Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.499 – 502

Identity Deception Detection and Security in Social Medium

Sheetal Antony[1], Prof. B. S. Umashankar[2]

[1]Department of Computer Science & Engineering, Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

[2]Department of Computer Science & Engineering, Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

[1] sheetal.mtechscs14@sahyadri.edu.in; [2] umashankar.cs@sahyadri.edu.in

Abstract— There has been a large increase in the usage of the Internet in the past few years. Identity deception has become an increasingly important issue in the social media environment. The case of blocked users initiating new accounts, often called sockpuppetry, is widely known. The past efforts to detect such users have been primarily based on verbal behaviour. Although these methods yield a high detection accuracy rate, they are computationally not very efficient for the social media environment. We present a detection method based on non-verbal behaviour and verbal behaviour for identity deception, which can be applied to many types of social media. We demonstrate that our proposed method results in high detection accuracy over previous methods proposed while being computationally efficient for the social media environment. We also demonstrate the potential of nonverbal behaviour data that exists in social media and how designers and developers can leverage such non-verbal information in detecting deception to safeguard their online communities. We create a social medium to demonstrate this.

Keywords— social, media, deceive, verbal, non-verbal, identity.

I. INTRODUCTION

There are a lot of social networks available online. The most popular ones are Facebook, MySpace, and Twitter. These let the individuals to create accounts and express their interests. They can publish their details such as personal information, educational background, family members, interests in the field of art, culture, movies, news, music, various cuisines.

In the past decade we have experienced an increasing level of interest in online social media, which enable users to not only create content but also exchange it using Web 2.0 technologies [1]. The number of users registering with social networking sites such as Facebook and Twitter keeps increasing at a rapid pace

amounting to 82 percent of the world's online population [2]. Social network usage has increased by 64% since 2005 [3].

The ease with which we can generate online pro les at a low cost has also led to ample opportunities for identity deception, which at times can have fatal consequences. A recent well-known example is the case of a mother pretending to be a teenage boy on the social networking site MySpace in order to obtain information from a teenage girl eventually leading to the girl committing suicide [4].

Other social media services such as collaborative projects have to engage in "cat-mouse" games by constantly having to block user accounts for individuals joining in with different account names not long after a block has been applied.

Solutions have been proposed that can assist in detecting multiple accounts owned by the same in-dividual but their effectiveness vary in terms of computational efficiency and complexity of practical implementation depending on the availability of the appropriate data [5], [6]. Moreover, these past methods have mainly focused on detecting deception through verbal communication (e.g., speech or text) and have ignored the potential of non-verbal (e.g., user activity or movement) deception detection, which has shown high success rates in the offline world [7], considering that nonverbal cues are 4.3 times more powerful than verbal cues in face-to-face communication [8].

In this paper we propose a novel approach that makes use of user verbal and non-verbal behaviour data in social media in order to detect multiple account identity deception.

II. LITERATURE SURVEY

A. The Deception Scenario:

Deception is when we try to transfer false information purposefully to cheat a particular person. The person who is deceived is unaware that he/she has been cheated. In this scenario we have a sender who is sending a message using a channel through which communication is taking place. There is a receiver who receives the message from a sender. The receiver is expecting the communication to be from a particular sender who is authentic. [2]

Deception detection theories are divided into those that are based on leakage cues (cues sent by the deceiver unwillingly due to factors such as cognitive overload) and strategic decisions (cues indicative of deception that are willingly transmitted by a deceiver in order to ensure deception success). To detect deception, both categories pick up cues from verbal and non-verbal communications. Human deception detection is arguably the most widely used method. Individuals can pick up cues from the environment in which an interaction takes place (e.g., a photograph that looks edited) with a deceiver and interpret these cues by understanding a deceiver's goals. The most critical factor in detecting deception is the time, which can vary from days to months, until a truth is uncovered by a previously deceived individual.

