JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

PROJECT TITLE: MITIGATING UNCONTROLLED SOCIAL MEDIA UTILITY

PRESENTED BY:

COLLINS O. BUNDE I132/0858/2013

EDWARD ONYANGO I132/3025/2013

A PROJECT PROPOSAL SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

2016©

SUPERVISOR

DR. SAMUEL LIYALA

ABSTRACT

A technology that started with a focus on the consumer, social media offers critical business advantages to enterprises, it is being leveraged as a powerful tool driving business objectives such as improved customer relations, better brand recognition and enhanced employee recruitment. While it affords companies many potential benefits it presents inherent security risks to these industries as well. Enterprises willing to incorporate social media into their business process must adopt an all-inclusive social media strategy that encompasses effective social media policies. Furthermore, enterprises should consider establishing local enterprise intelligent systems that focus on social media monitoring, for real-time social media monitoring and analysis of employee and customer sentiments. The study attempts to identify the existing risks in social media, and suggest a mitigation strategy for effective social media use that defines social media policy formulation guideline for use within the Kenyan industrial realm, Furthermore, the study proposes a contextualized methodology for brand reputation tracking for the enterprises that can be replicated locally among the Kenyan companies. Finally, the study suggests the implementation of such system for enhancing privacy and security in social media by the Kenyan enterprises. The system methodology used for this project is the agile, scrum methodology. Exploratory research design is used for the research, with regards to risks and privacy issues in social media in Kenya. This project is significant since it will help in addressing the social media risks and provide well-defined mitigation strategies against privacy and security concerns through enforcement of policies. In addition real-time monitoring through sentiment analysis will provide rich insightful intelligence that will help in profiling users both insider and outsiders by arresting bad posts before they create an uproar in the social media.

