Identifying Fake and Clone Accounts in Twitter

Dr. Subbarao Kolavennu, Mr. G. Rakesh Reddy, K. Rithika Reddy, K. Sirija, R. Rahul
[1]*Professor and Head of Department, Department of Cyber Security (CSC) Sphoorthy Engineering College, Hyderabad, India*
[2]*Assistant Professor, Department of Cyber Security (CSC) Sphoorthy Engineering College, Hyderabad, India*
[3,4,5]*Department of Cyber Security (CSC) Sphoorthy Engineering College, Hyderabad, India*

Abstract- An online social network, or OSN, is a hub for social interaction among users who share similar interests or real-world connections. With OSN's growing popularity, security and privacy concerns are also growing in this regard. Users of social networks are facing serious security issues due to cloned and fake profiles. One major risk is user profile cloning, in which pre-existing user information is taken to make duplicate profiles, which are subsequently used maliciously to damage the identity of the original profile owner. They have the ability to initiate threats such as spamming, phishing, and stalking. A fake profile is a social media account created in the name of a person or company that does not actually exist with the intention of carrying out malicious activity. In this paper, a detection methodology has been proposed that can detect fake and duplicate profiles on Twitter. The detection of fake profiles is made using a set of rules for genuine and false profiles. Profile cloning can be detected by two methods: similarity measures and C4.5 decision tree algorithms. Similarity measures involve two types: network relationships and attribute similarities. C4.5 identifies clones by constructing a decision tree with information gained into consideration. To see how well these two approaches enhance the identification of clone profiles, a comparison is done.

INTRODUCTION

Billions of individuals worldwide use online social networks (OSN) to create connections with one another. Examples of these networks include Facebook, Twitter, LinkedIn, Instagram, and others. A new era of networking has been brought in by social networks' accessibility and ease of use. On the network, online social networks (OSN) users exchange a great deal of information, including pictures, videos, phone numbers, email addresses, home addresses, family members, bank account information, profession information, and more. If attackers obtain this knowledge, the consequences might be severe. The majority of OSN users are easily targeted by these assaults since they are unaware of the security risks present in social networks. If children are the victims, the hazards are higher. In a profile cloning attack, a duplicate profile is created by stealing information from current users' profiles. These profiles are then misused to destroy the genuine identity of the original creators of the profiles.

PROJECT AIM AND OBJECTIVE

The aim of this project is to develop an efficient and robust system that can detect fake and clone accounts on Twitter using classification and distance measure algorithms clone profiles, a comparison is done, thereby enhancing the platform's integrity and security.

The objectives of this project are to:

- Create a dataset which contains both fake and genuine Twitter accounts.
- To distinguish between real and fake accounts, extract relevant information from the data.
- Select the proper distance measure and classification algorithms.
- To detect clone and fake Twitter accounts in real time, train the chosen algorithms and implement the model.

PROPOSED SYSTEM

The rising number of cloned and fake profiles has become a significant social threat. Because contact details such as phone numbers, email addresses, names of schools or colleges, corporate names, locations, and other details are freely accessible on social media platforms, hackers can use this information to establish fake or cloned profiles. Accordingly, they attempt to launch several attacks, such as spamming, phishing, cyberbullying, etc. They even make an effort to damage the company or its legitimate owner. Therefore, a detection technique that can distinguish between cloned and fake profiles has been proposed in an attempt to increase user security in their social lives.

ADVANTAGES

- High Accuracy
- Precision
- Recall

SCOPE OF THE STUDY

In order to improve the integrity and safety of Twitter, this study aims to distance measure algorithms in recognising fake and clone accounts. A comprehensive examination of several algorithmic strategies, such as Support Vector Machines (SVM), Random Forest, k-Nearest Neighbours (k-NN), and clustering methods, is included in the scope. The study will extract relevant features and behavioural patterns from Twitter data to differentiate between genuine and fake accounts through meticulous data collection and feature engineering.

Furthermore, to ensure robustness and flexibility, the study will additionally evaluate the performance of these algorithms using measures like accuracy, precision, recall, and F1-score, considering a wide variety of datasets and scenarios. Additionally, the implementation of these algorithms in real-world applications will be examined with a priority on their interpretability, scalability, and efficiency. With an in-depth analysis of these factors, the study aims to provide significant insights and approaches for identifying and reducing the impact of cloned and false accounts on Twitter, ultimately promoting a more secure and reliable online environment for users.

