

IMPLEMENTATION OF SECURITY IN IOV USING QUERY BASED CAPTCHA

Dhanvarshinie R,

Student,

Department of Information Technology,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Hamsini R,

Student,

Department of Information Technology,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Varna K Kumar,

Student,

Department of Information Technology,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Abstract: Network devices are used to congregate data from all over the world, share the assemble over internet for further processing and utilization. This competency serves as the core for Internet of things. IOV has its genesis in the confluence of IOT and mobile internet. But the security issues posed by IOV makes us question its credence. For example, during DDOS, an attacker can deny service to the clients by flooding the network or over consumption of bandwidth. This is where cryptographic verification (private server) and graphical Turing tests(public server) proves useful. They discern legitimate clients and malicious clients. This paper introduces a Query based CAPTCHA technique in VANET with more number of nodes to transmit the packets from client to server. It detects the assailants by using captcha verification during data process. The following parameters are analysed – data delivery rate, efficiency, loss of aggregated data and compares it with the performance of DDOS attack. This project is implemented in TCL, AWK, C++.

I. INTRODUCTION

CAPTCHA is an acronym for Completely Automated Public Turing Test to Tell Computers and Humans Apart.

CAPTCHA a human intuitive verification intended to guarantee the security of sites, which naturally confirms the nearness of human in the web applications. CAPTCHA executions have been established in excess of 3.5 million destinations globally, and people explain in excess of 300 million CAPTCHA consistently.

1.1 TYPES OF CAPTCHA

Text CAPTCHA, which requires the user to view a distorted string of alphanumeric characters in an image and enter the characters in an attached form.

Picture recognition CAPTCHAs, the user is provided with set of images and asked to identify it based on the queries.

Math CAPTCHAs - the user is provided with basic math problem and asked to solve, such as adding or subtracting two numbers.

3D Super CAPTCHAs - the user must identify a 3D image

I am not a robot CAPTCHA- requires the user to check a box.

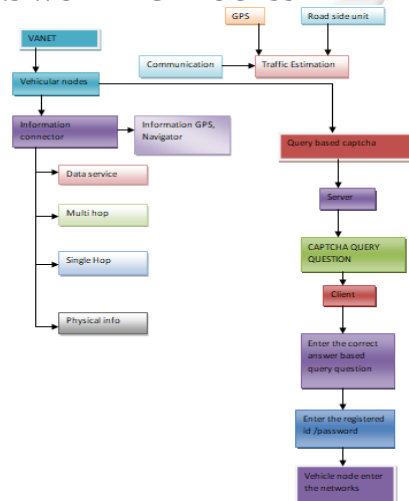
Marketing CAPTCHAs - require the user to type a particular word or phrase related to the sponsor's brand.

1.2 WORKING OF CAPTCHA

CAPTCHAs are a sort of Turing test. Simply, end clients are requested to play out some errand that a product bot can't do. Tests frequently include JPEG or GIF pictures, in light of the fact that while bots can distinguish the presence of a picture by perusing source code, they can't tell what the

picture portrays. Since some CAPTCHA pictures are hard to decipher, clients are typically given the choice to ask for another test.

1.3 WORKING PROCESS



II. DDOS ATTACK

There have been a number of incidents where people use the advantages of internet to spread panic in the society or in an organization. Among the advanced technique used in overwhelming the server, distributed denial of service (DDoS) is the main concern. A DDoS attack can be defined as the phenomenon in which a number of illegitimate systems attack a target thereby exhausting the victim's valuable recourses. The simultaneous incoming request form

different systems located at different places to the target system or server forces it to shut down thereby deny to provide service to legitimate clients.

III. RELATED WORK

^[1] A new Semantic Image CAPTCHA Using Geometric Transformations, a Captcha test should ensure the characteristics automated, usable, secure.

^[2] EmojiCaptcha is a novel method provides enhanced security for the web applications. These cognition based physical actions cannot be performed by any bots. The above method provides more security but performance lacks with respect to OCR attacks.

^[3] A Study of CAPTCHAs for Securing Web Services, presents a general method used to generate and break text-based and image based CAPTCHA's. A huge scope for research exists in designing new and novel CAPTCHA techniques that are user friendly, require less server processing and offer improved security control against bots.

^[4] Security Issues in Cloud Computing explains security issues and threats, detail of distributed denial of service and its solution via Two-Tier CAPTCHA.

