Jul - Dec- 2017

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Dwarka, Sector-9, New Delhi

Trinity Tech Review

Advisors

Dr. R.K. Tandon Chairman,
TIPS, Dwarka

Ms. Reema Tandon Vice Chairperson
TIPS, Dwarka

Editor-in-Chief

Prof. (Dr.) Vikas Rao Vadi
Director, TIPS Dwarka

Editorial Board

Prof. (Dr.) Sunil Kumar Khatri
Director, AIIT, Amity University, Noida

Prof. Prashant Johri
Director, Galgotia University

Prof. Naveen Kumar
Associate Professor, IGNOU

Prof. (Dr.) Saurabh Gupta
HOD (CSE) Dept, NIEC

Ms. Ritika Kapoor
Assistant Professor, TIPS, Dwarka

Ms. Shweta Sharma
Assistant Professor, TIPS, Dwarka

Vol 3, Issue 2

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Copyright © March 2015 Trinity Institute of Professional Studies, Dwarka. All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the under mentioned.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Sector-9, Dwarka, New Delhi-110075
Ph: 45636921/22/23/24, Telefax : 45636925
www.tips.edu.in, tips@tips.edu.in

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
"A+" Ranked Institution by SFRC, Govt. of NCT of Delhi.
Recognised under section 2(f) of the UGC Act, 1956
&
NAAC Accredited "B++" Grade Institution

STATEMENT ABOUT OWNERSHIP AND OTHER DETAILS OF TTR/TMR

FORM 5 (RULE 8)

1.	Printer's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
2.	Place of Publication	:	Delhi
3.	Periodicity of Publication	:	Quarterly
4.	Publisher's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
5.	Editor's Name	:	Dr. Vikas Rao Vadi
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
6.	Name and Address of the individual who owns the journal and partners or shareholders holding more than one per cent of the capital.	:	CHAIRMAN Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
7.	Hosted at (url)	:	www.tips.edu.in

I, Dr. R.K. Tandon, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.K. Tandon

Phishing –A Threat To Network Security

Shweta Sharma

This article surveys the literature on the Detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in end users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. To reduce the phishing attack, it is necessary to make awareness among the web user about the type of websites and spread the message to the web user that how the phishing website steal the confidential information of the web user. The web browser is used to access the websites so the web browser based solution can be helpful to the web user to protect their confidential information from phishing attack. The web browser can directly warn the user about the type of website with the help of add-on which is an optional tool installed on it. This solution is more effective than other solutions for protection from phishing attack. In addition, the web browser market is mostly using three browsers i.e. Internet Explorer, Mozilla Firefox and Google Chrome which comprises around 90% of the total web browsers use ,So these web browsers taken for the testing and finding the result at education institute. The study shows that when Firefox 2 web browser shows the phishing warnings on its display, none of the users entered sensitive information into the websites. The same study recommended that the result analysis of Internet Explorer's phishing warning. It is necessary that the web browser should accurately identify the phishing web sites (low false positive result) so that the user can trust on the web browser's warning messages. Some web browsers are already providing the alert system for possible malicious attacks. If the website is not having HTTPs protocol and the user is feeding their credential information on it, the web browser should display the alert message to the user about the possible phishing attack. If the website is suspicious then the web browser checks the security certificate whether it is present in the website or not. After checking the security certificate, the web browser alerts the user about the type of website. To check the performance of anti-phishing tools, a research study has been done at an educational institute. The concept behind the designing of the Anti-phishing tool is that when internet user hit the URL, a dialog box appear on the screen that inform the user about the type of the website whether it is phishing or not. In the proposed add-on, the system is divided into five different assigned groups and the performance of the system tool is tested by data mining algorithms.

The aim of the scams vary, victims might be tricked into a clicking a link through to a fake website with the aim of persuading them user to enter personal information. It is estimated that an average of 1.4 million of these websites are created every month.