SYSTEM STUDY FEASIBILITY STUDY

During this phase, the project's viability is assessed, and a business proposal with a very basic project plan and some cost estimates is presented. It is necessary to do a feasibility study of the suggested system during system analysis. This will guarantee that the company won't be burdened by the suggested system. Comprehending the primary system requirements is crucial for conducting a feasibility analysis.

Three key considerations involved in thefeasibility analysis are

- Economical feasibility
- Technical feasibility
- Social feasibility

ECONOMICAL FEASIBILITY

The purpose of this study is to evaluate the systems potential financial impact on the company. The company has a finite amount of money to dedicate to the systems research and development. The costs have to make sense. As a result the system was developed within the allocated budget which was made possible by the fact that the majority of the technologies were freely accessible. It was only necessary to buy the personalized items.

TECHNICAL FEASIBILITY

This study is being conducted in order to verify the technical needs of the system, or its technical feasibility. The development of any system must not place an excessive burden on the technical resources at hand. High demands on the available technical resources will result from this. High expectations will consequently be placed on the client. Since only little or non-existent adjustments are needed to deploy the established system, it must have modest requirements.

SOCIAL FEASIBILIT

Examining how much the user accepts the system is one of the study's objectives. Training the user to operate the system effectively is part of this procedure. The system must not make the user feel threatened; rather, they must acknowledge its necessity. The degree of user acceptance is entirely dependent upon the techniques used to familiarise and educate the user about the system. As the system's last user, he has to gain more confidence in order to offer some helpful critique, which is greatly appreciated.

LITERATURE SURVEY

These days, Fake and Clone profiles have become a very significant threat in social networks. So, a detection method is very much necessary to track these frauds who use people’s faith to gather private information and create duplicate profiles. Many authors have worked in this area and have proposed methods to identify these types of profiles in social networks. Some of these methods are discussed below.

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P Markatos [2] have proposed a prototype to check whether the users have become victim to cloning attack or not. Data is taken from the user profile and used to search OSN for profiles that match the information in the user profile and a similarity score is calculated based on commonality of attribute values. If the similarity score is above the threshold value then the specific profile is known as clone.

In their study [3], Brodka, Mateusz Sobas, and Henric Johnson presented two innovative techniques for identifying cloned profiles. The original and cloned profiles' attribute values are compared in the first technique, and network relationships are the basis for the second. A victim will be selected from among those who disbelieve that his profile has been cloned. Next, using query search, a search is conducted for profiles that share the victim's name, treating name as the primary key. After comparing the victim profile (Pv) and the potential clone (Pc), a similarity score (S) is determined. A clone profile is suspected if S(Pc, Pv) > Threshold. The user completes the verification process by hand because he is aware of which profile is a duplicate and which is his original.

In their work, Cresci S, Di Pietro R, Petrocchi M, Spognardi A, and Tesconi M [4] evaluated some of the most pertinent aspects currently in use and guidelines (advocated by the media and academia) for identifying bogus Twitter accounts. A collection of machine learning classifiers has been trained using these guidelines and characteristics.

Subsequently, they developed the Class A classifier, which successfully distinguishes between authentic and fraudulent accounts. Twitter fake account detection has been made easier with the use of a categorization algorithm proposed by Ahmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, and Hesham Hefny [5]. In the initial step, they gathered a few useful features for the identification process from various studies and filtered and weighted them. To determine the minimal set of characteristics that yield correct findings, numerous experiments are carried out. Only seven of the 22 features were found to be useful in identifying fake accounts, and these factors were then included in classification algorithms. The most accurate classification methodology is chosen after a comparison of the methods based on the results.

FUNDAMENTALS

Within machine learning and statistics the classification method is a supervised learning approach in which a computer program learns from input and then applies this knowledge to characterize new observations. A few classification strategies for Identifying fake and clone accounts in Twitter are listed below.