Table of Contents

1

Keywords/Abbreviations vi

Chapter 1 ..... **Error! Bookmark not defined.**

1.0 Introduction ..... **Error! Bookmark not defined.**

1.1 Background information ..... **Error! Bookmark not defined.**

1.1.0 Kenyan vision 2030 ICT policy objectives ..... **Error! Bookmark not defined.**

1.2 Statement of the problem ..... **Error! Bookmark not defined.**

1.3 Objectives ..... **Error! Bookmark not defined.**

1.3.1 Main Objective ..... **Error! Bookmark not defined.**

1.3.2 Specific Objectives ..... **Error! Bookmark not defined.**

1.4 Research questions ..... **Error! Bookmark not defined.**

1.5 Scope of the study ..... **Error! Bookmark not defined.**

1.6 Assumptions of the project ..... **Error! Bookmark not defined.**

1.7 Significance of the study ..... **Error! Bookmark not defined.**

1.8 Limitations of the study ..... **Error! Bookmark not defined.**

Chapter 2 ..... **Error! Bookmark not defined.**

2.0 Literature Review ..... **Error! Bookmark not defined.**

Social Media Monitory ..... **Error! Bookmark not defined.**

2.1.1 Social Media ..... **Error! Bookmark not defined.**

2.1.2 Social Media Monitoring ..... **Error! Bookmark not defined.**

2.1.3 Social Media Strategy ..... **Error! Bookmark not defined.**

2.1.4 Risk, Privacy Concerns, and Security Issues ..... **Error! Bookmark not defined.**

2.1 System Overview ..... **Error! Bookmark not defined.**

Chapter 3 ..... **Error! Bookmark not defined.**

3.0 Methodology ..... **Error! Bookmark not defined.**

3.1 System Methodology ..... **Error! Bookmark not defined.**

3.1.1 Overview ..... **Error! Bookmark not defined.**

3.2 Scrum Artifacts ..... **Error! Bookmark not defined.**

3.2.1 The Product Backlog. ..... **Error! Bookmark not defined.**

3.2.3 The Sprint Burn down Chart ..... **Error! Bookmark not defined.**

3.2.4 Impediment list. ..... **Error! Bookmark not defined.**

3.4 The Sprint Planning Meeting. ..... **Error! Bookmark not defined.**

3.5 The Daily Activities. ..... **Error! Bookmark not defined.**

3.6 Sprint Review Meeting ..... **Error! Bookmark not defined.**

3.6. Sprint Retrospect Meeting ..... **Error! Bookmark not defined.**

3.7 Project Startup ..... **Error! Bookmark not defined.**

Chapter 4. ..... **Error! Bookmark not defined.**

4.1 Research Findings ..... **Error! Bookmark not defined.**

4.1.1 The existing risks of social media utility across Kenyan enterprises..... **Error! Bookmark not defined.**

4.1.1.1 Cyber loafing ..... **Error! Bookmark not defined.**

4.1.1.2 Data leakage ..... **Error! Bookmark not defined.**

4.1.1.3 Social media squatting ..... **Error! Bookmark not defined.**

4.1.1.3 Phishing ..... **Error! Bookmark not defined.**

4.1.1.5 Cyber bullying ..... **Error! Bookmark not defined.**

4.1.2 Mitigations strategy ..... **Error! Bookmark not defined.**

4.1.3 Suggested Policy Formulation guideline for Social Networking Sites.... **Error! Bookmark not defined.**

4.2 System/Software Development ..... **Error! Bookmark not defined.**

4.2.1 Project Planning ..... **Error! Bookmark not defined.**

4.2.2 Architecture/High-Level Design ..... **Error! Bookmark not defined.**

4.2.2.1. Preconditions ..... **Error! Bookmark not defined.**

4.2.2.2 Design limitations ..... **Error! Bookmark not defined.**

Why machine learning? ..... **Error! Bookmark not defined.**

4.3.1 Design and Development ..... **Error! Bookmark not defined.**

4.3.1.1 System Requirements ..... **Error! Bookmark not defined.**

4.3.1.2 System Use Cases ..... **Error! Bookmark not defined.**

4.3.1.3 System Architecture ..... **Error! Bookmark not defined.**

4.4.1 Implementation ..... **Error! Bookmark not defined.**

4.4.5 Testing and validation ..... **Error! Bookmark not defined.**

Chapter 5 ..... **Error! Bookmark not defined.**

5.0 Discussion and Conclusion ..... **Error! Bookmark not defined.**

References..... **Error! Bookmark not defined.**

Appendixes..... **Error! Bookmark not defined.**

NLTK Installation and Setup ..... **Error! Bookmark not defined.**

Twitter OAuth 1.0a Flow with Ipython Notebook..... **Error! Bookmark not defined.**

Anaconda installation..... **Error! Bookmark not defined.**

Tweepy Installation ..... **Error! Bookmark not defined.**

Abbreviations

Abbreviations

N-Gram - an n-gram is a sequence of n words used in text or speech. When doing natural-language analysis, on the twitter sentiments it breaks up a piece of text by looking for commonly used n-grams or recurring sets of words that are often used together.

C.I.A confidentiality Integrity Accountability

E.S.N.Ts Enterprise Social Media Networking Tools.

A.P.I Application Programming Interface

REST Representation State Transfer

NLP Natural Language Processing

NLTK Natural Language Toolkit

USMU Uncensored Social Media Monitory

UML Unified Modelling Language

W.B.S Work Break Down Structure

S.Q.C.T Scope Quality Cost and Time

Chapter 1

1.0 Introduction

Web 2.0 and social media has widened opportunities for communication and networking, the information flows on the internet can be accessed through the use of open source intelligence tools, by crawling them and analyzing them for various reasons such as behavior prediction and opinion mining The introductory part of this chapter talks about social media use in within the Kenyan enterprises. Kenya like many other countries, has embraced the ideals of social businesses. Where social media technologies are being exploited successfully by the corporates to sell their brand identity, increase sales of product and services as well as augment customer satisfaction. Further on it goes to give an overview of the problems that arise from the use of these enterprise social media networking tools (E.S.N.Ts). Risks of these social media tools to the enterprises is the problem statement. Consequently it underlines the study objectives and its significance stating that the project will be significant in emancipating the enterprises on the need for establishing effective social media strategy which includes policies, risk assessment guidelines before the uptake of any of these social media tools and implementing local enterprise intelligent systems that can monitor in real time social media use within these enterprises. It is a study of how enterprises can effectively mitigate against the risk of social media use within the enterprise environment. The scope is limited to Kenya with a focus on the formulation of a social media strategy and the implementation of local enterprise intelligent systems as measures that will eventually help in mitigating this risks. Furthermore the assumptions of the study are indicated and the research questions formulated.

