Email, sometimes written as e-mail, is simply the shortened form of “electronic mail,” a system for receiving, sending, and storing electronic messages. It has gained nearly universal popularity around the world with the spread of the Internet. In many cases, email has become the preferred method for both personal and business communication. So, enhance the security provision in essential to maintain integrity and confidentiality of data. From an individual/end user standpoint, proactive email security measures comprise:

- Strong passwords
- Password spinning
- Desktop Computer-based antivirus/anti spam programs

Additionally, it enforces firewall and software -based spam filtering applications to limit untrustworthy, unsolicited and malicious email messages to some user’s inbox from delivery. Confidentiality of email involves making sure it's shielded from unauthorized access. Integrity of e-mail involves a guarantee that it destroyed or has not be altered by an unauthorized person. Availability of e-mail includes ensuring that mail servers remain online and able to service the user community. A weakness in any one among these three vital areas will undermine the security posture of an email system and open the door.

Some of the major threats to email security are:-

- Virus
- Spam
- Phishing

Virus: Viruses email security is endangered by a range of dilemmas. One of the high and most publicized risks of all the problems is viruses. Viruses are not so safe because they often deliver payloads that are exceptionally harmful, bringing down whole email systems, and destroying information.

Spam: Another major threat to email security today is SPAM, often cited by organizations as being their number one concern. Companies lose money when SPAM overloads server and network resources.

Phishing: Phishing is the procedure whereby identity thieves target customers of financial institutions and high profile online retailers, using common spamming techniques to generate large numbers of e-mails with the purpose of luring customers to spoofed web sites and fooling them into giving up personal information like passwords and credit card numbers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

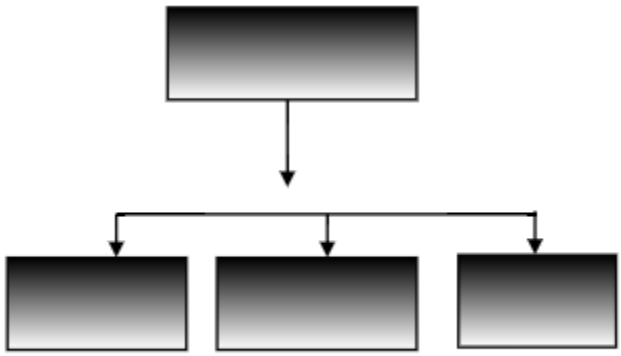

Fig: Threats of Email Security

II. RELATED WORK

Salvatore J. Stolfo and Shlomo Hershkop (2005) describe the Malicious Email Tracking (MET) system is an on-line "conduct-based" security system using anomaly detection techniques to detect deviations from a system's or user's routine e mail behaviour, rather than completely by attempting to identify known attacks against a system via signature-based systems. In this straightforward report, he enumerates the attributes implemented in the EMT system. To do this they carve their information into two sets: a training set and a test set with normal cross-validation methodology. The data mining algorithms used the training set to create classifiers to classify formerly concealed binaries had no examples inside that were seen during the training of an algorithm. This subset was used to examine an algorithms' process over its functionality over new malicious executables and data that was similar, unseen. Both training data and the evaluation were malicious executables assembled from public sources. The receiving system is then able to verify that an e mail advertised as coming from a special domain really came from email servers authorized to send email on behalf of that domain name. SPF and SenderID differ and are incredibly similar in strategy. Some email filtering techniques are based on behavioural characterization techniques designed to concentrate on the email being sent by the behaviours of the performers. Like contextual strategies, probabilistic replies are the result. Bhattacharyya et al. (2002) created a tool called "MET" (Malicious Email Tracker) that mention a client/server arrangement to track numbers of e mail sent and received to determine if there are viral propagations happening. Any viral e-mails that were identified can be filtered out identified, and new viral propagations can be found early.The depiction based approaches to filtering e mail only proper for filtering spam. Since email strikes mimic other average email features like message and speed content and are normally low volume, filtering is problematic.