SUPPORT VECTOR MACHINE

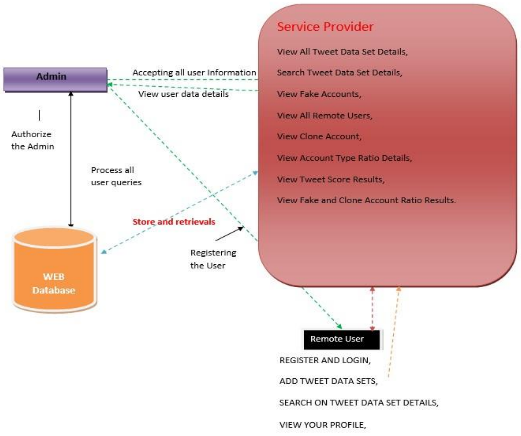
A potent supervised learning algorithm for regression and classification problems is called Support Vector Machine (SVM). SVM seeks to maximize the margin between classes by identifying the ideal hyperplane that best divides instances of various classes in the feature space. This is accomplished by raising the dimensionality of the input data and finding the hyperplane that maximizes the separation between the closest data points—also referred to as support vectors—for every class. SVM can handle data that is linearly separable or nonlinearly separable by using various kernel functions to map the input data into higher-dimensional feature spaces. These kernel functions include linear polynomial and radial basis function (RBF) kernels. Because SVM handles high-dimensional data well and generalizes well to new data it is widely used for a variety of applications such as text classification image recognition and anomaly detection.

C4.5 Decision Tree

The classic decision tree algorithm C4.5 which is useful for classification tasks can handle both continuous and discrete attributes. In order to minimize the uncertainty about class labels it recursively partitions the feature space based on attribute-value conditions which maximizes information gain and builds decision trees. C4.5 ensures efficient data splitting at each node by choosing the attribute that offers the highest information gain or gain ratio. By using this procedure C4.5 generates a hierarchical tree structure in which a class label is associated with each leaf node and an internal node represents a decision based on a feature attribute. C4.5 is a popular classification model in many domains due to its simplicity and effectiveness which are achieved by iteratively refining the decision boundaries and producing interpretable and efficient models.

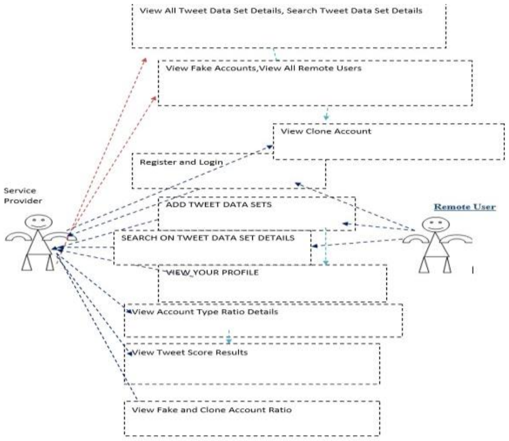
SYSTEM DESIGN

SYSTEM ARCHITECTURE



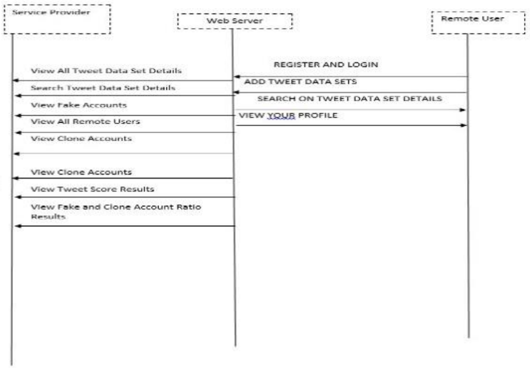
USE CASE DIAGRAM:

Use case diagrams are taken into account while doing a high-level system requirement analysis. Therefore, use cases are nothing more than the system functionalities described in an orderly fashion. They are created when the needs of a system are analysed and its functionalities are captured. The actors are the second item that is pertinent to the use cases. Anything that communicates with the system is an actor. The actors may be either external or internal apps, or they may be human users. To put it briefly, the following components need to be determined while creating a use case diagram.