1.1 **Background information**

Social media offers business advantages to both private enterprises and government agencies. Organizations use this social media to reach out to the digital audience efficiently and cost effectively. Social media tools are thus being embraced in the business world as important game-changing customer communication platforms. They necessitate networking with current and potential customer besides offering aid in promoting brand awareness in many different markets.

Furthermore, it has revolutionized the way people engage with the internet, opening a world of constant ‘anywhere, anytime’ access thanks to the plenty and popularity of smartphone devices such as Android, Blackberry and iPhones (A Cyveillance White Paper, 2015).

In a 2009 survey of companies that participate in online social media communities, 70 percent of respondents reported using social media of some kind in their businesses (Gordon, n.d.). Over 40 percent of such companies had employees whose job function included spending time on social media sites in order to maintain an organizational presence. More than a quarter of these companies maintained social media sites for employees’ personal announcements and social events. Fewer than ten percent blocked access to social media for any employees.

In Kenya, the more affordable tablet computers and the rise of smartphones in the country, not to mention, the competitively priced mobile data, converge to bring us to the age of the smart

audience (Kaigwa, Mark; Madung, Odanga; Samer, Costello;, 2015). Kenya, like in many other countries, enterprises are embracing the ideals of social media businesses. Social media technologies have been exploited successfully by the corporates to sell their brand identity, increase sales of product and services as well as augment customer satisfaction. This has already resulted into a dichotomy between the enterprises that have embraced this technology and those that are yet to, or mostly avoid it.

The bottom line is with all these roles and responsibilities; every enterprise needs an elaborate risk management plan that addresses the inherent risks. The starting point is always supposed to be a social media risk assessment, which should help institutions ascertain the key intrinsic risks that, exists and identify the appropriate mitigation strategies. Dr. Michael Ong once said, "Good Risk Management fosters vigilance in times of calm and instills discipline in times of crisis." (Macharia Kihuro, 2015).

Practical case studies in the Kenyan context of how social media has affected enterprises or employees. Chase Bank being put under receivership after the online uproar that tore the company to its core, arguably Chase Bank was brought down by social media. The case of a famous Disc Jockey, Delacreme being a victim of cyberbullying when explicit videos were posted on twitter and attracted nationwide tweets and retweets ultimately almost jeopardizing his career this and many untold stories are the impact of unmonitored social media.

1.1.0 Kenyan vision 2030 ICT policy objectives

Our project considers the Kenyan ICT objectives as the driving force, that is by harmonizing our goals with the I.C.T policy objectives we can as well be playing a part in the in the realization of the vision 2030 goals. The I.C.T policy objectives:

1. Points to establishing a cyber security strategy as a key objective of national security. In this regard, effective social media policy should be inculcated into the cyber security strategy for the achievement the vision 2030 goals.
2. Encourages the development of cyber security strategy with the aim of driving economic and social prosperity while at the same time protecting cyberspace reliant societies against cyber threats. Enterprises will ultimately promote economic growth by implementing appropriate mitigation strategies against social media risks.
3. An analysis of the security impacts of social media, for instance, cyberbullying would provide a regulatory framework and insight into technical solutions and law enforcement strategies and this would be appropriate for the detection and prevention of cyber threats across the country according to the Kenyan ICT policy strategy.

1.2 **Statement of the problem**

Social media offers benefits to industries, but in the same respect it poses severe security risks for enterprises. Without a proper social media strategy, enterprises fail to realize these benefits. Corporates are faced with a big challenge due the inherent risks they face with the rapid uptake of social media.