Other types involve tricking users into downloading and installing malware for stealthy approach to theft or unintentionally installing ransom-ware, providing the attacker with much more immediate profit. More comples phishing schemes can involve a long game, with hackers using fake profiles, emails and more to build up a rapport with the victim over months or years in such cases where specific individuals are targeted for specific data which they would only ever hand over to people they trusted. That data can be as simple as an email address and password, to financial data such as credit card details or online banking credentials or even personal data such as date of birth, address and a social security number. Anyone can be a victim, ranging from the Democratic National Committee to critical infrastructure, to commercial businesses or even individuals.**Phishing E-mail Campaigns and Phishing Site Trends – 2nd Quarter 2017**

The number of unique phishing email reports (campaigns) was largely consistent from month to month, except for a 21 percent spike in March 2017:

DETECTING PHISHING THROUGH PHISHTANK

Online fraud prevention databases such as Phish-Tank maintains URLs for millions of verified spoof websites used in phishing attacks intended to mimic thousands of legitimate entities. Concocted websites deceive users by attempting to appear as unique, legitimate commercial entities such as shipping companies, escrow services, investment banks, and online pharmacies. The objective of concocted websites is failure-to-ship fraud; taking customers' money without providing the agreed-upon goods or services. Both spoof and concocted websites are also commonly used to disseminate malware and viruses.

Anti-phishing tools are a type of protective technology designed to protect users against phishing attacks that rely on spoof or concocted websites. Existing anti-phishing tools use fraud cues and blacklists to determine whether a particular website is legitimate or a phish. Fraud cues are website content, linkage, and design elements that can serve as reliable indicators regarding the legitimacy of a website. These cues, which are generally derived from the body text, URL tokens, source code, images, links, and domain registration information of known legitimate and phishing websites, are then input into machine learning classification algorithms. Blacklists are databases of URLs for known phishing websites developed and maintained by online communities such as Phish-Tank. Blacklists are used by lookup-based tools, including anti-phishing security toolbars found in web browsers such as Internet Explorer and Firefox. Moreover, performance is also impacted by whether the website is concocted or a spoof . Accuracies for commonly used and state-of-the-art anti-phishing tools fall between 55% and 92%.

Encryption Decryption Technique For Cloud Computing Architecture

Santosh Kumar Singh

ABSTRACT:

Cloud the client like electricity grid. Distributed computing has increased incredible consideration from industry yet there are still numerous issues that are in their primitive stage fussing the development of Cloud. One of these issues is security of information frameworks allude to the accumulation of interconnected servers that are provisioned powerfully on request, for execution of application, to put away in the servers of data centres of Cloud computing suppliers. Numerous plans have been created. These plans have been Contemplated, examined and new technique has been proposed which infix the parameters of security like recuperation of information and classification of information such that it guarantees security of information put away in the servers of Cloud frameworks. The proposed plan depends on two techniques – Information Dispersal Algorithm and producing key from the image. Data dispersal calculation helps in keeping up classification and uprightness of information and key produced from picture will helps in recuperation of information.

1. INTRODUCTION

Big organizations like Google, Amazon, and Yahoo give services to users throughout the world with the help of websites hosted on the servers of their datacenters. Many centers were established by them to handle requests from users throughout the world. These organizations bought and established servers according to the peak traffic for the website; but, most of the time during a day, these servers were idle. There are many small organizations which have innovative ideas; but, they do not have enough

2. OBJECTIVE

a) To avoid or decrease all such cost, complexities, services and wastage of resources.

b) To meet the demands of user requests during peak hours.
c) To give the freedom to access the stored data like videos, photos and documents wherever internet is available like Apple's iCloud.

3. ABOUT CLOUD COMPUTING

Cloud Computing can be described as "a sort of parallel and appropriated framework involving an amassing of between associated and virtualized PCs that are powerfully provisioned, and presented as one or more brought together processing assets in light of organization level assentions developed through course of action between the organization supplier and the clients".

