International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

BEHAVIORAL ANALYTICS FOR IDENTITY THEFT DETECTION IN SOCIAL NETWORKS: A COMPOSITE MODELING APPROACH

[1]D.Saikrishna,[2]D. Manisha

[1]Assistant Professor, Department of MCA Student, Sree Chaitanya College of Engineering, Karimnagar

[2]MCA Student, Department of MCA Student, Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Our objective is to offer a path from raw behavioural data to a behavioural model capable of accurately, quickly, and effectively identifying online identity theft. We concentrate on this problem in online social networks (OSNs), where users frequently keep composite activity logs that combine multimodal, low-quality online user-generated content (UGC) with offline check-ins. When simulating user activity patterns, we establish that various record dimensions have a complementing influence, which is a helpful discovery. We recommend utilising a combined (as opposed to fused) model to capture elements of a user's composite behaviour that occur both online and offline in order to effectively use this complementary influence. We compare the suggested combination model with the combined model and traditional models after evaluating it on two real-world datasets, Yelp and Foursquare. Our model outperforms the current ones, according to the experimental data. The area under the receiver operating characteristic curve (AUC) values for Foursquare and Yelp were 0.956 and 0.947, respectively. For example, Yelp and Foursquare have disturbance rates (false-positive rates) of less than 1% and recall (true positive rates) of up to 72.2% and 65.3%, respectively. By achieving these results, we are able to evaluate a single composite behaviour and ensure the quick reaction latency of our method. Because it would provide insight on whether or whether composite behavioural patterns of people may be used to better real-time online identity verification, cybersecurity experts might benefit from this study.

I. INTRODUCTION

Owing to the Internet's rapid growth, more and more tasks—such as making hotel reservations, purchasing tickets, writing letters, getting medical treatment, and shopping—are being done online [1-4].The Internet does, however, carry certain potential security risks, such as the potential for financial information loss [5, 6], identity theft [6, and privacy breaches [3]. Accounts serve as users' agents in the virtual world. One prevalent kind of online crime is online identity theft, which is often described as the deliberate use of another person's account to get credit and other benefits in that person's name [7]. In fact, most cybercrimes, such as spam [9], fraud [8], and blackmail [5], originate from compromised accounts [1]. For this reason, protecting customers' online safety depends on identifying identity theft.

Most conventional identity authentication methods depend on access

control mechanisms, including passwords and tokens [11], [12]. But when it comes to managing their passwords or tokens, customers have to pay for certain services. With appropriate implementation, biometric identification [13]–[15] ushers in the era of password-free access. However, because of a few flaws, these access control techniques are useless for real-time web applications [16], [17].

They don't cause any inconvenience. Users need to give the login procedure additional time.

2) They are not endless. No further security can be provided by the defensive system after the access control has been breached.

Behavior-based suspect account detection has been proposed as a much-anticipated way to seek a continuous and nonintrusive identity authentication for online services [16], [18], and [19]. It is required to document the users' dubious behaviour patterns in order to differentiate between the suspicious accounts. The problems may be divided into two categories: the identification of hacked accounts [21] and fake/sybil accounts [20]. The fraudulent/Sybil account often behaves differently from how most people do. Meanwhile, the compromised account often displays odd behaviour, sometimes even acting as a fake or sybil account. It could be fixed by spotting changes in users' behaviour patterns.Since phoney or sybil accounts' actions are often simpler to recognise than those of the former, identifying them is relatively easier than detecting hacked accounts. It may be accomplished by using a variety of population-level strategies that have been well studied, including clustering [22], [23], classification [5], [24]–[26], and statistical or empirical principles [8], [27], and [28]. As a result, we focus only on identifying compromised accounts—also referred to as identity theft—using behavioural models at the individual level.

According to current research, identity theft may be detected at the person level via the use of suspicious behaviour detection [9], [29]–[35]. The efficiency of these tactics is largely dependent on the quality of the behaviour data. They often encounter subpar behaviour records as a consequence of limitations on data collecting or issues with privacy [3]. In particular, the applicability of a strategy may be limited and the likelihood of insufficient data compromising its efficacy may grow if it depends only on one dimension of behavioural data. Unfortunately, many of the currently available studies, such those on keystroke [29], click stream [32], [36], touch-interaction [37], and user-generated content (UGC) [9], [33], [34], and [38], only address a single facet of user behaviour.