Employees and consumers alike can use the social media to cause, brand and reputation damage as well as other security risks to the enterprise. Employees pose an insider threat, and are perceived to be the weakest link in the security chain. They present these corporates with an uphill task, in protecting sensitive and confidential information, and devising measures to debar sharing of such information. Social media monitoring of company brand mentions in these social networks provides a real time opportunity to apply proactive measures to mitigate this risks as and when they occur. Hence companies should consider implementing such intelligent systems not only for market share gain but also to aid in enhancing security and preventing privacy violations. A security model that includes a social media strategy, policy formulation coupled up with local enterprise intelligent systems can help them mitigate such risks.

1.3 **Objectives**

1.3.1 Main Objective

To identify the existing risks of social media utility across Kenyan enterprises.

1.3.2 Specific Objectives

1. To suggest mitigation strategy for effective social media use that defines, policy formulation guideline for the enterprise use within the Kenyan industrial realm.
2. Propose a contextualized methodology for brand reputation tracking within the enterprise that can be replicated locally among the Kenyan companies.
3. Suggest the implementation of such intelligent systems for enhancing privacy and security in social media

This project will monitor twitter content generated by Kenyans online, the content that will be monitored includes tweets, comments, and mentions. This will be exclusively done by monitoring English words since our classifier will only be trained on the English words. We did not focus on spoken vernacular languages such as Swahili and Sheng'.

From the twitter platform, we will be able to classify user comments as either positive or negative and append a polarity or confidence score which determines how negative a particular sentiment is. The findings, as well as the methodology used, are discussed in the later chapters.

1.4 **Research questions**

What risks are most Kenyan enterprises exposed to as result of uncontrolled social media use?

How will local enterprise intelligent system such as sentiment analysis systems, help these enterprises in mitigating the risks arising from the social media use.

What are the mitigation strategies implemented for social media surveillance to help in dealing with suspicious user activities on a timely basis, like flagging off negative comments/statements, or issues of negative brand images to these enterprises? Before they get out of hand?

1.5 **Scope of the study**

The project will be executed as a study of the enterprises within Kenya, taking a case study of Safaricom, the study will focus on the existing social media risks to these enterprises and the resultant impact to the enterprise environment. In addition, we look at social media strategy as being of importance to companies that have embraced social media and the need for formulation of effective social media policies. Finally, we implement a sentiment analysis system to monitor, employee and consumer comments towards corporates and their brands. The methodology used will be the scrum methodology for the implementation phase where we use sentiment analysis techniques by leveraging the use of the Twitter platform as the social media case study for the project. The research design will be exploratory research since it relies on secondary research such as reviewing available literature in addition to the use of the internet.

1.6 **Assumptions of the project**

Most Kenyan enterprises are using twitter social media platform since we are going to do sentiment analysis leveraging the twitter API. This methodology is applied on only one social media site with the assumption that it might highlight its applicability and the success rate of the same technique to other social sites.

Most of the Kenyan enterprises are using social media as part of the social business objective to promote their brands and to increase their customer base.

Most of the Kenyan enterprises have not implemented any local cyber intelligence techniques of monitoring the social media, for instance, sentiment analysis and opinion mining.

1.7 **Significance of the study**

This project is necessary because it will help enterprises in reducing risks that arise from data leakages, cyberbullying, and social media squatting and social engineering effects of social media and maintain their privacy against the malicious online users. In addition, these institutions will be able to account for the existing employee productivity hours by putting up measures to control cyberloafing during work hours.

The project will also emancipate the enterprises on the need for establishing effective social media strategy which includes policies, risk assessment guidelines before the uptake of any of these social media tools and implementing local enterprise intelligent systems that can monitor in real time social media use within these enterprises.

1.8 **Limitations of the study**

The system is limited to the twitter platform currently thus doesn’t cover other social media sites.