View All Tweet Data Set Details, Search Tweet Data Set Details
View Fake Accounts,View All Remote Users
View Clone Account
Register and Login
ADD TWEET DATA SETS
SEARCH ON TWEET DATA SET DETAILS
VIEW YOUR PROFILE
View Account Type Ratio Details
View Tweet Score Results
View Fake and Clone Account Ratio
Service Provider
Remote User

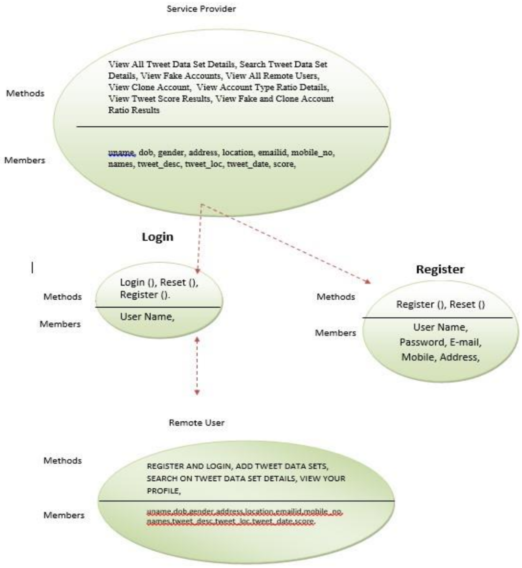
SEQUENCE DIAGRAM:

In the Unified Modelling Language (UML), a sequence diagram is a type of interaction diagram that illustrates the relationships and sequence in which processes operate with one another. It is a Message Sequence Chart construct. A sequence diagram displays the messages that are transferred between various processes or objects in the order that they occur, as horizontal arrows, and as parallel vertical lines ("lifelines") representing the various processes or objects that exist simultaneously. This enables the graphical specification of basic runtime scenarios.



CLASS DIAGRAM:

A class diagram, as used in software engineering, is a sort of static structural diagram in the Unified Modelling Language (UML) that illustrates a system's classes, attributes, operations (or methods), and interactions between the classes. It indicates which class has the data.


Service Provider
Methods
View All Tweet Data Set Details, Search Tweet Data Set Details, View Fake Accounts, View All Remote Users, View Clone Account, View Account Type Ratio Details, View Tweet Score Results, View Fake and Clone Account Ratio Results
Members
uname, dob, gender, address, location, emailid, mobile_no, names, tweet_desc, tweet_loc, tweet_date, score,
Login
Methods
Login (), Reset (), Register ().
Members
User Name,
Register
Methods
Register (), Reset ()
Members
User Name, Password, E-mail, Mobile, Address,
Remote User
Methods
REGISTER AND LOGIN, ADD TWEET DATA SETS, SEARCH ON TWEET DATA SET DETAILS, VIEW YOUR PROFILE,
Members
uname,dob,gender,address,location,emailid,mobile_no, names,tweet_desc,tweet_loc,tweet_date,score,

IMPLEMENTATION

The implementation of identifying fake and clone accounts in Twitter using classification and distance measure algorithms involves several steps. First, relevant features are extracted from Twitter account data, including profile information, posting behavior and network characteristics.

These features are then used to create a structured dataset where each account is represented by a set of feature-value pairs. Then, the dataset is labeled, designating each account as either genuine or fake based on established criteria or human judgment.

DATA COLLECTION PREPROCESSING

First, information is collected from Twitter, including account metadata including profile details, posting patterns, engagement metrics, and network properties. This data is carefully cleaned to remove noise, inconsistencies, and missing numbers, guaranteeing its dependability and quality. The cleansed data is then used to extract relevant elements, such as network attributes, engagement metrics, posting frequency, and indicators of profile completeness.

To ensure consistency, numerical characteristics are scaled, and categorical variables can be encoded to make them work with classification algorithms. The pre-processed data is then divided into training and testing sets to make the process of creating and assessing detection models easier. By doing these actions, a precise and strong basis is created for the later phases of model deployment and training, which are used to detect fake and duplicate Twitter accounts.