Characteristics of Cloud Computing:

a) It is a sort of customer server model such that customers are administration requesters and servers are service providers.

b) There are heterogeneous sorts of servers accessible at service provider site to satisfy the differing requests of customers.

c) Cloud Computing is like utility Computing. The services are given because of the measure of assets utilized for the given time.
d) Location independent.

Types of Cloud:

Cloud systems are separated into classes on the premise of the sort of customers which will be taking its services. Distinctive sorts of Cloud accessible are as per the following:

a) Public Cloud
b) Private Cloud
c) Community Cloud

4. IMPLEMENTATION ISSUES ON CLOUD COMPUTING

There are diverse issues in Cloud that is keeping relationship from using Cloud. These issues are according to the accompanying:

a) Privacy: Cloud advantages process customers' data on machines that customers don't have or work, this presents security issues and essential clients' control.

b) Security: While driving Cloud administrations suppliers use information stockpiling and transmission encryption, customer confirmation etc.

c) Reliability

d) Ownership: Once information is committed to the Cloud, a couple people stretch that they would lose a couple or most of their privileges of their information.

e) Data versatility and change

f) Intellectual property: An association makes something new and it uses Cloud administration as a component of the innovation.

5. PROPOSED WORK AND PROCESSING

Here a new data storage security scheme for Cloud systems has been proposed in this research viz. Images based recursive information hiding scheme. The proposed plan fulfils all the expressed goals. It depends on two techniques:

a) Data (Information) Dispersal Algorithm
b) Generating key from image using RSA algorithm.

Input/output structure for proposed work: Index Page to store data on the Cloud.
Inputs
Input the text file
Input an image file for key.

Processing
Text file is divided into several shares.
RSA Key is generated from the image for encryption of the shares.
All parts (shares) of the file are then encrypted using the key.
They are then stored in the Cloud having different servers.
On Sending Files to the servers, System monitoring

the cloud accesses its database and gives the information regarding the servers available in the Cloud. It contains IP Addresses of the servers. CloudSim3.0 library is used to create Virtual Cloud. After getting the IP Addresses of the servers, file is divided into equal shares. Image Files are used to create key for encryption process. Shares are then encrypted using this key. All these shares are stored in the cloud using the IP Addresses information. Information related to the encrypted share, their storage system IP address, key used in storage of shares are stored in the Cloud Monitor.
Shares are decrypted using AES algorithm using Image key as a decryption key which is generated using RSA. After decryption, shares are combined to get the input file. If the image used for encryption matches with the image used for decryption then only the data can be retrieved.

6. MATERIAL AND TOOLS UTILIZED

For mimicking Cloud applications, CloudSim is the best recreation apparatus accessible. CloudSim is an extensible reenactment toolbox that empowers displaying and recreation of Cloud registering frameworks and application provisioning situations. It executes bland application provisioning strategies that can be reached out easily and constrained endeavors.

CloudSim propagation instrument take after Java. In this instrument, all components are classes and the limits that these substances can perform are selected as methods. In the wake of growing a component class, methods are called to play out the application.

7. IMPLEMENTATION:

For the simulation of experiment in CloudSim, certain parameters of Cloud have been set. These parameters are:

1) One user – There is only one user in this experiment who sends one file to the Cloud for data storage in its servers.

2) One Datacenter Broker – In this experiment, only one datacenter broker is included.

3) One Datacenter – Generally, there are many datacenters available with Cloud service provider and datacenter broker chooses one of these datacenters depending on the QOS requirements of the user. However, in this experiment, only one datacenter is included and it is assumed that this datacenter meets the QOS requirements of client's application.
4) Fifteen hosts – Generally, there are thousands of hosts available with each datacenter of Cloud service providers; but, in this experiment only fifteen hosts are taken considering the size of file.

Hardware characteristics of hosts – The hosts are of heterogeneous nature at Cloud service provider's organization. This feature is important in cases where compute service is provided by Cloud such that hosts are assigned according to the computing requirements of the application. But in storage servers, this feature is not important.