A particular issue with identity deception in social media is the presence of multiple identities by one user. Both online and offline studies have been conducted in an attempt to solve the problem of detecting duplicate account records. Wang et al. [3] in their study attempted to identify duplicate records in a criminal database using a variety of similarity-based detection algorithms. Attributes such as name, address, social security number and date of birth from a criminal database were compared as strings using a string comparator and the level of disagreement for these items was obtained between different user records.

Furthermore, they obtained the overall disagreement between records based on these attributes, and those matches that had a disagreement below a certain threshold were considered as the same account. The most direct solution to identify duplicates in a database with the highest accuracy is a cross-comparison for the full length of accounts in a database.

B. Motivation for Deception

When a deceiver transfers false information purposefully they will definitely have some motives though some people do it to while away time. The person who is going to deceive i.e. the deceiver will do that because of the gain he/ she is going to receive from the mystification. The motivation may be instrumental or goal-driven, relational and identity driven goals. The intention of the deceit may be either to actually harm due to spitefulness. It may be only a genial sign of the amiability [1].

C. Related Works

A deceiver's goal is to use everything at his/her disposal to keep a low suspicion from his/her target and this applies to both verbal and non-verbal behaviours. There is also a moral cost for a deceiver that wills affect the likelihood of using deception [5]. The software design of the social medium also affects deception through

factors such as the perceived level of security provided by the system along with mechanisms that enhance trust and make assurances [6]. The deceptive action transmitted through cyberspace also has attributes such as the number of targets and the expiry date associated with it that influence its success. Finally, a victim's ability to detect deception is an important factor that influences deception success. Humans have been consistently shown to be bad deception detectors [7].

Michail Tsikerdekis and Sherali Zeadally [1] used the various non-verbal behaviors to identify the mystification. Various aspects come under the non-verbal behavior. The style in which the user messages, the way they navigate through the social media, their behavioural patterns.

In this paper they tried to identify the deceit when the same attacker creates many accounts providing fake information. When the person would be blocked, they create another account.

This approach focuses on the activities of the user. It protects the privacy of users. It does not leak the personal account information of the users. Thus using this method, we can identify the same user does deceit using many accounts. The deceitful activities are predicted. Thus there can be a prevention of the unusual activities that will cause harm to the users.

This paper provides a future scope to combine verbal behavior with non-verbal behavior. Thus in our work we will use the combination of these two behaviours to identify the deception more effectively.

III. MODEL AND ARCHITECTURE

A. Proposed System

We are in a need of a system that can use verbal and non-verbal behavioural patterns to detect identity deception. We also need to provide a safe socializing environment for the users so that they can share their information safely.

B. System Architecture

The architectural design will show the conceptual model of the application. It shows the overall architecture of the system. In the figure 1, the various users login into the system after their account creation. The admin manages these users.

The details and the activities of the user are analysed and we detect if there is any deception. The details are verified in the database. If we detect any deception, we pose some security questions and test the user and alert the admin.

