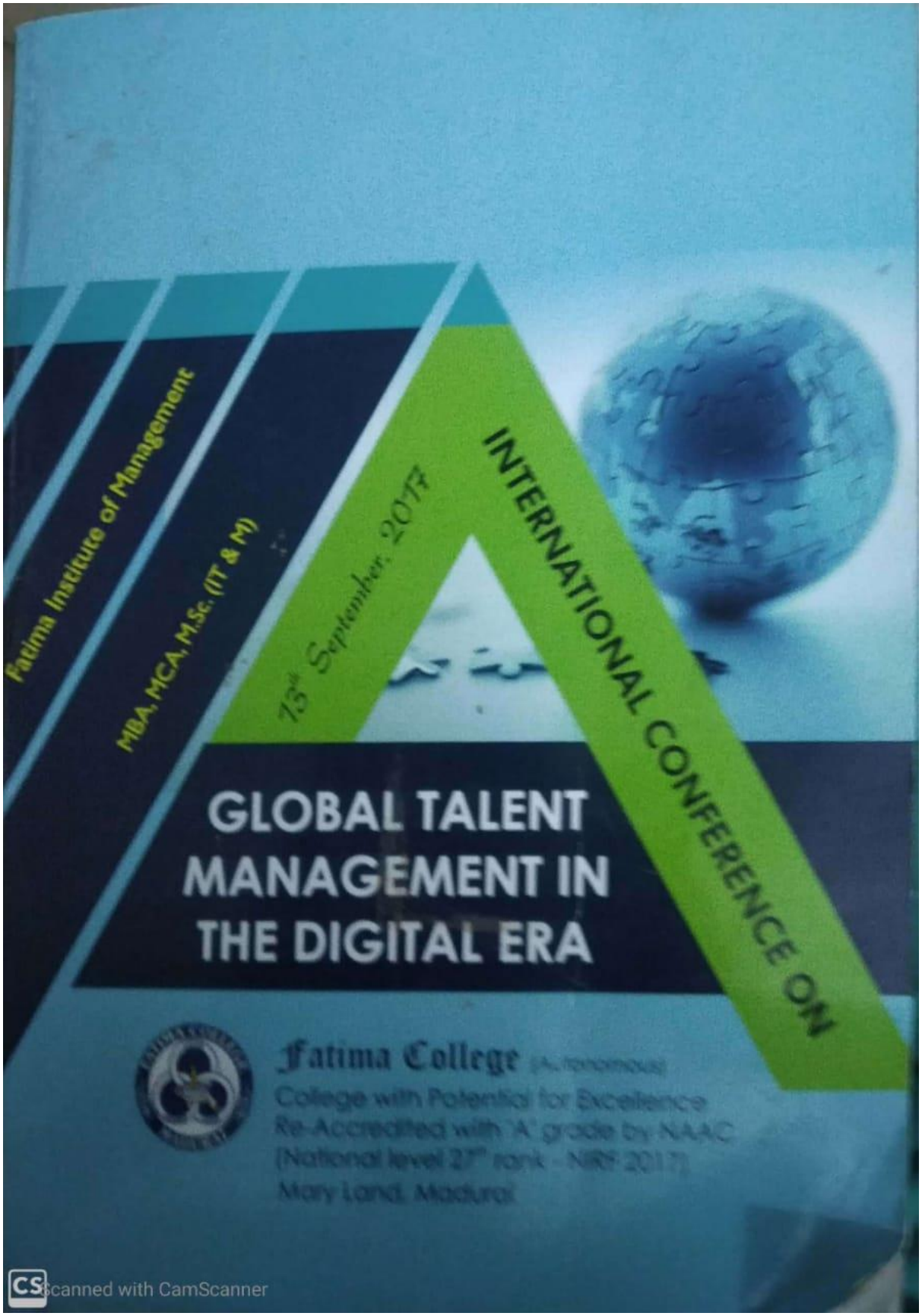

INTERNATIONAL CONFERENCE ON

GLOBAL TALENT MANAGEMENT IN THE DIGITAL ERA

13th September 2017

Organized by

Departments of MBA, MCA & M.Sc. IT

Fatima College (Autonomous)
College with Potential for Excellence
Re-Accredited with 'A' grade by NAAC
(National level 27th rank - NIRF 2017)
Mary Land, Madurai – 625 018.

PREVENTION OF MALWARE USING RASP IN MOBILE APPLICATION

Mrs.R.M.Mallika
Assistant professor, Department of BCom CE, Fatima college, Madurai, Tamilnadu

Introduction

Mobile users demand uncompromised convenience and intuitive functionality on all devices. At the same time, enterprises must prevent confidential customer information from getting into the hands of malicious adversaries who view the mobile environment as an irresistible opportunity.

Enhancing **mobile app security** is a critical element of an effective fraud prevention strategy. VASCO protects the mobile app platform from evolving threats, enabling innovative companies to securely deliver new offerings for the mobile channel.

Objectives

- *RASP Security*

Rasp Security

Malware designed to attack mobile apps and steal your customer's data is at an all-time high. VASCO's DIGIPASS for Apps-RASP provides complete and dynamic protection for your mobile apps by actively detecting, preventing and reporting on attacks, using unique identifiers, and can protect data and transactions from even the strongest attacks by shutting down the app altogether if required.

Runtime Application Self-Protection (RASP)

What is Runtime Application Self-Protection (RASP)

Runtime application self-protection (RASP) is a security technology that is built into an application and can detect and then prevent real-time application attacks. RASP prevents attacks by "self-protecting" or reconfiguring automatically without human intervention in response to certain conditions (threats, faults, etc.).

RASP comes into play when the application is executed (runtime), causing the program to monitor itself and detect malicious input and behaviour.

By moving beyond security only at the perimeter of a network or an endpoint, RASP enables applications to defend themselves.

In real time, RASP analyzes both the application's behaviour and the context of the behaviour. Thus, continuous security analysis is implemented, with the system responding immediately to any recognized attacks.

How Runtime Application Self-Protection (RASP) Works

RASP basically embeds security into the running application where it resides on the server. It then intercepts all calls to the system to ensure they're secure. Ultimately, RASP implants validation of data requests directly into the application.

RASP can be applied to Web and non-Web applications, and doesn't affect the application design. Rather, the detection and protection features are added to the servers an application runs on.