Table: Server Table in Cloud Monitor

Servers Information	Type_of_data	Description
Server_ID	Int	Unique Server ID
Server_IP	Character	Server IP Address

A database is maintained in the monitor of the cloud. Suppose there are five servers – Server1, Server2, Server3, Server4, and Server5 in the cloud. Information related to the storage are stored in Storage table in Cloud monitor.

Table: Storage Table in Cloud Monitor

Information Stored	Type_of_data	Description
Share_Name	Int	Share_Name
Server_IP	Character	Server IP Address
Key_value	Character	Key used for encyption
Filename	Character	Filename
FileNo	Int	Sequence of share

Data is stored in the form of decrypted files in the server.

Table: Files stored in servers after encryption using image key

Server 1	Server 2	Server 3	Server 4	Server 5
S1.dat	S2.dat	S3.dat	S4.dat	S5.dat
S6.dat	S7.dat	S8.dat	S9.dat	S10.dat
S11.dat				

In Second Phase these shares are decoded to get S1.txt from S1.dat, S2.txt from S2.dat, S3.txt from S3.dat, S4.txt from S4.dat, S5.txt from S5.dat, S6.txt from S6.dat, S7.txt from S7.dat, S8.txt from S8.dat, S9.txt from S9.dat, S10.txt from S10.dat and S11.txt from S11.dat with same IMAGE key and joined to a solitary file S. On Downloading ClousSim3.0, Hard storage Drive class is inherited by Cloud Hard drive Storage. Cloud Hard drive Storage Class is calling the constructors of Hard drive Storage Class. It is also using the functions of Hard Drive Storage Class to store the files on the cloud.

8. FUTURE SCOPE:

This exploration is for online information stockpiling in a distributed computing environment. The proposed work portrays the utilization of an information apportioning plan called Information dispersal for actualizing such security. The chunks of data after encryption are put away on the servers. Cloud information stockpiling has numerous focal points. It's not expensive, doesn't require establishment, needn't bother with supplanting, has reinforcement and recuperation frameworks, has no physical nearness, requires no faculty and doesn't require vitality for force or cooling. Cloud information stockpiling however have a few noteworthy downsides, including execution, accessibility, contradictory interfaces and absence of gauges. In this exploration work, servers are picked in the system and they should be recovered to reproduce the first information. Information reproduction obliges access to every server, and the learning of the servers on which the information or data are put away. This plan may likewise be utilized for information security as a part of sensor systems and web voting conventions, in armed force for sending private information's.

Developing the TweetBot

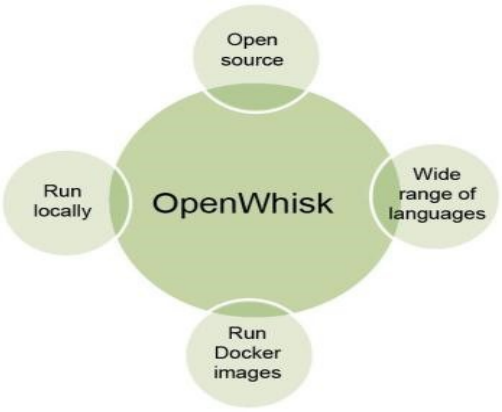
Nisha Bansal

Introduction:

It would be nice to automatically retweet the tweets that have our favourite hashtags (such as #serverless or #opensource). That's the topic we'll explore in this article. We are going to implement a bot (let's call it TweetBot), in which one can specify the hashtags to retweet at specified time intervals. We will start with writing an auto-retweeting code in Python and get it working on our machine. Later, we will deploy it in OpenWhisk on IBM Bluemix.

