International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

A COUNTERMEASURE FOR SECURITY INTENSIFICATION IN CLOUD USING CaPGP

[1]**Mohanambal. K,** [2]**Preetha. S,** [3]**Sakthi Priya. N,** [4]**Sindhuja. C,** [5]**Sowmiya. A.**

[1]Assistant professor(O.G), Department of Information Technology, Valliammai Engineering College.

[2][3][4][5]UG Students, Department of Information Technology, Valliammai Engineering College, Tamil Nadu, India.

Abstract *- The malware attacks attempt to deplete the cloud services with bogus request which is a major threat in cloud. A mechanism to intensify the login security in cloud is suggested. The concept of CaPGP – CAPTCHA as Puzzle and Graphical Password is introduced because CAPTCHA is one way to discriminate human and malware apart. The computations at the client side are made intensive than on the server side by making the malwares fail to resolve and attempt to attack. The client is made to resolve the software puzzle that is generated randomly with time constraints where the malware is defeated. The password is made stronger so as to counter the guessing attacks and cookies during login. CAPTACHA's nowadays are cracked easily by Optical Character Reader (OCR) which proves the technological advancement. Hence image based CAPTCHA which requires the verification task to be complete after the mouse click where OCR also fails. Moreover the proposed system shows how to implement the software puzzle in generic server-browser model.*

Index terms: Software puzzle, CaPGP, image based CAPTCHA's, Optical Character Reader.

I. INTRODUCTION

According to the statistics, 70% of the users limit themselves to utilize cloud services, due to several attacks prevailing in cloud. The major attacks include Denial-of-Service attack, Online Guessing attack, and Malware attack. These attacks attempt to deplete our sensitive data in cloud. The seriousness of these attacks has led to the advent of numerous defense mechanisms. Thus, a countermeasure is provided to overcome these attacks. The concept of CAPTCHA as Puzzle and Graphical Password (CaPGP) is used to intensify the security. The advancement in technology where Optical Character Reader (OCR) [2] is used to crack the text based CAPTCHA's which has become more prone to malware attacks. So, image based CAPTCHA's replaces the text based CAPTCHA.

The computational cost at client side is made stronger than at the server side using CPU only code block. The attacker is able to hack the sensitive data by resolving the puzzle using Graphical Processing Unit (GPU) [1]. The GPU has the ability to compute millions of code instructions in a limited amount of time. Thus GPU enables the attacker to easily resolve the computation at lower cost, thus simultaneously reducing the complexity of the attacker. Hence, CPU only code blocks are exploited to defeat against the GPU-inflated attacks.

The randomly generated puzzle is made protective using secret keys and code protection mechanism. The protected puzzle is sent to the client who computes it with some constraints and submits to the server. The server in turn evaluates it with the original solution saved in the database. If both matches then the server permit the access to the services, else the access is denied.

1.2 CPU code block

The CPU processor is much slower than a GPU processor, but one CPU core is comparatively faster than one GPU core. The malwares try to resolve the puzzle algorithm using GPU processor so that the client side computations become less intensive. Thus, the GPU processors are much likely to the malware attacks. The existing puzzle algorithm, assumes that the malwares solves the puzzle using CPU, which is not always true. Currently the malwares use many core GPU to inflate computational capacity which decreases the computational cost ratio. To counter this issue, the generated puzzle in the proposed system could not be resolved using GPU processor. Hence CPU code block is

only used which resists the malwares from cracking the puzzle resolving mechanism.

II. Word Crush

The password in the login phase is made stronger using bubble sorting algorithm. The bubble sort algorithm follows O (n^2) which is highly stable and efficient in sorting compact words like passwords. The password can be entered in any shuffled order. The server in turn uses the bubble sorting algorithm to match it with the original password. This mechanism makes the password stronger against several attacks like guessing attacks.

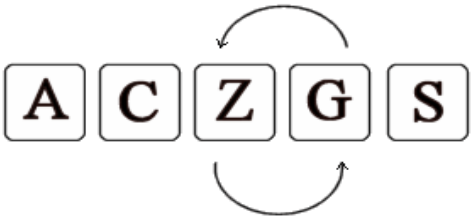

Fig. 2.1- Bubble sorting

The bubble sorting algorithm makes multiple passes through all the elements present in the list unless it is completely matched with the original list. Moreover if there are 'k' items in the list, the bubble sort makes the 'k-1' pairs of items in its first pass. The algorithm used in word crush is illustrated in the below figure.

```
Begin bubblesortAlg(password)
    for all elements of password
      if password[i] > password[i+1]
         swap(password[i], password[i+1]
      end if
    end for
   return password
end bubblesortAlg
```

Fig. 2.2 – Algorithm for word crush

III. Six panel cartoon CAPTCHA

The CAPTCHA – Completely Automated Public Turing test to Tell Computers and Humans Apart is one way to distinguish computers and humans. But nowadays the developing technologies uses the Optical Character Reader (OCR) which can even crack the text based CAPTCHA's. Hence, image based CAPTCHA were used to intensify security. The existing image based CAPTCHA consists of different images which are much prone to the guessing attacks. So, we propose the Six-panel cartoon CAPTCHA which has similar images with unique identification mark. Hence, it would make the intruder difficult to identify the original CAPTCHA image.

