International Journal on Applications in Information and Communication Engineering
Volume 3: Issue 2: April 2017, pp 1- 4. www.aetsjournal.com ISSN (Online) : 2394-6237

ENABLING SECURITY FOR WEB APPLICATION IN CLOUD

T. Palani Raja Praleesh. P. P, Sanchu. B, Sarath. P. M, Sreerag. P.

Abstract— Earlier, the computer and networks were mostly used by the employee of the organization for data sharing and also to share their hardware resources. For those few decades of its existence, they were used by university researches for sending e-mail and by the industrial employees for sharing hardware. So as in all of these cases, security did not get any attention. But many of them use these networks for many of their needs. Therefore network security became a great concern. So earlier times the data was shared physically, by hardcopy or by administrative means. This project offers security and also usability as it suits well with our practical applications for improving online security. It can be improvised with advertisement data for the CAPTCHA image used in this security means. Puzzle technology used in this project makes the password as graphical password. This whole idea of the security is based on the hard mathematical problem on cryptographic primitive. Both sender and receiver must ensure message integration.

Keywords — : security, password,puzzle,cryptography

I. INTRODUCTION

Most of the security problem focusses on the connection of the corporate network to the internet and the related issues such as malwares and the hacking issues which may be a threat to the data of the corporate. There may also be prevalent many threats to the corporate data which are not related to the internet, it may be internal issues like people which may intrude to the internal system. For such corporates, internal risks are negligible by using firewall. The security primitives are way different for global web, internet. Security is given the highest priority in the case of internet. The inter-connectivity of computers world-wide can create so much vulnerabilities in case of accessibility of personal information by hackers. So the security is to be strictly provided for highly confidential data.

1) Network Security

Security is a vast topic and covers a many aspects ofit. In its simplest form, it is concerned with making sure that unauthorized people cannot read, or secretly modify messages intended for other recipients. It is concerned with people trying to access remote services which they are unauthorized to use. Most security problems are intentionally caused by malicious people who try to gain some benefit of it, like getting attention, or to harm or hurt someone or to retrieve sensitive data. Network security problems can be divided roughly into four nearly interconnected areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information off the hands of unauthorized people. This is the main thing that usually comes to mind when people think about network security. Authentication tidy sum with determining who can you can talk to before revealing sensitive entropy or entry into a business deal. Nonrepudiation deals with signatures and other sensitive documents. Integrity control deals with the continuity of the data and no data is lost anywhere.

2) Techniques in Web Security

Network security consists of the policies and practices taken to prevent and monitor any unauthorized access, misuse, alteration, or denial of a computer network and network-accessible resources or services. Network security involves the authorization of access to data in a network or systems, which is controlled by the network administrator. Users select or are provided an ID and password or other authenticating data that allows them access to information and programs within their access needs. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals who use it. Networks can be private, such as within a company compound access, and others which might be open to public access. Network

T. Palani Raja ME.CSE , Assistant Professor, Department of Computer Science and Engineering , Nehru Institute of Technology, Coimbatore
Praleesh. P. P , UG Scholars, Computer Science and Engineering , Nehru Institute of Technology, Coimbatore.
Sanchu. B , UG Scholars, Computer Science and Engineering , Nehru Institute of Technology, Coimbatore.
Sarath. P. M , UG Scholars, Computer Science and Engineering , Nehru Institute of Technology, Coimbatore.
Sreerag . P , UG Scholars, Computer Science and Engineering , Nehru Institute of Technology, Coimbatore.
s

security is involved in organizations, enterprises, and other types of institutions for their data security needs. It does as name explains: It secures the network, as well as keeps track on the various data changes and interactions on networks between systems.

3) Challenges in Web Security

Websites and web applications face more security threats than ever before as cybercriminals seek to target users via the sites they visit. Keeping up with the latest threats and securing a site is a full time job for concerned people. It requires far more than simple updates and anti-virus software as for usual systems. Understanding the challenges of website security is the first step towards blocking malicious attacks on your site and visitors as well. Website Attacks are Becoming More Advanced day by day. Hackers are on the lookout for every possible vulnerability in websites to break in to steal the data. Many now work as groups with sophisticated software designed specifically to seek out and exploit outdated software, flimsy firewalls, unencrypted databases and many other areas of target to keep up with the hackers. It only takes a single point of entry for a hacker to get in and corrupt a site or steal valuable data which is a major problem.The switch to the Open Web Platform for many web applications has only further complicated the threat landscape which makes the job of hackers simple. Hackers see these applications as more high value, making them desirable targets for sensitive information. Gaining access to even a single login can be enough for hackers to take over your databases.

II. EXISTING SYSTEM

Nowadays the security primitives are based on hard mathematical problems. Basic two step procedure is mostly followed, which is now easily broken .These methods don't cover the security measure to counter the shoulder attacks or attacks inside the corporate environment.

Disadvantages

- This paradigm has achieved just a limited success as compared with the cryptographic primitive based on hard math problems and the wide range of lotion
- Gaining access to even a single login can be enough for hackers to take over your databases.
- It only takes a single point of entry for a hacker to get in and corrupt a site or steal valuable data which is a major problem.

III. PROPOSED SYSTEM

We nowadays tense a new surety primitive person based on hard AI problems, namely graphical password scheme of rules figure on top of Puzzle technology, which we call Puzzle as graphical passwords (CaPRP).CaPRP is both a Puzzle and a graphical password scheme. CaPRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. It is seen that, a CaPRP password can be got only probabilistically by automatic online guessing attacks even if the password is in the search set. We present exemplary CaPRPs built on both text Puzzle and image-recognition Puzzle and finger print. One of them is a text CaPRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on Captcha images. CaPRP offers protection against online dictionary attacks on passwords, which is a prominent way to crack passwords so far. It also is included with much other security systems to tackle all others aspects of security compromises.

Advantages Of Proposed System:

- It go reasonable protection and usability and appears to conniption well with some practical applications for improving online security..
- This threat is widespread and considered as a top cyber security risk. Defence against online dictionary attacks is a more important problem than it might appear.
- Puzzle Login(top of Puzzle technology using mathematical problems).
- Image Puzzle Solving Using AES Algorithm.

IV. MODULES

1. Puzzle Login
2. Random Captcha Selection
3. Fingerprint detection
4. OTP Generation
5. Online Bank

1) Puzzle Login

The security and usability problems present in the usual text-based Login and password schemes have resulted in the making of Puzzle password schemes as a better possible alternative.

We can visualize the sum 1+2+3+...+n as a triangle of digits. Numbers which have such a pattern of dactyl are called Triangle (or triangular) turn , written T(n), the

sum of the whole number from 1 to n meter by the use of Factorial base Login Mystifier Solving.

2) Random Captcha Selection

A CAPTCHA selection is a test is used to separate humans and machines. CAPTCHA stands for "Completely Automated Turing test to tell Computers and Humans Apart." It is normally an image test or a simple mathematics problem which a human can only read or solve, but a computer cannot. It is made to prevent computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts.

Each person is selected randomly and entirely by chance , such that each individual has the same chance of being selected at any stage during the duplicate process, and each subset of n someone has the same probability of being selected for the sample as any other subset of n individuals.. This process and technique is known as simple random sampling, and this method should not be confused with systematic random sampling. A simple random sample is an unbiased process of surveying.

3) Finger Detection

It is process to extract finger regions from input fingerprint image which has normalized intensity and equal in size. The appearance features are extracted from detected finger part which includes changes of finger such as furrows and wrinkles (skin texture).In this system model, an executable (.dll- dynamic link library) file is utilized to extract the fingerprint region. It is used for finger detection process which is based on hear like features and adaptive boosting method.

4) OTP Generation

A one-time password (OTP) is a password that will be valid for only one login session or transaction for a user, on a computer system or other digital device. OTPs prevents a number of disadvantages that are associated with traditional (static) password-based authentication; a number of applications also includetwo factor authentication by ensuring that the one-time password requires access to something a person has as well as something a the person only knows (such as a PIN)

5)Online Bank

Online bank building also known as net banking, e-banking, or virtual banking, is an electronic defrayal method acting that enables customers or the users of a bank or other financial creation to demeanor a kitchen range of financial transactions through that financial institution's website.. The online money box ing system will typically connect to or be part of the core banking system operated by a bank itself and is in direct contrast to branch banking that was the traditional way customers access to the banking services.

