An Overview of Identity Deception Approaches and Its Effects

Ms. M. Preensta Ebenazer[#1], Dr. P. Sumathi[*2]

[#1] *Research Scholar, PG & Research Department of Computer Science, Government Arts College (Autonomous),*

Coimbatore, INDIA.

[*2]*Assistant Professor, PG & Research Department of Computer Science, Government Arts College (Autonomous),*

Coimbatore, INDIA

Abstract — *Identity deception plays an important role in today's real world environment where malicious activities have increased enormously. Identity deception needs to be identified in order to prevent malicious activities that are initiated by the attackers. There are various research works that have been conducted previously with a major focus on avoiding the involvement of fake users from creating chaos. The methodologies mentioned in the proceeding sections, follow various ways to identity deception process. Most of the research works emphasised on verbal behaviour of the user activities to predict identity deception while some of the works focussed on non verbal behaviour of the user activities to predict identity deception. Several methodologies have been analyzed to find the better and flexible mechanism which can perform identity deception process effectively. From the analysis it has been made evident that the non verbal behaviour based approach can find identity deceptions that are caused by fake users in a better way. The non verbal behaviour based methodologies have a high detection accuracy rate than verbal based behaviours.*

Keywords — *Identity Deception, Non verbal Behaviour and Fake Users*

I. Introduction

Social networks are online applications that permit the users to connect by way of various link types. Based on the provided details, these networks let people to list details about themselves that are appropriate to the fundamentals of network [6]

Identity deception is the process of hiding an individual's identity while communicating with others. Identity deception may cause various problems which may lead to large economic loss in the real world environment. One of the important problems that are caused by identity deception is the financial theft which is done by faking others' account. In bank accounts there is a limitation for providing credit cards in order to control the cash flow among the fake persons [5]. However, a person can buy multiple credit cards by faking his/ her identity thus causing serious financial problems. Another important issue that may arise due to identity deception is the problem caused by terrorists. A terrorist may involve in identity deception to create fake identities that results in global economic loss. This cannot be identified effectively by the police department though there are large volumes of fake records in the police database. The police departments usually attempt to catch or impound criminals only by matching the criminal records with the police department databases. However the automatic matching and retrieval module cannot identify the real person involved in the criminal activity even though there is a presence of records of that person. This is because of fake identity creation where the automatic module cannot match the fake identities. Another problem that may arise due to identity deception is the social media fake identity establishment. This is the most encountered problem today where the person involves in unwanted activities in other person's profile by creating more fake id's. This cannot be stopped by blocking a person because the blocked person may create another fake id. Terminating users with fake ids need to be done with more concern to implement a user-friendly environment.

Identity deception is the most important issue in the real world environment which leads to various research focuses. There are various research works that have been conducted previously which focuses towards the elimination of identity deception activities. Identity deception can be done in many ways. The two most important ways are

- Verbal behaviour based
- Non-verbal behaviour based

Verbal behaviour based methodologies attempts to predict the changes present in the user profile based on direct information like their profile information, way of responding, time of usage etc. However, verbal behaviour methods cannot predict the user information accurately due to presence of fake identity information.

Non-verbal based methodologies are based on predicting users with the help of indirect information like usage scenario, terminating criteria, way of messaging, etc., Non-verbal based behaviour can be used to predict the fake users accurately than verbal behaviour.

The main contribution of this work is to analyse various researches that have been conducted to identify the identity deception nature in order to predict better and optimized approach which in turn can be used for further study. The previous researches that have been conducted towards identity deception are also listed and described in detail in the following sections.

The organization of this work is given as follows: In section 1, a basic introductory of identity deception is given. In section 2, various research methodologies that have been conducted previously are discussed. In section 3, analysis of the various methodologies is given. In section 4, the Conclusion of this paper is discussed.

II. Literature Review

In this section, various previous researches are discussed in detail which attempt to detect identity deception accurately and in turn can be used to avoid the fake identity corruption. The approaches that are based on different techniques and methodologies are mentioned below

Thomas et al. [7] introduced a novel approach for identifying the identity deception based on the non-verbal behaviour in an automated manner. This approach attempts to find the deceptive behaviour in the airport security checking unit. It is done by capturing the video of the person who are crossing the security and analyzing it for non-verbal behaviour. First, the video is segmented into image frames to make it ready for processing. Then the face and hand parts are segmented from the images to predict motion difference. The motion difference is found by extracting the features and comparing it with the available features. This method provides a better result by predicting the feature difference by calculating the threshold value.