FEATURE EXTRACTION

A crucial stage in detecting fake and clone accounts on Twitter is feature extraction, which entails taking pertinent data and turning it into useful features. This procedure includes a number of components, including network properties, posting patterns, engagement metrics, and profile data. Analysts can create a thorough representation of every Twitter account by extracting variables such as content similarity, follower-following ratio, frequency of posts, and completeness of the profile. By providing inputs to classification algorithms, these characteristics help identify abnormalities and discern between authentic and fake accounts. Detection systems can identify minute trends that point to fake or clone accounts through efficient feature extraction, enhancing the reliability and integrity of the Twitter network

MODELING:

Modelling involves employing machine learning algorithms to evaluate extracted data and categorise accounts as authentic or fraudulent in order to detect fake and clone accounts on Twitter. The goal of the modelling process is to identify minute trends that point to fake or clone accounts through the selection and training of classification models like Support Vector Machines, Decision Trees, or Neural Networks. These models may successfully identify between genuine and fraudulent accounts by fine-tuning model parameters and assessing performance using measures like accuracy and precision. This improves platform security and user trust.

EVALUATION:

During the evaluation stage of Twitter account identification, the efficacy of the detection system is evaluated by means of a thorough examination of the classification outcomes. The success of the system is measured by computing evaluation metrics including accuracy, precision, recall, and F1-score, which compare the predicted labels of Twitter accounts produced by the trained model with their genuine labels. These metrics give information about how well the model distinguishes between real and fake accounts, which enables optimisation and fine-tuning to improve detection accuracy. Detection systems are able to accurately detect clone and fake accounts on Twitter by means of thorough examination, which enhances user trust and the integrity of the network.

DEPLOYMENT AND MONITORING

Real-time account classification is facilitated by the integration of the trained detection model into the platform's infrastructure.

With this implementation, account activity can be continuously monitored, allowing the model to identify and flag suspect behaviour as it happens. Frequent monitoring is keeping an eye on the model's performance measures, like accuracy and false positive rates, and modifying the model's parameters or training set as needed to keep it functional. Through proactive system monitoring and timely response to new risks, the platform may effectively reduce the number of fake accounts, hence preserving its integrity and cultivating user confidence.

TESTING

Finding errors is the goal of testing. The process of testing a work product involves attempting to find every potential flaw or vulnerability. It offers a means to verify if individual parts, subassemblies, assemblies, and/or a final product are functioning. Software emulation is the process of testing software to make sure it satisfies user requirements and expectations and doesn't malfunction in an unacceptable way.

There are several kinds of tests.

UNIT TESTING:

The process of designing test cases for unit testing ensures that the core logic of the programme is operating correctly and that programme inputs result in legitimate outputs. Validation should be done on all internal code flows and decision branches. It is the testing of the application's separate software components. Prior to integration, it is completed following the conclusion of a single unit. This is an intrusive structural test that depends on an understanding of its structure. Unit tests evaluate a particular application, system configuration, or business process at the component level.

INTEGRATION TESTING:

The purpose of integration tests is to verify if interconnected software components function as a single programme. The fundamental results of screens or fields are the main focus of event-driven testing. Although unit testing successfully demonstrated that each component was satisfied separately, integration tests verify that the combination of components is accurate and consistent. The express purpose of integration testing is to reveal any issues that result from the combination of various components.

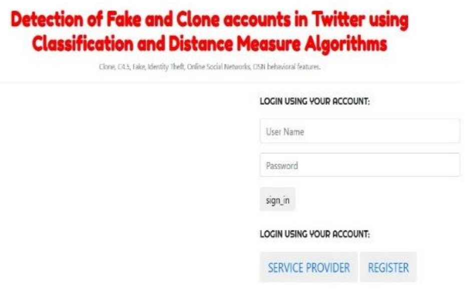
USER ACCEPTANCE TESTING:

The purpose of integration tests is to verify if interconnected software components function as a single programme. The fundamental results of screens or fields are the main focus of event-driven testing. Although unit testing successfully demonstrated that each component was satisfied separately, integration tests verify that the combination of components is accurate and consistent. The express purpose of integration testing is to reveal any issues that result from the combination of various components.