Development:

In order to write the Python code for auto-retweeting, the prerequisite is that Python 3 must be installed in one's machine.The Twitter API provides programmatic access to read and write Twitter data, create a new tweet, read user profile and follower data, retweet, and more. For this, one must first create a Twitter application (https://apps.twitter.com/ and note down the Oauth credentials for the bot configuration. The Twitter API in Python can be accessed using the TwitterFollowBot Python module. Using this module, you can do much more than just retweet - you can auto follow and aut -like. For developing the TwitterBOt, one must install the module into a folder rather the default bin directory. For that, use the following command : pip install --target <target_folder> TwitterFollowBotLet us now create a program that uses the TwitterFollowBot Python module to retweet the latest 'count' number of tweets with a specific phrase for e.g. '#Serverless'. For that, we need to create a TwitterFollowBot instance. The TwitterFollowBot uses the config.txt file in the current directory to configure the bot.




```
# Program to retweet five latest tweets based on a hashtag (#Serverless)

from TwitterFollowBot import TwitterBot

def retweet():

# create an instance of the TwitterFollowBot

# by default, the bot will look for a configuration

file called config.txt

# in your current directory

my_bot = TwitterBot()

# autoretweets the 5(count)

latest tweets that matches the hashtag

my_bot.auto_rt("#Serverless", count = 5)

return {'message' : 'retweeted successfully'}

retweet()
```

When we execute the Python script, it connects to the Twitter API and retweets. The result throws up a warning indicating that the followers.txt isn't updated; you can just ignore that warning or update the files to get rid of the warning. The program displays the tweets that are retweeted, so we know it is working.After we get the code working in our machine, it is time to deploy and execute it in the cloud using the serverless approach. We are going to use Apache OpenWhisk as the serverless platform. We will use IBM Bluemix as the cloud platform to deploy the OpenWhisk action(s).

Apache OpenWhisk

Apache OpenWhisk is an open source serverless cloud platform that executes functions in response to events at any scale.OpenWhisk was started by IBM and is now incubated by Apache. Adobe is an important contributor to the project and has contributed the API Gateway. OpenWhisk executes functions (called actions) in response to events (called triggers). Since it is serverless, you just need to provide your code to be executed; specifically, you don't need to concern yourself with how to manage the life cycle or operations of the underlying containers that execute the code.

Here are some key aspects of OpenWhisk:

It's open source. If you want, you can explore the code and tinker with it, and change it according to your requirements. Support for a wide range of programming languages including Node.js 6, Python 3, PHP 7.1 and Swift 3.1.1 is available.

Actions (serverless functions) can also be custom executable programs packaged in a Docker container, i.e., you can run Docker images in OpenWhisk.

We can run it locally

In order to use TweetBot in a serverless approach, we need to install OpenWhisk in our machine and have a BlueMix account. The beauty of serverless technology is that you don't have to rewrite your entire application; just tweak the plain code that runs in your machine and you'll be fine! Surprisingly, our TweetBot requires only one change — it should have a main function with an input parameter (dictionary type) and is to be saved as a main.py file.

Here is the modified Python code:

```
# Program to retweet five latest tweets based on a hashtag (#Serverless) from TwitterFollowBot import TwitterBot
def retweet(dict):


#create an instance of the TwitterFollowBot
```

```
# in your current directory
# Program to retweet five latest tweets based on a hashtag (#Serverless) from TwitterFollowBot import TwitterBot
def retweet(dict):

#create an instance of the TwitterFollowBot

# by default, the bot will look for a configuration file called config.txt

# in your current directory
my_bot = TwitterBot()
# autoretweets the 5(count) latest tweets that matches the hashtag
my_bot.auto_rt("#Serverless", count = 5)
def main(dict):
retweet(dict)

return {'message' : 'retweeted successfully'}
```

· Now, save this Python code in a file named main.py. Create the config.txt, already-followed.txt, followers.txt and following.txt (as earlier), and zip them all with the main.py file and the TwitterFollowBot dependency module files.

· Invocation process

Once the wsk CLI (command line interface) is installed and the zip file is ready, follow the steps given below.