In this research, we provide a multidimensional behavioural data-based approach to identity theft detection that may not be sufficient in all dimensions. Based on these characteristics, we choose the online social network (OSN) as a sample scenario, where most users' behaviours are coarsely recorded [39]. In the era of the Internet, users' actions combine their offline, online, social, and perceptual/cognitive pursuits. Behavioural data may be gathered via a variety of applications, such as online tip-posting in instant messaging services, offline check-ins in location-based services (LBSs),

and social relationship-building in online social services. Consequently, we build our approach based on the combined behaviours of individuals from these groups.

The user behavioural data in OSNs that can be used for online identity theft detection are often too low-quality or restricted to build suitable behavioural models due to data collection challenges, user privacy requirements, and the fact that some users have multiple behavioural records. Our goal is to show that, even in situations where the data is woefully deficient in any one dimension, multidimensional behavioural data may still be used to generate a high-quality (quick, robust, and efficient) behavioural model.

Behavioural data is often integrated using the fused and combined manners paradigms. Fused models are a more fundamental and straightforward kind of composite behaviour models (CBMs). They initially gather features in each behaviour space before developing a comprehensive measure based on these attributes in several dimensions. Because of the possible complementing effects across different behaviour spaces, they could be a viable choice for integration [7], [17]. Fused models, however, may still improve identification efficacy since they do not take into account potential relationships between different behavioural domains. We use the example of a person who visited a park and posted a picture on a social media website. If this composite behaviour is split into two separate, distinct parts—the user once went to a park and submitted a picture—removing it from a group of users would be more challenging. This is due to the possibility that more users than in the initial circumstance will meet these two simple requirements. On the other hand, the combined model could be able to better capitalise on the associations between various behaviours, increasing the efficacy of identification and boosting user trust in their behaviour patterns. The fundamental reasoning for the distinctions between the joint and fused models is also explained by the well-known Chain Rule for Entropy [40], which asserts that the entropy of many simultaneous events is equal to the sum of the entropies of each individual event if the events are independent. It shows that the overall behaviour has less uncertainty than the total uncertainty in each component [41].

Therefore, to appropriately use the data included in composite behaviours for the intent of user profiling, we propose a joint model based on Bayesian networks, or more specifically, a joint probabilistic generative model named CBM. In two different behaviour spaces—the online behaviour space for user-generated content and the offline behaviour space for check-in location—it offers a mix of basic features. Drawing on the composite behaviour of an individual, we conjecture the subsequent generating process. Based on their behavioural distribution, a user unintentionally selects a certain pattern of behaviour while planning to attend an event and at the same time make recommendations online. Next, he or she generates a topic and a targeted venue, respectively, based on the subject and venue distributions of the present pattern. In the end, the development of his or her comments follows the proper topic-word allocation. To estimate the

parameters of the previously described distributions, we use the collapsed Gibbs sampling approach [42].

For any composite behaviour, represented by a triple-tuple (u, v,D), we can calculate the probability that user u will visit venue v and use a set of words D to write a tip online using the joint model CBM. Taking into consideration the different degrees of user activity, we generate a relative anomalous score Sr to measure the frequency of each composite behaviour (u, v, and D). We can now identify identity theft suspects in real time based on a single composite behaviour thanks to the use of these techniques.

We evaluate our joint model against three standard models and their fused model [17] using two real-world OSN datasets: Yelp [44] and Foursquare [43]. The area under the receiver operating characteristic curve (AUC) serves as our measure of detection effectiveness. Specifically, under the same conditions, the fused model can only attain 60.8% and 60.4%, respectively; while, in Foursquare and Yelp, the recall [true positive rate (TPR)] may reach as high as 65.3% and 72.2%, respectively, with a comparable disturbance rate [false-positive rate (FPR)] of less than 1%. Notably, this performance can be achieved by examining a single composite behaviour for every authentication, guaranteeing the quick reaction time of our detection technique. As a perceptive result, we find that there is a true complementing influence between different low-quality record dimensions when it comes to modelling user behaviour.

The main contributions are summed up in three parts.

We propose a combined model, dubbed CBM, that can capture both online and offline aspects of a user's composite behaviour, to help make appropriate use of coarse behavioural data.

2) We create a relative anomalous score Sr to measure the frequency of recurrence of each composite behaviour in order to perform real-time identity theft detection.

3) To demonstrate that CBM is effective, we do experiments on two real-world datasets. The results show how responsive and effective our approach is when compared to existing models.