OUTPUT TESTING:

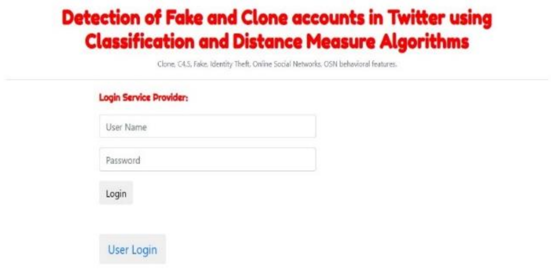
The suggested system's output must be tested when the validation testing is finished, as no system can be useful if it cannot generate the necessary output in the appropriate format. By asking users what format they need, you may test the outputs that the system is considering producing or displaying. As a result, there are two ways to think about the output format: one is on screen, and the other is printed. Finished, as no system can be useful if it cannot generate the necessary output in the appropriate format. By asking users what format they need, you may test the outputs that the system is considering producing or displaying. As a result, there are two ways to think about the output format: one is on screen, and the other is printed.

OUPUT DISPLAY:



Detection of Fake and Clone accounts in Twitter using Classification and Distance Measure Algorithms

Clone, C4.5, Fake, Identity Theft, Online Social Networks, OSN behavioral features.



Detection of Fake and Clone accounts in Twitter using Classification and Distance Measure Algorithms

Clone, C4.5, Fake, Identity Theft, Online Social Networks, OSN behavioral features.

CONCLUSION

In online social networks, clone and fake profiles have grown to be a major issue. In daily life, we learn about various hazards posed by these profiles. Thus, a technique for detecting fake and clone Twitter profiles has been proposed. A set of rules was implemented for fake detection, and these rules can distinguish between real and fake profiles. Similarity Measures and the C4.5 algorithm were used to detect clones, and the results were compared to assess performance. Compared to C4.5, clone identification with Similarity Measures performed better and could identify the majority of the clones supplied into the system. Only the profile attributes for clone and fake detection have been taken into consideration in this work. This study can be expanded in the future by adding some NLP approaches and considering tweets as well.

REFERENCE

[1] Sowmya P and Madhumita Chatterjee," Detection of Fake and Cloned Profiles in Online Social Networks", Proceedings 2019: Conference on Technologies for Future Cities (CTFC)

[2] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", 2013

[3] Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile Cloning Detection in Social Networks", 2014 European Network Intelligence Conference

[4] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angello Spognardi, Maurizio Tesconi, "Fame for sale: Efficient detection of fake Twitter followers", 2015 Elsevier's journal Decision Support Systems, Volume 80

[5] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set", World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering Vol:10, 2016

[6] M.A.Devmane and N.K.Rana, "Detection and Prevention of Profile Cloning in Online Social Networks", 2014 IEEE International Conference on Recent Advances and Innovations in Engineering

[7] Kiruthiga. S, Kola Sujatha. P and Kannan. A, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques" 2014 International Conference on Recent Trends in Information Technology

[8] Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, Ceyhun Akyol, "Twitter fake account detection", 2017 International Conference on Computer Science and Engineering (UBMK)

[9] Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A.S, "Python based Machine Learning for Profile Matching", International Research Journal of Engineering and Technology (IRJET), 2018

[10] Olga Peled, Michael Fire, Lior Rokach, Yuval Elovici, "Entity Matching in Online Social Networks", 2013 International Conference on Social Computing

[11] Aditi Gupta and Rishabh Kaushal, "Towards Detecting Fake User Accounts in Facebook", 2017 ISEA Asia Security and Privacy (ISEASP)

[12] Michael Fire, Roy Goldschmidt, Yuval Elovici, "Online Social Networks: Threats and Solutions", JOURNAL OF LATEX CLASS FILES, VOL. 11, NO. 4, DECEMBER 2012, IEEE Communications Surveys & Tutorials

[13] Ashraf Khalil, Hassan Hajjdiab and Nabeel Al-Qirim, "Detecting Fake Followers in Twitter: A Machine Learning Approach" 2017 International Journal of Machine Learning and Computing

[14] Mohammad Reza Khayyambashi and Fatemeh Salehi Rizi, "An approach for detecting profile cloning in online social networks" 2013 International Conference on e-Commerce in Developing Countries: with focus on e-Security

[15] Mauro Conti, Radha Poovendran and Marco Secchiero, "FakeBook: Detecting Fake Profiles in On-line Social Networks", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining