Best Project Groups Year 2013-14

Sr. No.	Name of Students	Title	Area	Sponsoring Company
1	Manasi Belhe Kriti Shrivastava	Graph analysis and mining	Data Mining, Language R	TRDDC
2	Monica Marathe Anagha Lagu Aditi Rathi Shikha Mehta	End-Point Data Loss Prevention (DLP) System for a Malicious User	Information Security, Windows, Visual Studio	Symantec
3	Shreya Joshi Niveda Iyer Gurpreet Khalsa Kanchan Kalokhe	Vault Security	Image Processing, Mobile Application, Android	Persistent Systems Ltd.
4	Aishwarya Raj Priyanshu Chaturvedi Shikha Singh Sneha	Multi-protocol Connector/Device Simulator	Testing Framework,	IBM
5	Mayuri Naware Devika Sadekar Sunanda Shanbhag Sapna Shenvi	Screen Sharing between remote Android devices	Mobile Based, Android	GS Labs

Graph analysis and mining

Abstract

With the increasing reliance of business on IT, the success of today's business highly depends on the success of its underlying IT system. Hence, it is becoming increasingly important to better understand and control the IT operations.

IT systems are becoming complex day-by-day with continuous evolution and increasing scale and complexity. These systems lack end-to-end transparency which makes it difficult to maintain and upgrade IT system. The system become highly brittle and unpredictable to any change in the system. Various data sources are available to capture IT operations such as system alerts, CMDB, Monitoring data, etc. Intelligent mining of these data sources can help analytics operations.

The Focus of this research is to end-to-end transparency.

We aim to discover entities, mine their relationships, and create maps of IT operations. These maps can be used to derive many increasing observations and insight into IT behavior.

There are various application of these graphs such as detection of resolver communities, generation of problem signatures, and analysis of changes in the system etc. We limit our scope to one such application that is improving the transition of operations and generating an efficient transition plan. Transition Methodology is the process of migrating knowledge, systems, and operating capabilities between two organizations, for example, from an in-house staff to an outsourcing environment. The overall success of the outsourcing engagement is very much dependent on the effectiveness of the transition. The current approach for transition is intuitive and not analytics driven hence is inefficient, costly can carries risk. We propose to generate an efficient transition plan using analytics.

End-Point Data Loss Prevention (DLP) System for a Malicious User

Abstract

The creation and sharing of digital information within a typical enterprise continues to accelerate. Every company has sensitive information concerning various business aspects of the organization that should be kept securely. A single “insider” breach of sensitive data, whether inadvertent, internal or downright malicious, can expose the company to far reaching financial, public relations, legal and brand reputation costs.

A comprehensive solution in the form of a Data Loss Prevention (DLP) system will help an organization find, classify , and control the use of sensitive data throughout company. The system will reduce the risk of loss of data, which can be in the form of private or company information, intellectual property (IP), financial or patent information, credit-card data, and other information depending on the business and the industry. It will prevent and/or monitor and report the inadvertent or malicious disclosure of sensitive information. Thus the system will prevent violations of general corporate security and behavioral policies.

Our proposed system for DLP handles a malicious user attempting an illegitimate access to a sensitive document from an unknown user application. Based on the level of sensitivity of the document, desktop activity is captured and a DLP incident attaching the desktop is reported to the administrator. If the document is highly sensitive, the unknown application is blocked from opening the document at endpoint. A prototype for this system has been built on Mac OS.

Vault Security

Abstract

Vault Security was contemplated in mind the rise in theft now-a-days. It is basically a surveillance system with the added feature where the user gives a list (Images) of authorized users. During a break-in of the vault, an image of the intruder is captured and matched against database. On database recognition, the user receives a notification on his Smartphone via an application. Thus this security system helps identify the perpetrator (in case of a theft). Vault Security system can be used for residential as well as commercial purposes. Also taking into consideration the nominal cost for setting up the system “ Vault Security” is the best option for safeguarding all assets.

Multi-protocol Connector/Device Simulator

Abstract

Software testing is any activity aimed at evaluating an attribute or capability of a program or system and determining that it meets its required specifications. All software developed need to be tested before they can be deployed. The same case is true for any cloud based software or application.

Cloud testing is a means of testing cloud-based applications that use resources found in the cloud. By resources we mean any element (hardware, software and infrastructure) necessary to carry out the tests. But testing of cloud applications needs all the related devices to be present at the time of testing. If the devices are present then the testing process can be commenced easily and one can proceed for further development. But if any of the required devices are not present then the overall process of application development is impeded

In such cases there should be a way with which we can substitute these devices This can be achieved by simulators.

The simulator provides a generalized and extensible framework that enables modeling, simulation and experimentation of emerging cloud application and services. Our project includes the testing based request and response via various prominent protocols like HTTP, REST, and SOAP etc. However the simulator does the sanity testing. Thus our project resolves the availability issue of cloud devices and accelerates the testing process for a cloud based application.

Screen Sharing between remote Android devices

Abstract

As smart phones become increasingly powerful, the experience of sharing the small screen becomes more compelling for the average user. There have been several desktop application, which facilitate screen sharing between remote desktops as well as from desktop to mobile phones. However, screen sharing of Android phones has always been a problem because of the lack of permissions granted on the application layer.

This project is to develop a screen sharing application for Android OS. This application will share the screen of sender's mobile phone with recipient's device. Modifying the Android OS, which will allow devices to share screen without requiring root access, is an approach that will be used to develop the application. The reason being, in the present version of Android OS, the screen's information is stored in a data structure called the Framebuffer. But at the application level of Android, access to the FrameBuffer is restricted. Hence, in order to have access to it, the application will be developed in the Framework layer of the OS and thereby modifying the Android OS. Changes made in the framework layer will facilitate this sharing of screen.

Screen sharing can also be further developed to support controlling the remote device, which would help broaden its application.