Most employees may not be willing to give up their privacy to participate as they have a freedom of expression and privacy on the web.

Chapter 2

2.0 Literature Review

2.1 Social Media Monitory

2.1.1 Social Media

Isaca, (2016) describes social media as a technology that involves the creation and dissemination of content through social networks using the Internet. According to, Chi, (2016), it is a channel of communication based on mobile technology and the internet where people can share content with each other. A Cyveillance White Paper, (2015) regards it as a phenomenon so unprecedented, opening new worlds of opportunities for industries globally and that while the potential and rewards, this notwithstanding it also presents numerous challenges and risks. Organizations are faced with a hard time establishing and enforcing effective social media strategies. Some organizations afraid of the dangers of exposure, prohibit social media use. On the other hand, companies not wishing to be left behind, have leveraged E.S.N.Ts without developing effective social media use policies or conducting a risk assessment. Nonetheless, no alternative fully satisfies this ideal since companies that do not embrace E.S.N.Ts will not realize the benefits and will be disadvantaged to their opponents that have embraced them.

In 2009, the U.S. military considered a near-total ban on social media sites throughout the Department of Defense. Military officials cited inherent technical security weaknesses and lack of security safeguards on social media sites (Schachtman, 2009).

2.1.2 Social Media Monitoring

Social media monitoring tools are designed to gather facts about consumer actions, purchase, and attitudes without having to survey customers. Companies can gather information about customer preferences by observing how they talk about companies on platforms such as Facebook and Twitter. Social media monitoring give's companies much more insight into how their products fare in the marketplace and how to be successful with customers and prospects. In the same respect, we can leverage the use of these monitoring tools to monitor employees and customer behavior of narcissism and malevolence and be able to arrest comments that may result into reputation damage to the companies. Most industries and companies are more focused on the market share rather than also taking proactive measures to mitigate security risk. The concept of thought is that having the

right security processes will help a company realize benefits in the long term and as a result can save the company from financial losses and reputational damage.

A report by Price Water Coopers in 2013 on how organizations detected their most significant breach (pwc, 2013) consisted of the following. Routine internal security monitoring detected 42% of the worst breaches, while 30% were obvious from the business impact (e.g. system outage, assets lost). 9% of organizations worst security incidents were discovered by accident up to 6% in 2012. This really justifies the need for continuous monitoring as a factor key in mitigating the risks.

Users often appear to be unaware of the fact that their data are being processed for various reasons, such as consumer behavior analysis, personalized advertisement, opinion mining or profiling that's according to Gritzalis, Kandias Stavrou & Mitrou. In order to raise awareness, researchers have conducted attacks on realistic environments, consisting of Social Media communities or groups. (Gritzalis; Kandias; Stavrou; Mitrou; 2012). For this reasons social media monitoring will play a key role in enhancing social media security. They also suggest that, the rise of social media usage has influenced researchers towards opinion mining and sentiment analysis, which constitute computational techniques in social computing. As presented by King etal, social computing is a computing paradigm that involves multi-disciplinary approach in analyzing and modelling social behavior on different media and platforms to produce intelligence and interactive platform results

2.1.3 Social Media Strategy

Social media strategy is fundamental for every company to realize the benefits of social media. Cyveillance White Paper, (2015) indicates that with the growth of social media it is increasingly being part of the daily life for millions of people, enterprises should thus be accountable in developing proactive social media strategies that will protect all facets of the business while taking advantage opportunities present while engaging with customers. Effective social media presence boiled down to its very core, is made up of four parts: A strategy, Monitoring and refining, Active social presence and passive social presence (Gray, n.d.). It is important to have a plan, so that an enterprise can know how they are going to measure the success of these tools, besides putting into consideration what happens when something goes wrong. Hence there is every reason for every Kenyan enterprise to have an objective in mind when taking up these social media tools (Gray, n.d.).

According to Michael Cross the author of the book Social media security. The fundamental objective for developing a security strategy for this social networks is for people to do their duties without compromising security. The following should be considered when creating a social media security strategy: How will security be achieved, who will be held responsible. It also encompasses areas related to use of social media, including the network security details, corporate workstations, firewall restrictions and mobile devices issued to employees, (Cross, n.d.).

