

Fatima Institute of Management

MBA, MCA, M.Sc. (IT & M)

13th September, 2017

INTERNATIONAL CONFERENCE ON

GLOBAL TALENT MANAGEMENT IN THE DIGITAL ERA



Fatima College (Autonomous)

College with Potential for Excellence
Re-Accredited with 'A' grade by NAAC
(National level 3rd rank - NIRF 2017)
May Land, Madurai

**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.**

120	Finding Multiple Spoofing Attackers Using Cluster Analysis P. Ganesh Babu	528
121	E Learning Provides a Platform to Learn. (Survey) Jerrysagayaclinton Jeyaraju	533
122	Healthcare Data Security in Cloud Computing A.Kottai Chamy & C.Nagarajan	537
123	Data Security and Privacy in Cloud Computing Lija.M	542
124	Prevention of Malware Using Rasp in Mobile Application Mrs.K.M.Malini	546
125	Detecting Image Email Using Shape Based Feature Extraction Mallikka Rajalingam	548
126	Resource-Based Security Measures in Anonymizing Networks R.Meenakshi	554
127	An Analysis on Big Data Analytics and Tools V.Rajathi	557
128	An Analysis on Big Data Analytics Techniques Er.J.Rajendran	560
129	Big Data Analytics Tools and Frameworks K.Rajeswari	566
130	Efficient Data Cleaning Algorithm and Swift Unique User Identification Algorithm Using Coalesced Hashing and Binary S. Ranjena Sriram & Dr.S. Sheeja	572
131	Big Data Analytics Features Implement in Oracle M.Sathya & R.Rajareka	579
131	Security Issues on Cloud Computing – An Analysis Vijayalatha.R & Hemalatha.B.V	583
132	Predictive Analysis of Users Behaviours in Web Usage Mining K.Selvaraj & M.Muthu Madhavan	587
133	Smart Glass Technology J.N Amirtha	591
134	Intrusion Detection Using Datamining Technique Ms.S.Sridevi	595
135	Opportunities and Challenges in Cloud Computing Jane. V. A & Stephen.A	599
136	Hybrid System for Microarray Data Mrs.S.Subha	603
137	Data Mining in Education Sector K. Sudharani	608
138	Web Usage Mining: A Review on Data Pre-Processing Techniques N.Vinothini	612

PREVENTION OF MALWARE USING RASP IN MOBILE APPLICATION

Mrs. R. N. Mahesh

Assistant professor, Department of B.Com. CA, 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 DRGPASS 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.