III.HANDSHAKING PROTOCOL

Handshaking is an automated process of discussion that sets parameters of a communications channel before ordinary communication over the channel begins established between two things. In the process of handshaking following steps are carried out:-

1. The client will select two graphics while registration procedure.
2. The server sends arbitrary set of pictures to client on assessing password and username.
3. The client sends to server and picks on graphic. Once the chosen image is assessed server admits it with second picture along with first image.
4. The login procedure is commenced when the two pictures sent in the server are checked by the client. This confirms server and the communication is taken as trusted.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

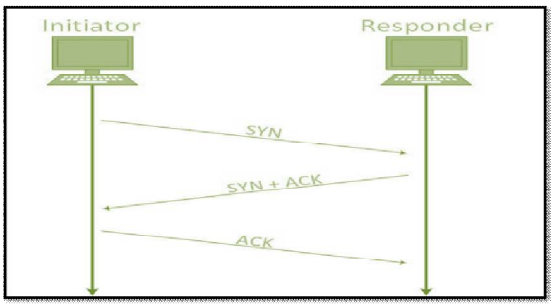

Fig: Handshaking Protocol
(Source: www.cisco.com)

IV.N*N GRID PATTERN

The number grid pattern is a very useful feature for mobile phones. The user first chooses a pin code from the mobile phone settings. This pin is used a major security feature in mobile phone. The user is only authenticated on successful entry of PIN. This N*N grid pattern can also be used as a major verification process in Email systems. Users can select PIN of their own choice while registration. This pin will be verified during the login process.

V.VOICE RECOGNITION

This procedure supplies computers with the ability to listen to spoken language and decide what continues to be said. In other words, it processes audio input by converting it including language. The important steps of an average language recognizer are as follows:

- Grammar layout: Analyses the spectrum (i.e., the frequency) attributes of the incoming audio.
- Signal processing: Clarifies the words that may be spoken by an user and the patterns by which they may be talked and compares the spectrum patterns to the patterns of the phonemes of the language .It also compares the sequence of likely phonemes against the words and patterns of words defined by the active grammars.
- Outcome generation: Supplies the program with info about the words the recognizer has found in the incoming sound.
-

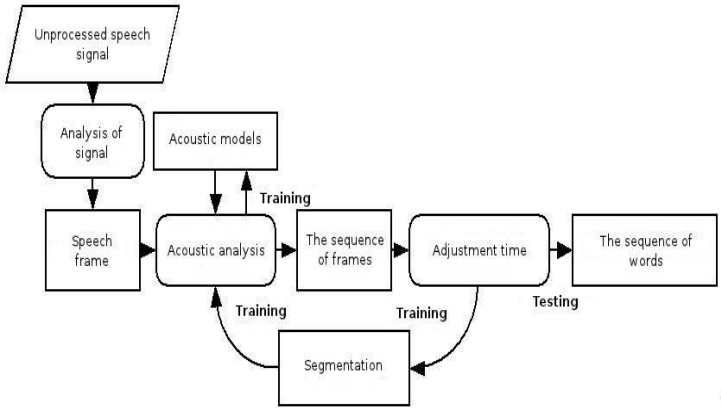

Fig: Speech Recognition process
(Source: http://www.slideshare.net)

In the recognition procedure, the speech signal must be digitized before the signal can be processed by computer. The signal is converted to a sequence of feature vectors according to temporal and spectral measurements. Speech recognition engine which are acoustic model and language model requires two types of file. Acoustic model represent

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

sub- word units or often called phonemes. It's created by compiling audio recordings of language and their transcriptions into statistical representations of the sound that compose each word. W). The language model is a file containing the probabilities of set of controls and words which models are hypothesised. The equation that represents language model is. The vital part of speech recognition system is the search measure. In this step, many blends of words must be investigated to find the most probable word sequence. Depending on the chosen standard, the speech recognition categorizations can be carried base on a tree structure

VI.FACE RECOGNITION

Eigen faces is the name given to a set of eigenvectors when they are used in the computer vision problem of human face recognition. The eigenvectors are derived from the covariance matrix of the probability distribution over the high-dimensional vector space of face images. The Eigen faces themselves form a basis set of images used to build the covariance matrix. This creates dimension reduction by enabling the smaller set of basis images to represent the initial training pictures. Classification can be achieved by comparing the basis set represents faces. To recognize faces, those seen by the system, gallery images, are saved as collections of weights describing the contribution each Eigen face has to that picture. When a fresh face is presented to the system for categorization, its own weights are found by projecting the image onto the collection of Eigen faces. This supplies a set of weights. These weights are then classified against all weights in the gallery place to discover the closest match. A nearest neighbour technique is an easy strategy for finding the Euclidean between two vectors, where the minimum can be classified as the subject that is closest.