2.1.4 Risk, Privacy Concerns, and Security Issues

Not wishing to be left behind, many enterprises are seeking to leverage social media tools. Since the tools are new to many enterprises and do not require new infrastructure, social media technologies may be introduced to the enterprise by business and marketing teams without IT involvement, a project plan or risk assessment (Isaca, 2015). It is, therefore, important that the enterprise creates a proper plan to address the risks that accompany the technology.

According to Cross, (n.d.), the trade-off of security exists on such things as technology, equipment, network access and content, and the many threats on the Internet, there are tactics, and tools for protection of systems. Cisco 2013 Annual Security Report, states that mass audience sites, such as social media have high concentration of online security threats. Social media not only gives opportunity to transmit sensitive information for business but also facilitates spreading of false information, which is just as damaging.

2.1.4.1 Insufficient Authentication Controls

Most social media applications, allow confidential information to be spread in many different locations. Hence even novice users can introduce flaws that can badly affect the entire system. Administrative accounts with no security controls, such as adequately strong passwords, ca be brute-forced by attackers to determine passwords for a given account, which can be replicated to other accounts with single-sign-on arrangement. The attacker can eventually have administrative access to a number of systems.

2.1.4.2 Cyber loafing

According to pwc. (2013) most staff-related incidents normally involve staff misuse of the Internet or email. This happens in more than three-quarters of large organizations and around two-fifths of small businesses. Cyber loafing is the wastage of time in unnecessary web browsing and social media sites.

2.1.4.4 Social media squatting

Cyber-squatting is becoming more common each and every day in Kenya. Both celebrities and Government officials alike are being targeted by cyber squatters. Enterprises are also not left behind in this, we got people who masquerade as genuine company accounts on Facebook, Twitter, and LinkedIn. Business owners should therefore register their domain name immediately they start operations to avoid cyber squatters from registering the name under their details as they wait for the business owner to approach them so they can demand payments (Cybersquatters-hit-e-commerce, 2016).

2.1.4.5 Phishing

Though phishing is not exclusive to social media, there has been a current spike in phishing attacks linked with social media sites (Fisher, 2011). Many people view social media sites on cell phones or other mobile devices. Which makes it harder to distinguish actual and bogus web sites. Additionally, social media enables attackers to send phishing messages that appear to come from someone that the victim knows. Having obtained login information for a few accounts, scammers

will then send out messages to everyone connected to the compromised accounts, often with an enticing subject line that suggests familiarity with the victims (Baker, 2009)

2.1.4.6 Information Leakage

Currently there is no distinction between work personal lives due since the dawn of "always on connectivity". Younger workers use the same technologies in the office as at home. Furthermore, social sites like Twitter and Facebook create the misconception of acquaintance and affection on the Internet, people may for this reason be inclined to share information that their employer would have wished to keep reserved. Even though people may not be divulging trade secrets, but the collective effect of small, details can help a business's opponents gain valuable insights about that company's current situation and future plans.

2.1 **System Overview**

At the beginning of the project, it was suitable to provide a methodology that fitted well to the enterprise. A review of the available literature on online social media monitoring and opinion mining was therefore used to better understand the methodologies used in preceding projects as regards the sentiment analysis for social media monitoring.

Umati project incubated from a popular innovation hub in Kenya called I-hub, developed a system for election monitoring, for the identification and detection of hate speech. The methodology that was thought ideal for Umati was one that considered the dynamic and unique characteristics of the Kenyan online space, e.g. the multiple languages spoken online, the need for local monitors who understood not only the vernacular languages but the ethnically divided politics in Kenya, the lack of a workable definition of hate speech that suited the Kenyan context and budgetary limitations. The Umati project having provided a way to collect and study hate speech incidents from the Kenyan cyberspace, is however only limited to the election periods which renders it inactive for a longer period before another election. On the contrary our project focuses on the local enterprises all year round whereas the Umati project was a nationwide project for the entire country at election periods, the other difference is that we are analyzing brand hate messages while the Umati project focused on hate speech.