· Step 1. Create and update an action: Log in to the IBM Bluemix account (https://console.bluemix.net/openwhisk/) and create a new action. You can upload the zip files with a new action. You can upload the zip files with dependencies only via the CLI. The syntax is : wsk action create <action-name> --kind <language:version> <file_name>

Sample Command:

wsk action create tweetBot --kind python:3 OpenWhisk.zip

· Step 2. Invoke the function (non-blocking mode): The syntax is:wsk action invoke <action-name>

Sample Command: wsk action invoke tweetBot

· Step 3. Check for the result: Since we invoked the function in a non-blocking mode (because we haven't added the '–blocking' parameter), the command returned immediately, but it is executing in the background. The syntax is:wsk activation result <action ID>

Sample Command:

Wsk activation result

f4df0d1dcb12488396978d2cda832b09

Step 4. Check out the logs: The syntax is: wsk activation logs <action ID>

Sample Command:

wsk activation logs f4df0d1dcb12488396978d2cda832b09Automate the invocation

The moment the action was invoked, your Twitter account would have retweeted the five latest tweets that have the hashtag '#Serverless' in it. However, this is still a manual invocation. For maximum impact, it would be better to automate the invocation process as well, so that you can configure the action and forget it once and for all.

· A periodic trigger would be the best option. It triggers the action based on a specific time, and will retweet the latest tweets with '#Serverless' in it. One can either choose a pattern or write a cron expression.

· Words of caution

Before we end this article, here are a couple of things one should be careful about:

OpenWhisk is open source and free, but to deploy it, we use IBM Bluemix which isn't free. The TweetBot action will seamlessly run in the free tier, but for any other application, please estimate the monthly costs.

This action uses the Twitter API in the background via the TwitterFollowBot module.

1. Misusing this may lead to the banning of your Twitter app, so please make sure you clearly read the Twitter automation rules.

Conclusion:

In this article, we discussed a TweetBot that can be written to automatically retweet the latest tweets with certain given hashtags. We wrote the actions (serverless functions) in Python, and deployed them in OpenWhisk on IBM Bluemix. We also used triggers to automatically invoke the actions at

How Biometrics is Changing Market Research

Surbhi Srivastava

Biometrics has traditionally lived in the silos of physiological psychology departments, neuroscience classrooms, and in UX/UI circles.

However, companies like Expedia are realizing the wealth of information that biometrics can produce, and they're pairing this data with website usability tests to deliver troves of information, that, quite literally, have kept the company as a major player in the extremely competitive online travel website business.

Bloomberg did a recent profile of how Expedia is using biometrics in their recent usability lab to learn how people's psyches play into their travel booking patterns. Namely, what excited them ? Planning a vacation is an imaginative experience, replete with the visions of sitting on a beach sipping a Mai Tai, yet a website's configurations, search process, and booking process can quickly stifle these visions of tropical grandeur. Instead of simply clicking to book, people get kicked off of screens and redirected to mind-numbering task pages where they're required to search optimal number, and, ultimately, pre pay for said experienceSo, Expedia is seeking to retain that emotional high that captures people prior to booking a trip and learn how they can maintain it throughout the checkout experience. And they're doing it with biometrics.

Who, back up there. Biometrics? Many of us associate biometrics with our company's health screening day. The biometrics we're talking about here are slightly different.

In market research, here's the gist of how it works Sample is recruited and brought to a focus group facility or market research setting

· The participant is asked to don galvanic skin response sensors on one hand

· They're then asked to surf through a site. They may be sitting next to a researcher, who asks them questions, or they may be self-directed so that the research team can see how they naturally navigate through their experience

· Depending on the technology employed, they will either have face sensors attached or their responses and eye tracking is captured through video

That's it. Pretty painless if you're a participant in the study. A thorough market research company will then interviews the participant and go through a debriefing session to capture the experience in the subject's own words. The final results are added to the data pile, which will later be sorted and analyzed by the firm commissioning the study.