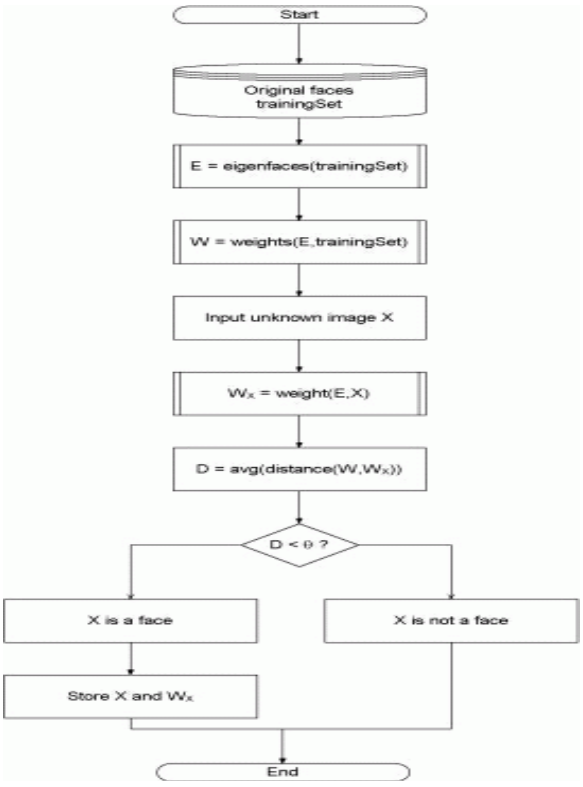

Fig: Eigen Face Recognition
(Source: openbio.sourceforge.net)

VII.METHODOLOGY

The proposed approach is aimed at providing various options of security at user level. The user can choose between layers of security options provided. The current approach has following advantages:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

- Multiple Layers of Security to avoid unwanted usage of essential contents.
- User can choose layers of security as per the need.
- Optimal processing time, delay in communication are avoided.
- Easy to access & benefits of high level of security then existing systems.
- Prevents un-authorized access by adding overlying protection.
- Avoids unusual contact to confidential data.
- User oriented layers of security they can easily add/remove the security layers.

The basic algorithm is as follows:-

1. Display login screen
2. If new user then create profile else initiate login.
3. If login name and password match then initiate security layer 1 handshaking protocol.
4. If authentication at layer1 is success then initiate security layer 2 grid patterns else logout.
5. If authentication at layer2 is success then open inbox else initiate security layer 3 face recognition.
6. If authentication at layer3 is success then open inbox else initiate security layer 4 voice recognition.
7. If authentication at layer4 is success then open inbox else logout