The Panopticon project done by, Gritzalis, Kandias, Stavrou & Mitrou, (2014), analyzed how a complex information shared on social media can be used in order to achieve a dual purpose of: (a) Dealing with the insider threat prediction and prevention, as malevolent insiders and predisposition towards computer crime being closely related to the personality trait of narcissism. They proposed a method of outlier detection in social media via influence, usage intensity, and Klout scores evaluation in order to detect users with narcissistic behaviors. Gritzalis, Kandias, Stavrou & Mitrou, (2014). Also proposed a method for group analysis under the prism of group homogeneity, being an important characteristic to prevent the manifestation of insider threats. The Panopticon project was the most suitable to replicate to the Kenyan enterprise by analyzing insider and outsider threat of conceit. Though they focused only on the insider threats our project

also focusses on the outsider threat as well and how the self-righteous activities of both employees and customers might affect the enterprise leading to such factors as flash mobs, boycotts, and reputation damage (Gritzalis, Kandias, Stavrou, & Mitrou, 2014).

Ijarie project done in Germany used both sentiment analysis and image analysis to help determine and detect cyberbullying in the cyberspace. They defined cyberbullying as an attack that depends on frightening, intentionally insulting, awkward or annoying people via mobile phones or on the internet over social networking websites, instant messaging and emails application (Anuja,Shubham, Nalini,Arun. n.d.). The image analysis involved the extraction of meaningful data from images by means of digital image processing techniques, this entailed procedures such as reading bar coded tags by implementing the skin color detection algorithm to detect images. Text analysis, on the other hand, was characterized by using preprocessing techniques such as stop word removal and stemming. Bag of words model being the primary stage in Natural Language Processing was mainly used in sentiment analysis.

According to Wright, (2016), researchers from the University of Cardiff have been awarded more than $800,000 by the US Department of Justice to develop a pre-crime detection system that uses social media. The system relies on drawing on big data from social media to identify on potential crimes before they happen. The project builds on existing work conducted by Professor Matthew Williams, Director of the Social Data Science Lab at the Data Innovation Research Institute and Professor of Criminology at Cardiff University and Dr. Peter Burnap, senior lecturer in Computer Science & Informatics, to look for signatures of crime and disorder in open source communications, not crimes themselves (Wright, 2016).

The new project is meant to collect Twitter posts containing terms that already have been labeled as hate speech by human annotators over a period of 12 months (Wright, 2016). These two measures will then be entered into statistical models to identify if there is a correlation, that is, whether an increase in hate speech in a given area is also statistically linked to an increase in recorded hate crimes on the streets. The project is meant to use the same similar machine learning techniques to build new hate speech algorithms based on the US data (Wright, 2016).. If the project succeeds, then social media data may be used in conjunction with conventional data sources to improve predictions of hate crimes offline. These new forms of data are also attractive as they can provide new information on changing risks in near real time, unlike conventional data that is often weeks or months out of dates as indicated by Wright, (2016) .

Brand Name tracking

Istats a company in Kenya that does social media monitoring solution that tracks activities of Kenyan brands on twitter. Jack. (2015) gives a report about a measure of brand conversation with the aim of outlining the most talked about brands on twitter and by extension the most visible brands. They gave a report on data based on 1.13M tweets spanning across 95 brands. With

categories including Media, Energy, FMCG's, Motoring, Insurance, Retail, Service, and Telcos. The data was compiled to give a comparative report on how brands are performing on twitter in terms of conversation – driven by the popularity of twitter locally. The metrics used in the project were: Number of posts mentioning a brand, number of unique people mentioning a brand and the average following of the sum of users mentioning the brand to estimate reach (Jack, 2015).