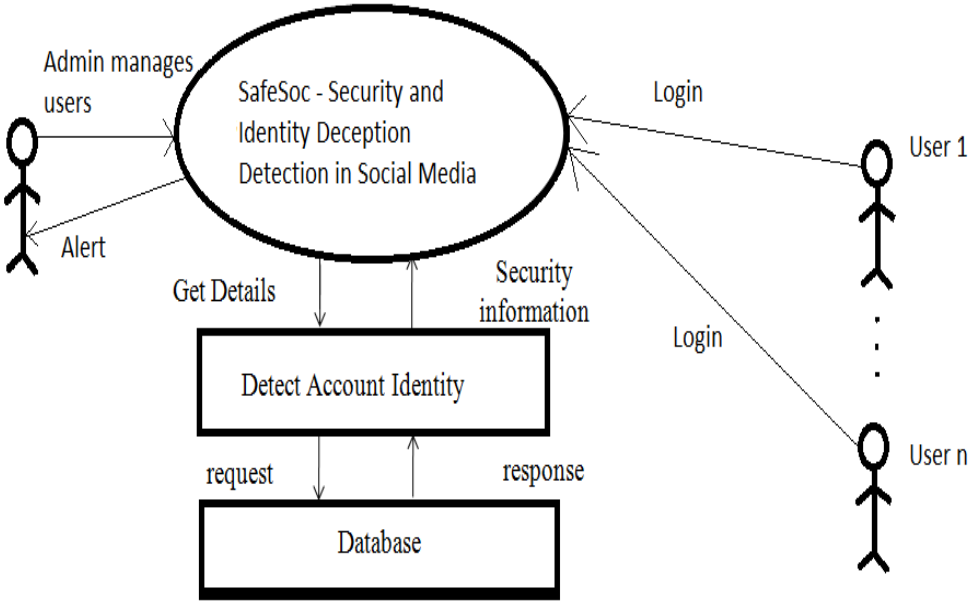

Fig. 1 System Architecture

C. System Implementation

The social medium is created where users can create their profiles, view profiles of their friends and send messages to their friends. The users can edit their profile and also change the password.

In Verbal Deception Detection Module, we are checking the verbal behaviors of the user like mobile number, username, e-mail, etc... When the user enters these details we store it in the database. It is ensured that account creation is allowed only if two accounts don't have the same details mentioned above.

In the Non-Verbal Deception Detection Module, we are detecting the various characteristics like movement and actions of the user. The activities of the users are monitored for the occurrence of any abnormal deceptive activity.

Many such characteristics are used to ensure that there are no fake profiles made and the accounts of users are not being misused by others.

IV. CONCLUSIONS

In this work we present a method to detect deception and provide security in social medium using the verbal and non-verbal behavior of a user. A combination of these two methods has brought greater results than using them individually. As a future scope we can improve on the image processing algorithm and also include other factors in verbal and non-verbal behavior.

ACKNOWLEDGEMENT

I would like to thank God Almighty for blessing me to complete this work.

I am profoundly indebted to my guide, Mr. B. S. Umashankar, Professor, Department of Computer Science and Engineering, Sahyadri College of Engineering and Management, for innumerable acts of timely advice and encouragement.

I would like to express my sincere thanks to my beloved family members and friends for their wishes and encouragement throughout the work.

REFERENCES

[1] Michail Tsikerdekis and Sherali Zeadally, *Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behavior*, IEEE Transactions On Information Forensics And Security, Vol. 9, No. 8, August 2014.

[2] Li J, Wang GA, Chen H, "PRM-based identity matching using social context", In:Intelligence and Security Informatics, IEEE International Conference, 2008.

[3] M. Argyle, V. Salter, H. Nicholson, M. Williams, and P. Burgess, "The communication of inferior and superior attitudes by verbal and non-verbal signals", British J. Social Clinical Psychol., vol. 9, no. 3, pp. 222-231, Sep.1970.

[4] Anna Squicciarini and Christopher Griffin, "An Informed Model of Personal Information Release in Social Networking Sites", arXiv: 1206.0981v1 [cs.SI] 5 Jun 2012.

[5] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", 3rd IEEE International Workshop on Security and Social Networking (SESOC), March 2011

[6] J. K. Burgoon, "A communication model of personal space violations: Explication and an initial test," *Human Commun. Res.*, vol. 4, no. 2, pp. 129–142, Dec. 1978.

[7] J. Kleinberg, C. H. Papadimitriou, and P. Raghavan, "On the value of private information", In Proc. of the 8th conference on Theoretical aspects of rationality and knowledge, TARK '01, pages 249-257, San Francisco, CA, USA, 2001.

[8] T. Solorio, R. Hasan, and M. Mizan, "A case study of sockpuppet detection in Wikipedia", in Proc. Workshop Lang. Anal. Social Media, pp. 59-68, 2013.