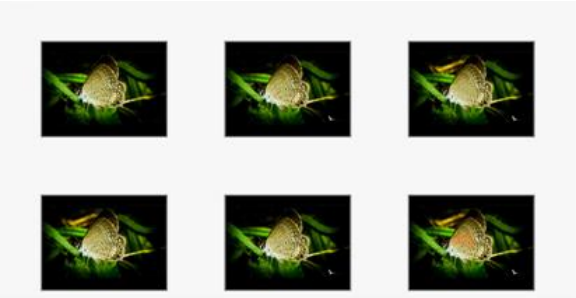

Fig. 3.1 – six panel cartoon CAPTCHA

The Fig 3.1 shows the six panel image based CAPTCHA which gives high resistance to several malware attacks like guessing attack. The unique identification mark remains constant for each user and it is strictly prone to intruder's alteration. In the proposed system, the new user while registration is independent of selecting his own CAPTCHA image, which the attacker is unaware.

The working mechanism in the proposed method is as follows,

- The six-panel cartoon CAPTCHA is selected randomly from the database.
- The arrangement of the six panel cartoon CAPTCHA's are shuffled for every login process.
- The shuffled cartoon CAPTCHA's are imposed to the client logging in.
- The client has to select the original CAPTCHA for authorization purpose.
- The server then validates the selected CAPTCHA with the original CAPTCHA and allows for further access.

IV. Puzzle Generation and Solving Mechanism

In order to construct the puzzle, the server randomly chooses 'n' code blocks from the image database. The server then generates the puzzle using the shift rows and mix columns steps in Advanced Encryption Standard Algorithm. The generated software puzzle's algorithm is not published in advance, which intensifies the security to a greater extent. The puzzle is generated only after the client requests the server instead of publishing it in advance.

The AES algorithm has 128 bits block size and varying key size with 128, 192 and 256 bits. The proposed system is implemented with 128 bits key size having 10 rounds. Each round has the following stages,

- Substitution bytes
- Shift rows
- Mix columns
- Add round key

The client uses the concept of Drag and Drop (DnD) to resolve the puzzle. The main focus on puzzle solving using Drag and Drop is to test the human's cognitive processing where the malicious software or the malwares fails completely.

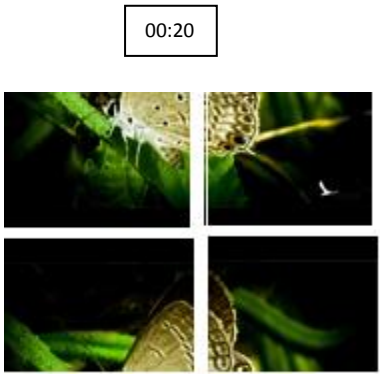

Fig. 4.1(a) – Shuffled image

Fig. 4.1(b) – Rearranged image

In Fig 4.1 (a) the shuffled puzzle image generated is rearranged Fig. 4.1 (b) by the client with some time limitations. The malicious software takes time to initially analyze the image, which fails them to solve the puzzle within specified time. This mechanism is introduced to intensify client computation which simultaneously increases the security.

V. Code Protection

Code obfuscation is one problem where the confusion emerges due to technological development. AES Algorithm provides two layer encryption to resolve the above issue. The outer layer encrypts the generated puzzle and the inner layer encrypts the challenge as data puzzle does.

Once the puzzle has been generated the client has to solve within the specified constraints and submit to the server. The server then validates it with the original puzzle to analyze the user to be authorized.

When the generated puzzle is built on existing data puzzle, the count of generated puzzle is required to be more so that the attacker cannot resolve or crack the puzzle using equivalent GPU core.

VI. Conclusion

In this paper, we focused on enhancing security to cloud applications which is a great threat to cloud services. The novelty is concentrated in creating highly secure image based CAPTCHA's that completely resists the malware attacks like guessing attacks, relay attacks, denial of service attacks etc. The human's cognitive processing abilities are tested during the puzzle solving, in which the malicious code fails. The login mechanism in the proposed work as in word crush is an alternative approach to overcome guessing attack.

References

[1] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng," Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", January, 2015

[2] Takumi Yamamoto,Tokuichiro Suzuki, Masakatsu Nishigaki," A Proposal of Four-panel cartoon CAPTCHA", Japan, 2010

[3] J.Santhiya," A Study on Game-Based Cartoon CAPTCHA", December, 2015.

[4] Chen-Chiung Hsieh and Zong-Yu Wu, "Anti-SIFT Images Based CAPTCHA Using Versatile Characters", Taiwan, 2013.

[5] J.Larimer. (Oct, 28, 2014) pushdo SSL DDoS Attacks. [Online].

Available:
http://www.iss.net/threats/pushdoSSLDDoS.html

[6] C. Douligeris and A. Mitrokotsa, "DDoS Attacks and Defense Mechanisms: classification and state of the art", compta. Netw, vol.44, no.5, pp. 643-666, 2004.

[7] A.Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in Proc. Netw. Distrib. Syst. Secur. Symp.., 1999,pp. 151-165.

[8] T. J. McNevin, J.M. Park, and R. Marchany, "pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks," Virginia Tech Univ., Dept. Elect. Comput. Eng., Blacksburg, VA, USA, Tech. Rep. TR-ECE-04-10, Oct. 2004.

[9] R. Shankesi, O.Fatemieh, and C. A. Gunter, "Resource inflation threats to denial of service countermeasures," Dept. Comput. Sci., UIUC, Champaign, IL, USA, Tech. Rep., Oct. 2010. [Online].

[10] D. Keppel, S. J. Eggers, and R. R. Henry, "A case for runtime code generation," Dept. Comput. Sci. Eng., Univ. Washington, Seattle, WA,USA, Tech. Rep. CSE-91-11-04, 1991.