Jack, (2015), reports that they analyzed brands with the most positive sentiments. In their report Durex achieved the highest score in the positive sentiments, the sentiment score checked for key words and phrases that depict the tone of a post. The post is then scored between 0.0 and 1.0 where 1 is fully positive and 0 is negative. However, the tone was contextualized since they sometimes are not directed on the brand.

The limitations of these is that for a business to thrive the social business strategy is key to promoting their brands and reaching out to potential customers, but with the rising cyber-crime cases, where malicious persons are now leveraging these social media tools to cause exposure to enterprises, we can still use social media monitoring towards analyzing and modelling social behavior that may be able to provide cyber threat intelligence enabling organizations to protect their information infrastructure and employees from physical and online threats found within and outside the network perimeter.

After the review of the literature in the fore mentioned areas, we did propose a system design framework below for the implementation of the project: The system can be accessed from either a laptop or a desktop computer, then leveraging the use of the twitter API, with python code we can access tweets in real-time. Once we access the tweets we do sentiment analysis on the stream of tweets by tracking a given brand name In this case we considered a Safaricom as the case study of the project. Safaricom being a brand with large following, due to its position the market and the large customer base, it attracts a number of mentions on a daily basis. Once we analyze the tweets, each tweet is thus classified as being either positive or negative and assigned a polarity score. In making our system more intelligent, we have a watchdog application that monitors for tweets with a higher polarity score more than 0.8. These tweets are then sent via email to the individual responsible for social media monitory in a company or any relevant personnel with that duty, these tweets can then be analyzed to determine which ones are more sensitive to the company, and which ones would result into damage of company or brand reputation. After which a decision can be made whether to arrest or flag the post before it creates an uproar in the social media. Alternatively, a decision can be made to send cease and desist letter to the individuals. This data is also useful in profiling this users through opinion mining.

The system implementation thus has the goal of providing the company with information they need to address quickly and protect their businesses and reputation. This is because most industries and companies are more focused on the market share rather than, also taking proactive measures to mitigate security risks. The concept of thought is that having the right security processes will help a company realize benefits in the long term and as a result can save them from financial losses and reputational damage.

Figure1: Proposed system Architecture, Adapted from (Anuja,Shubham, Nalini, Arun)

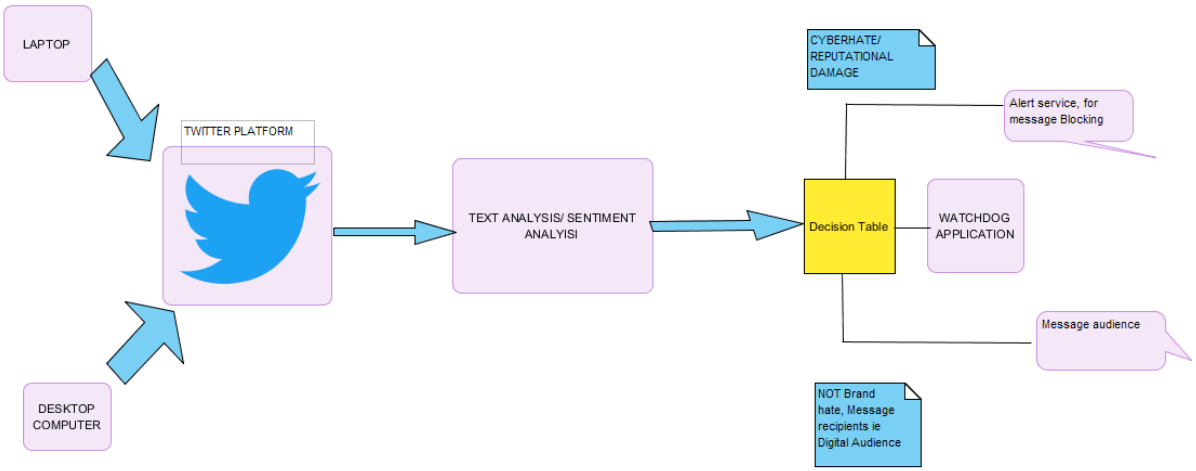

Figure 1proposed System Architecture