However, this approach cannot be useful due to the differences present in high dimensional images through which one cannot identify criminal forgeries.

G. Alan Wang et al. [1] overcame the above problem by supporting the high dimensional data. It attempts to detect the deceptive behaviour by finding identity deception with the help of similar records present in the police criminal records. To do this, an adaptive algorithm is proposed in this methodology through which deceptive behaviour can be predicted even in case of missing values. This approach compares and matches the details of the individual person who has committed crimes with that of the identical records present in the police database. The experimental tests conducted by this work's author proved that this approach can predict deceptive behaviour even in case of more than 30% of missing values.

The above two works can detect the deceptive behaviours with static data only. It cannot adapt with the data which are changing dynamically and also with large volumes of data.

Georgios Kontaxis et al. [4] concentrated on the deceptive activities that occurred in the social media. The number of users is increasing in the social media where the fake profiles have also increased. In this work, a novel approach is introduced which tends to find and remove clone profiles present in social media. By doing so, the attacks that are performed by the attackers who create many fake profiles can be reduced by guaranteeing user-friendly environment. It is done by creating and maintaining the user specific information in the server database, where the profiles will not be allowed to be created if it matches with the information submitted by the user.

The above methodologies concentrate on predicting fake accounts. But those approaches cannot completely avoid the fake profiles that are created.

Qiang Cao et al. [8] introduced an approach that concentrated on detection of fake accounts based on the log likelihood value. This is done by using a new approach named Sybil Rank in which users are ranked based on their fake information. The fake profiles are identified by matching each profile with the other profiles aiming to detect the similar information. The testing environment of this work proves that the proposed approach can detect 90% of fake accounts than the existing approaches.

All the approaches discussed above concentrates on detecting and eliminating the user profiles and do not concentrate on the privacy issues of the users where the valid users' privacy may get violated.

Anna Squicciarini and Christopher Griffin [2] introduced a new methodology which focuses on the privacy issues of the users before analyzing their personal profiles. The social media networks concentrate on these activities that implemented an informed model for privacy reasons. This model enables users to setup their user profiles through which one can limit the information that are shared with others. This information profile needs to be validated periodically in order to limit issues present in the various approaches.

The information diffusion from multiple sources may lead to accurate prediction of the deceptive behaviour which is not handled by any of the works defined above.

Chuan Peng et al. [3] intended to identify the information diffusion from multiple sources, by predicting the deceptive behaviour with more accuracy. To achieve this, more social network service providers are integrated together to work, where their user profile information is shared among each other. The larger amounts of data sets that are collected from multiple sources are called as Digg. This digg is used to identify wrong behaviours that are involved in the various user profiles through which deceptive behaviour can be predicted well.

All these approaches tend to identify the user deceptive activities with the help of information that reside in the database like their profile information, text messages etc which may lead to wrong prediction where users may reveal wrong information..

Michail Tsikerdekis and Sherali Zeadally [5] introduced a novel way to identify the deceptive behaviour based on the non-verbal behaviour. The non-verbal behaviour of the user profiles relate to many similarities like the user's texting style behaviour and their movement across different pages. This methodology aims to concentrate on the user activities, thus protecting the privacy of users without leaking their personal information. This approach can be used to identify the deceptive behaviour in multiple accounts which are created by single attacker who involves in malicious activities. The malicious activities are predicted in order to avoid the unusual activities that may affect the user profiles.

III. Analysis

The advantages and disadvantages of these approaches which are discussed above are compared with each other to identify the better or suitable approach that can be utilized for identity deception. In table 1, comparison of these approaches are given and discussed in a detailed manner mentioning the advantages and disadvantages of each and every method