IV. EXISTING SYSTEM

In VANET (Vehicular ad hoc network) communication between vehicles is done by Road Side Unit (RSU). Because of the expansion in vehicles, vehicles message are directed to every node in amended time way. Because of remote medium the vehicles messages are influenced due to DDOS(Distributed Denial of Service).

4.1 Disadvantages of DDOS ATTACK

- Efficiency is less.
- Data delivery rate between vehicles is less.
- Loss of aggregated data is high.

V. PROPOSED SYSTEM

Query based captcha technique

In order to overcome this attack Query based CAPTCHA technique is implemented to detect the forgery users by using captcha verification. This verification is done amid the information exchange from client to server with the assistance of intermediate nodes. In this framework, when a vehicle enters the network the admin produces an arbitrary captcha. In addition to this, a random question is raised based on the above captcha. When the client's answer matches the predefined captcha's answer, the client is considered as authenticated user else it is detected as attacker and the process is aborted. After the process, the client is validated with client id and password. If the login credentials satisfy, then the vehicle is allowed to enter the network.

5.1 ALGORITHM

Algorithm for query based captcha technique.

Step1: Initialization of query based captcha from admin.

Step2: Generating random captcha for user's vehicle.

Step3: Generating random query based captcha questions for user's vehicle.

Step4: If ($Q_{\text{random}} = \text{Usr}Q_{\text{random}}$)

$Q_{\text{random}} = \text{Admin captcha question.}$

$\text{Usr}Q = \text{User entered answer.}$

Returns enter into authentication.

Step5: else

Step6: end

Algorithm for authentication process by admin.

Step1: Initialization of authentication from admin.

Step2: Notify to enter the user name and password.

Step3: if ($\text{Usr}_{\text{id}} = \text{Reg}_{\text{id}}$)

$\text{Usr}_{\text{id}} = \text{ID input from the user.}$

$\text{Reg}_{\text{id}} = \text{already register user id.}$

Returns enter into password.

Step4: else

Exit

Step5: if ($\text{Usr}_{\text{pwd}} = \text{Reg}_{\text{pwd}}$)

$\text{Usr}_{\text{pwd}} = \text{PASSWORD input from the user.}$

$\text{Reg}_{\text{pwd}} = \text{already register user PASSWORD.}$

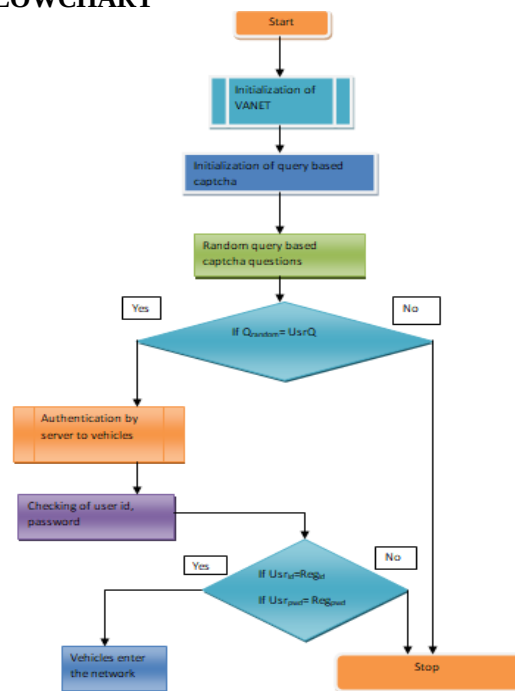
Returns enter into VANET network.

Step6: else

Exit

Step7: end.

5.2 FLOWCHART



5.3 PSEUDOCODE

1. Pseudo code for query based captcha technique

if ($Q_{\text{random}} = \text{Usr}Q_{\text{random}}$)

Returns enter in to authentication.

else

return exit.

2. Pseudo code for query based captcha technique

if ($\text{Usr}_{\text{id}} = \text{Reg}_{\text{id}}$)

Returns enter in to password.