V. SYSTEM ARCHITECTURE

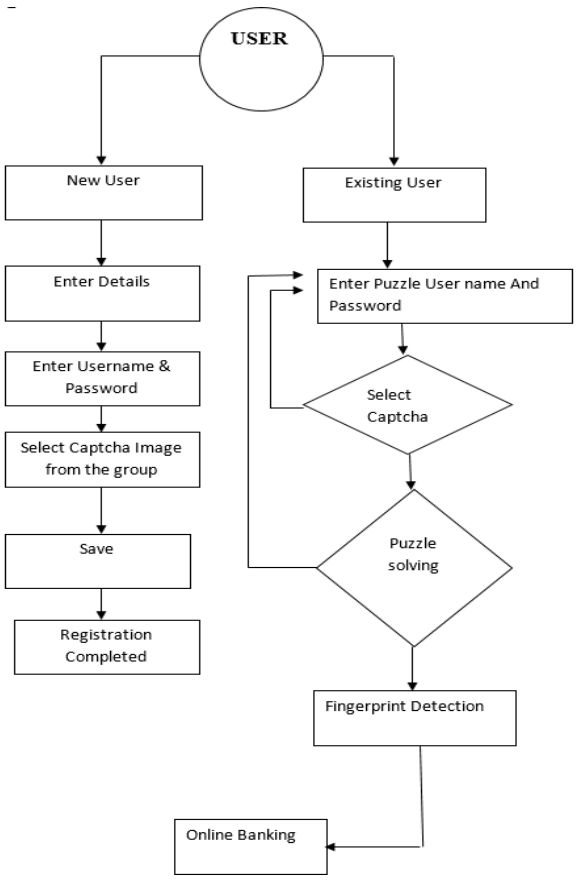

Fig 1 System Architecture

VI. CONCLUSION

The software puzzle with fingerprint system offers reasonable security for improving online security. It may be built upon a data puzzle, it can be linked with any existing server-side data puzzle scheme, and easily moved as the present client puzzle schemes do. CAPTHCHA is widely research field act as internet rectifier to secure web applications by recognized human from robots. Along with CAPTCHA the introduction of unique Fingerprint improves the resistance of online services. CAPTCHA and Fingerprint offers protection against online shoulder attacks on passwords which have been a major threat for many online services. By using this type of security system will help to achieve better usability and security as compared to the password system. CAPTCHA can be easily use by an educated user. No need of technical skill, by using intellectual mind to solve this CAPTCHA and help to reduce time complexity.

VII. FUTURE WORK:

The authors propose use of machine learning classifiers to attacks on captchas. In the same, authors study how efficient statistical classifier is at recognizing captcha letters. In the authors study, how good humans are at solving well-known captchas using Mechanical Detecting and removing lines is a well-studied field in computer vision since the ’70s. Two well-known and efficient algorithms that can be used against captchas with lines are the Canny detection and the Hough Transform Removing noise using a Markov Random Field (Gibbs) was introduced in Many image descriptors have been proposed over the last decades: one of the first and most used descriptors is the Harris Corner detector introduced. However, recently it has been replaced by more complex descriptors that are insensitive to scale end rotation (to a certain extent).

REFERENCES

[1] Adams and M. Sasse. (1999) “Users are not the enemy,” Commun. ACM, vol. 42, pp. 40–46.
[2] Alain Forget, Sonia Chiasson, & Robert Biddle.” Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords” School of Computer Science, Carleton University, Ottawa, Canada
[3] ARTigo, http://www.artigo.org/.2
[4] Birget, J.C., D. Hong, and N. Memon. (2006).” Graphical Passwords Based on Robust Discretization” IEEE Trans. Info. Forensics and Security, 1(3).
[5] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. (2007) ”A Second Look at the Usabilityof Click-based Graphical Passwords.” ACM SOUPS.
[6] Dinei Florencio, Cormac Herley. (2007) ”*A Large-Scale Study ofweb password habits*. International World Wide Web Conference Committee (IW3C2). Banff,Alberta, Canada,pp.657:665,
[7] F. Aloul, S. Zahidi, and W. El-Hajj. (2009) “Two factor authentication using mobile phones,” Proc. Comput. Syst. Appl. pp. 641–644.
[8] FurkanTari,”A Comparison of Perceived and Real Shoulder-surfingRisks between Alphanumeric and Graphical Passwords” Dept. of Information Systems, UMBC
[9] G. E. Blonder.(1996) “Graphical passwords,” U.S. Patent 5 559 961,.
[10] Goldberg.I. (1996) “Visual Key Fingerprint Code” http://www.cs.berkeley.edu/iang/visprint.c.
[11] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. (2012) “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in Proc. IEEE Symp. Security Privacy, pp. 553–567.
[12] Jiangsu, 210016, P.R. China
[13] Jonathan M. McCuneand Adrian Perrig.” Seeing-Is-Believing: using camera phones for human-verifiable authentication”CyLab, Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA, USA
[14] Laur, S. and Nyberg, K. (2006) “Efficient mutualdata authentication using manually authenticated strings “Proceedings of Cryptology and Network Security (*CANS)*, pp.90–107.
[15] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis. (2013) “How to attack twofactor authentication internet banking,” in Proc. 17th Int. Conf. Financial Cryptography, , pp. 322–328.
[16] R . Biddle, S. Chiasson, and P. van Oorschot.(2012)“Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys vol. 44, no. 4, p. 19.
[17] S. Chiasson, P. C. van Oorschot, and R. Biddle. (2007) “Graphical password authentication using cued click points,” in Proc. 12th Eur. Symp. Res. Comput. Security, pp. 359–374.
[18] S. Man, D. Hong, M. Matthews, and J. C. Birget. (2006) "Ashoulder-surfing resistant graphical passwordscheme,"
[19] S.Chiasson, R. Biddle, and P. van Oorschot. (2007) “Asecond look at the usability of click-based graphical passwords,” in Proc. 3rd Symp. Usable Privacy Security, pp. 1–12.
[20] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle2. “Graphical PasswordAuthentication Using Cued Click Points” 1.School of Computer Science, Carleton University, Ottawa, Canada 2.Human-Oriented Technology Lab, Carleton University, Ottawa, Canada (chiasson,paulv)@scs.carleton.ca, Robert biddle@carleton.ca
[21] Zhipeng Liu. ” A Large-Scale Study of Web Password Habits of Chinese Network Users” College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Yudao Street 29, Nanjing,