I. Analysis of Identity Deception Methodologies

S.NO	TITLE	AUTHOR	METHOD	ADVANTAGES	DISADVANTAGES
1	Deception Detection through Automatic, Unobtrusive Analysis of Non verbal Behaviour	Thomas O. Meservy, Matthew L. Jensen, John Kruse, Judee K. Burgoon, and Jay F	Automated, unobtrusive system	• Envision a future version of the system that automatically segments interesting portions of an interaction.	• This approach is not useful in the case of high dimensional images through which one cannot identify criminal forgeries
2	Automatically Detecting Criminal Identity Deception: An Adaptive Detection Algorithm	G. Alan Wang, Hsinchun Chen, Jennifer J. Xu, and Homa Atabakhsh	Adaptive detection algorithm	• There were significant variations in the detection accuracy when values were missing in the address attribute, regardless of the percentage of incomplete records	• Requires great amounts of manual information processing and is very time-consuming • This method is quite inefficient for large-scale datasets.
3	Detecting Social Network Profile Cloning	Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos	IAC Approach	• Highest level of precision rate in this system • Time complexity is low in this system	• An important drawback of this system is that it currently uses only the LinkedIn social network. • This system doesn't have appropriate string matching features to overcome wrongly typed information, or deliberately injected mistakes • Accuracy rate of the system is lower
4	Aiding the Detection of Fake Accounts in Large Scale Social Online Services	Qiang Cao, Michael Sirivianos and Xiaowei Yang Tiago Pregueiro	SybilRank	• High precision • SybilRank can process very large social graphs using a few commodity machines	• Computational overhead of this system is higher than the other systems • Number of iterations is sufficient to reach an approximately uniform distribution of degree-normalized trust over the fast-mixing non-Sybil region, but limits the trust escaping to the Sybil region. • Reliability of the system is lower

5	An Informed Model of Personal Information Release in Social Networking Sites”	Anna Squicciarini and Christopher Griffin	Deception model	• Highest quality of the experiment result • More faster than the other systems	• Computational overhead of the system is higher
6	Predicting Information Diffusion Initiated from Multiple Sources in Online Social Networks	Chuan Peng, Kuai Xu, Feng Wang and Haiyan Wang	Digg	• Achieved an average of 75% prediction accuracy • Effectively characterized and predicted the process of information diffusion	• Time complexity rate of the system is lower • False positive and false negative rate is lowest in this system
7	Key Players Identification in Social Network for Preventing Private Information Leakage	T.Priyanka	KPP-POS and KPP-NEG	• Improved security by classification of different kind of malicious behavior	• There may be an possibility of corruption of nodes while transferring data among different user profiles
8	Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behaviour	Michail Tsikerdekis and Sherali Zeadally	Detection method based on nonverbal behaviour for identity deception	• More precision and better accuracy • Better support in detecting identity deception with presence of non verbal behavior	• More time consumption

IV. Conclusion

Identity deception is one of the major problems faced by the real world environment which tends to degrade the user performance considerably by performing malicious activities on their profile. In this paper, various methodologies are analysed to predict the unusual behaviours present in the user profiles. Each and every method identifies the deceptive behaviour in different perspectives. Finally from the analysis it has been ascertained that the multiple identity deception based on non verbal behaviour provides better and accurate results than other methodologies in terms of precision and recall measures.

References

[1] *G. Alan Wang, Hsinchun Chen, Jennifer J. Xu, and Homa Atabakhsh "Automatically Detecting Criminal Identity Deception: An Adaptive Detection Algorithm", IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 36, No. 5, September 2006*

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

[3] *Chuan Peng, Kuai Xu, Feng Wang and Haiyan Wang, "Predicting Information Diffusion Initiated from Multiple Sources in Online Social Networks", in Proceedings of International Conference on Distributed Computing Systems (ICDCS), Vol. 2, October 2013*

[4] *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*

[5] *Michail Tsikerdekis and Sherali Zeadally, "Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behaviour", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 8, August 2014*

[6] T.Priyanka, "*Key Players Identification in Social Network for Preventing Private Key Players Identification in Social Network for Preventing Private*", International Journal of Computer Trends and Technology (IJCTT) – volume 10 number 3 – Apr 2014

[7] *Thomas O. Meservy, Matthew L. Jensen, John Kruse, Judee K. Burgoon, and Jay F, "Deception Detection through Automatic, Unobtrusive Analysis of Non verbal Behaviour", IEEE Intelligent Systems, Vol. 20, No. 5, September 2005*

[8] *Qiang Cao, Michael Sirivianos and Xiaowei Yang Tiago Pregueiro, "Aiding the Detection of Fake Accounts in Large Scale Social Online Services", In SIGCOMM Poster Session, April 2011.*