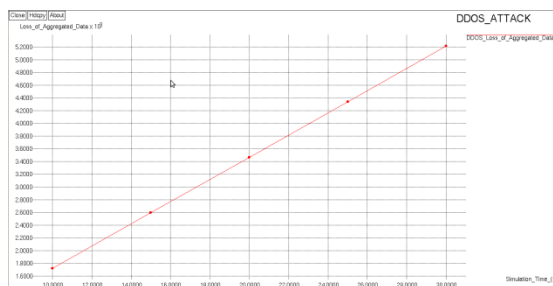
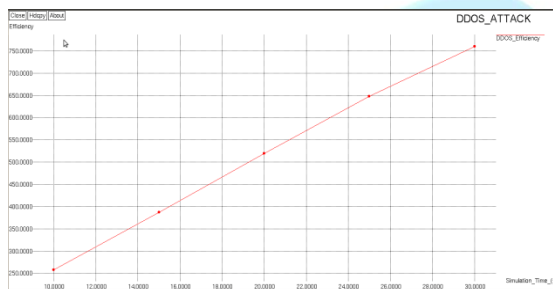
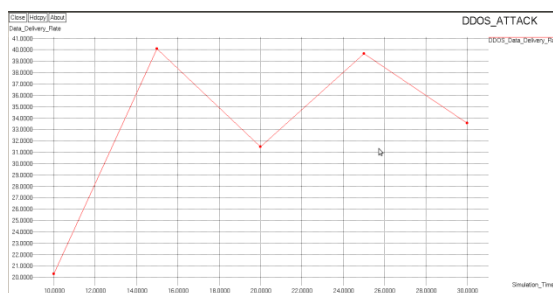
```
else
return exit.
if (Usrpwd = Regpwd)
else
return exit.
```

5.4 ADVANTAGES

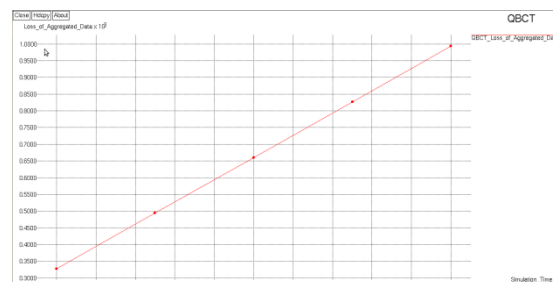
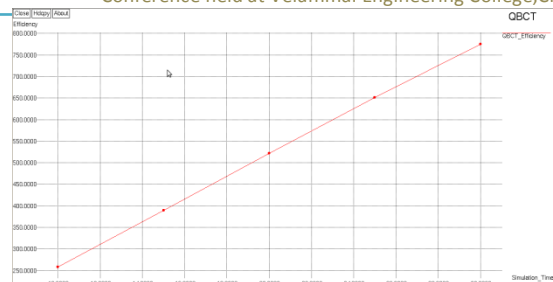
- Efficiency is high.
- Data delivery rate between vehicles is high.
- Loss of aggregated data is less.

VI. SIMULATION RESULTS

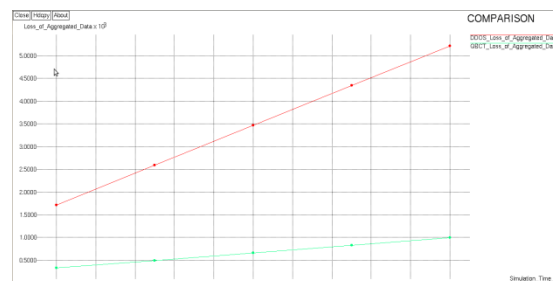
Before attack



After attack:



After attack with Query based CAPTCHA technique



VII. CONCLUSION

The Query based CAPTCHA technique is used to increase the performance after DDOS attack. The parameters such as Data Delivery rate, Efficiency, Loss of aggregated data is compared and output is evaluated which clearly portrays the increase in performance.

VIII. REFERENCES

- [1]. Maryam Mehrnejad Abbas GhaemiBafghi, AhadHarati and EhsanToreini, "SEIMCHA: A New Semantic Image CAPTCHA Using Geometric Transformations," International Journal of Information Security, vol.4, No: 1, September 2012.
- [2]. S. ThangaveluT.PurusothamanG.Gowrison, "EmojiCaptcha: A secured Picture Character approach against OCR Attacks", International Journal of Computer Science and Information Technology & Security, Vol.7,No.1,Jan-Feb 2017.
- [3]. M Tariq Banday N.A. Shah, "A Study of CAPTCHAs for Securing Web Services", International Journal of Secure Digital Information Age, Vol. 1. No. 2, December 2009.
- [4]. PoonamYadavSujata, "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA", International Journal on Cloud Computing : Services and Architecture, Vol. 3, No. 3, June 2013.