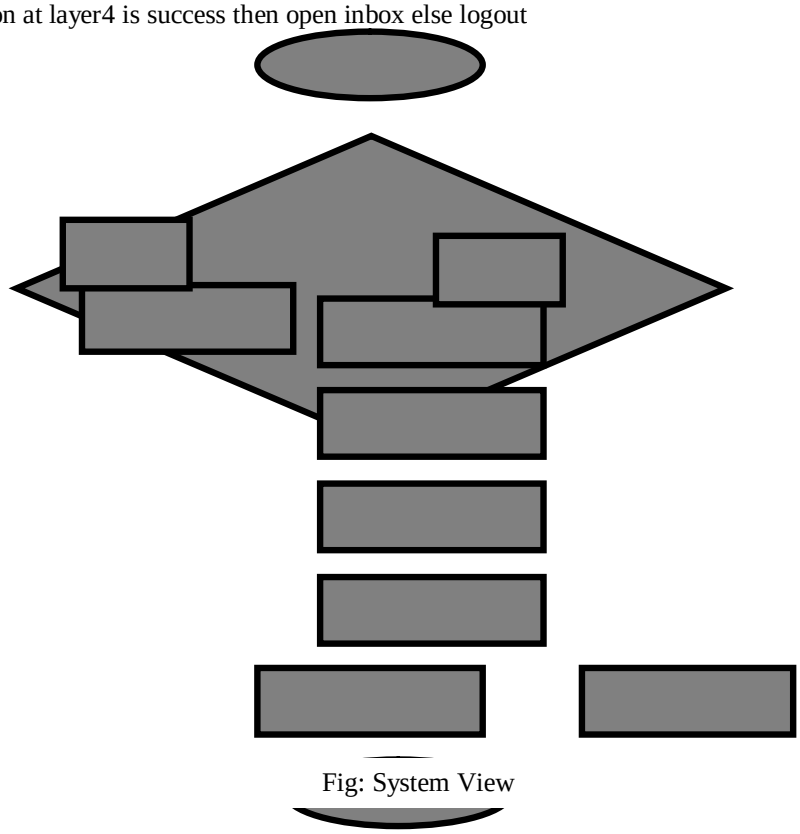

Fig: System View

VIII.EXPERIMENTAL RESULTS

The major features of proposed system are:-

- Prevents un-authorized access by adding overlying protection.
- Avoids unusual contact to confidential data.
- User oriented layers of security they can easily add/remove the security layers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A comparative study has been conducted and following observations have been recorded:-

Basis	Existing System	Proposed System
Login system	Provides only Login Id & password for security.	Provides Login Id & password along with security image & grid pattern.
Security Layers	Login page, captcha & mobile verification.	Login page, image based verification & grid pattern.
User Oriented	User cannot add extra security all things are predefined.	User can add extra layers of security as per need.
Data Security	Anyone can fetch Login id & password & can access important E-mail contents.	Multiple Layer of security adds to the safeguard unusual access of E-mail contents.
Processing Speed	Optimal	Similar to existing one.

IX.CONCLUSION

Now in e-mail systems there no means to check the links between client and server. Handshaking is an automated process that establishes parameters for communication between two apparatus that are different before standard communicating starts. Like the way a human handshake establishes the stage for the communicating to follow, the computing handshake supplies both devices with the fundamental rules for the way information would be to be shared between them. Current password systems make the users pick passwords which can be too complicated for their sake to remember, and this also increases helpdesk costs (or they overuse the password reset option, which is always a threat, e-mail security being basically null); or, more typically, this antagonizes users. A PIN is just a password -- a password which constrained in size and is limited to digits, but a password nonetheless. PIN sound right in other payment devices which sport just little keyboards; likewise, mobile phones, specifically ATM systems and contexts where digits are natural. Since an individual has the full keyboard with letters for a Web site, this really is much less applicable. Remembering passwords and personal identification number will often be cumbersome of users .Using a two component authentication it'll provide the first strong authentication procedure that'll be able to replace passwords. It will now not be essential as you'll be able to log in to your own account by simply using your voice and your face to remember your passwords.

REFERENCES

1. R.M. Amin, Julie J.C.H. Ryan, and J. René van Dorp “Detecting Targeted Malicious Email ” P George .
2. Salvatore J. Stolfo, Shlomo Hershkop, Ke Wang, Olivier Nimeskern,” EMT/MET: Systems for Modeling and Detecting Errant Email” Columbia University {sal, shlomo, kewang, on2005}@cs.columbia.edu
3. Matthew G. Schultz, Eleazar Eskin and Erez Zadok “Data Mining Methods for Detection of New Malicious Executables” Department of Computer Science Columbia University{mgs,eeskin}@cs.columbia.edu
4. J. B. Postel, "RFC 821 Simple Mail Transfer Protocol", August 1982, http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc0821.html
5. Sebastiani, F., 2002. Machine learning in automated text categorization. ACM Computing Surveys, 34(1):1-47.
6. Dwork, C., Goldberg A., Naor M.. On memory-bound functions for fighting spam. In Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003), August 2003.
7. R.J. Hall. How to avoid unwanted email. Communications of the ACM, March 1998.
8. Golbeck, J., Hendler, J. Reputation network analysis for email filtering. In Proceedings of the First Conference on Email and Anti-Spam (CEAS), 2004.’
9. J. Lyon and M. Wong. RFC4406 - Sender ID: Authenticating E-Mail, April 2006. URL http://www.ietf.org/rfc/rfc4406.txt.
10. J. Leslie, D. Crocker, and D. Otis. Domain Name Accreditation (DNA), February 2005. URL http://tools.ietf.org/html/draft-ietf-marid-csv-dna-02.