So let's not downplay what a market research firm learns through biometrics

Although the study may seem simple in terms of the steps required, the data that the qualitative research biometrics produce is anything but simple. The research team is given reams of data points that pinpoint electrodermal activity (which is widely used to measure changes in autonomic sympathetic arousal that are integrated with emotional and cognitive states indicating stress responses); facial expression emotion analysis; heat mapping; and eye tracking. Once analyzed, the data points show how people react, on a physiological level, to website content, layout, and specific tasks or experiences that they're asked to do. It's fascinating and gives amazing insight into the emotional landscape that drives what people click on, navigate to, and are pulled in by.Since we're in-person researchers, here at InterQ, our task is to take this technology and overlay it with qualitative research as much as we can. Biometric UX testing produces beautiful spreadsheet data, but our real question is what is the thinking behind those emotions-spelled-out-through-numbers ? How was the person processing the experience during the task ? Do their self-reported insights match up to what we see in physiological markers ? What is the story behind these numbers, and how can that translate into measurably improving the website, content, or user journey ?

Combining these insights is where the real magic happens, and it's a game changer in terms of how it affects outputs in design, be it on a website, app, or software program. Expedia has learned the power of it, and it's helped them stay on top of the game in the online travel website industry.

Information Quality-Backend Testing

Priyanka Rattan

Usually when we perform testing of any application, we mainly look for the frontend, but we never realize how backend operation can actually intercept changes that can bring many issues in the application. With more India's online shopping registering a phenomenal 100 per cent annual growth, many retail chains and consumer durable companies are joining the Web bandwagon to tap the e shopping market. Users don't take a second to reject a site when they find any security issue, user interface issue or any other issue. According to Google, India have more than 120 million Internet users, out of which around half opt for online purchases and the number is growing every year. To win the trust of so many users it becomes very important to deliver a bug free application for this and this involves great testing effort which includes back end testing of e-commerce websites with domain specified testing thoroughly.

Users are mainly concerned with front end of:

- Home Page
  PDP (Product Detail Page)
- PLP (Product Listing Page)
- Stock availability
- Cart
- Checkout
- Payment
- SearchExtra features like
- Coupons/Promotions/Payback points /Wallet
- Cross Sell/ Upsell
- You may also like/ Similar items/Accessories section
- Check for delivery option
- Compare tray
- Wish list /Email a friend/ / Notify the price
- Review

METHODS

But a lot is happening at the backend. Being a tester are we confident enough that we will be able to deliver a reliable product to so many users?

How backend testing can help to achieve a more reliable application?

UI testing (WCMS Cockpit):

WCMS is multi-channel publishing system that allows you to easily maintain websites, both the transactional and non transactional parts of sites. Provides an intuitive, graphical user interface for data presentation and management.

Product Content Management (PCM):

Product Content Management (PCM) , delivers consolidation and centralized management of product information and attributes across all channels.

Management Console (MC):

The Back office area is an administrative tool to help run e-commerce business efficiently. It enhances the capabilities of the Back office UI, providing ready-to-use, reusable components that enable to build custom business tools tailored to specific user needs, simplifying administrative tasks.

Customer Service Cockpit (CS Cockpit):

When customers can't find the answers they need, they can become frustrated and often click away from partially completed forms or abandon their shopping carts. In order to recover these customers, service contact points – including call centers, chat, email, and even Web-enabled customer self-service – need to be able to deliver the appropriate information and resolutions quickly.

Automation Testing

Once the application is stable we can perform automation testing to save time for regression testing when enhancements are done. For automation testing scripts are generated using tools like selenium which is an open source tool or any paid tool like QTP. Scripts can be generated for

1) Checkout Flow
2) Integration with 3rd party
3) Backend Functionality of the system

CONCLUSION

If testing is done properly including the backend and automation testing can affect the usability which in turn will affect the no of users using the application and profit margin will definitely go up. What's most important when testing e-commerce websites is to make sure that each feature has correctly implemented its requirements not just look and feel but logically as well.