Problem Statement:

Online social networks (OSNs) have been widely used, which has made it easier for many cyber risks to flourish. One such threat is identity theft, which is becoming more and more sophisticated. Traditional identity theft detection techniques in online social networks sometimes depend on rigid, rule-based procedures that are unable to keep up with the ever-evolving strategies used by malevolent actors. Current methods are insufficient for precise and prompt identity theft detection because they often cannot fully model and evaluate composite behaviors, which combine many aspects of user interactions. Furthermore, it is very difficult to discern between real and fraudulent activity on these platforms due to the dynamic and interrelated nature of social relationships. Identity theft detection requires a sophisticated comprehension of both individual and group user activities, including textual, visual, and temporal

aspects. The inadequacies of existing detection techniques impede the proactive identification of identity theft cases, hence placing users at risk of financial, reputational, and personal consequences.

Consequently, the current issue is on the limitations of traditional identity theft detection methods in online social networks, calling for a paradigm change in favor of composite behavioral modeling. Creating an intelligent and flexible model that incorporates several behavioral elements is essential to successfully detect oblique patterns suggestive of identity theft and to improve user security in online social networks.

Objectives:

Create Composite Behavioral Models: To offer a comprehensive picture of user behavior in online social networks, create sophisticated composite behavioral models that take into account textual, visual, and temporal components of user interactions.
Include Machine Learning Methodologies: Train the composite behavioral models on a variety of datasets using machine learning techniques, such as ensemble methods and deep learning, so that the system can pick up on and adjust to changing identity theft strategies.
Representation and Extraction of Features: In order to ensure that users' online activity is comprehensively represented for identity theft detection, it is recommended to implement effective feature extraction algorithms to collect key behavioral features from user activities, profiles, postings, and interactions.
Monitoring and Analysis in Real-Time: Provide systems for tracking and analyzing user activity in online social networks in real time so that composite behavioral models may quickly spot unusual trends that can point to identity theft.
Alerts and Dynamic Thresholds:
Set flexible cutoff points that take into account how online social network users behave. This will allow you to respond quickly to possible identity theft situations by setting off alarms when the composite behavioral models identify changes from typical user behavior.
Integration Across Platforms:
To provide a flexible and platform-agnostic identity theft detection system, allow the composite behavioral models to function fluidly across several social networking platforms, taking into account the various user behaviors and characteristics distinctive of each platform.

II. LITERATURE SURVEY

Proc. Internet Measurement Conference, Nov. 2016, pp. 65–79; J. Onaolapo, E. Mariconti, and G. Stringhini, "What happens after you are pwnd: Understanding the use of leaked Webmail credentials in thenwild."
Subterranean discussion boards have become an essential tool for selling and distributing stolen personal data in recent years. The forums have, however, progressively come to be utilized as information sources for data breaches. As a consequence, there is a growing tendency in the announcement of data theft outcomes via forum posts. By locating these linkages, the hacked third party may react to the data breach event more swiftly. In order to do this, we built a technology that can automatically detect the threads connected

to data breaches. on real time, the technology can keep an eye out for and identify data breaches on underground forums. Additionally, by using the feature extraction approach based on the LDA topic model, the research was able to further uncover the phrasing features of the threads. The data set for this study was gathered from both the dark and surface webs. In addition, we evaluated many supervised classification algorithms in this application situation and chose the optimal approach for the classifier in order to enhance system performance. On the experimental data set, we were able to identify over 92% of the data breach threads using the approach.

In Proc. Int. Conf. Collaborationn Technol., A. Mohan presents "A medical domain collaborative anomaly detection framework for identifying medical identity theft."

The crucial job of anomaly detection has been used extensively in a variety of contexts. Its use in public healthcare, in particular, is an essential management activity that may raise the standard of treatment while averting enormous financial losses. In this work, we propose and test a provider-consumer model-based anomaly detection system in the healthcare industry. There are two stages to our process. Anomaly scores are initially assigned to cities (consumers) based on their demand, and in the second step, the scores are transferred from cities to hospitals (providers). We showed the method's capacity to identify possibly fraudulent hospitals by applying it to a genuine database from the Brazilian public healthcare system that documents medical operations that cost more than $8.5 billion between 2008 and 2012. The Brazilian government is using this approach to identify hospitals that exhibit unusual patterns that need further investigation. Our primary contributions are (i) a straightforward and efficient method for detecting anomalies in the healthcare industry; (ii) our approach doesn't require knowledge of medical regulations or provider information; (iii) the consumer perspective analysis enables the identification of anomalies that would have been missed by traditional methods; and (iv) we validated the method thoroughly on a real database.

"Unique in the shopping mall: On the reidentifiability of credit card metadata," Science, vol. 347, no. 6221, pp. 536–539, Jan. 2015, Y.-A. de Montjoye, L. Radaelli, V. K. Singh, and A. S. Pentland.

Massive human behavior data sets have the power to drastically change how we do research, battle illness, and build cities. However, crucial information is included in metadata. The widespread usage and, eventually, effect of these data sets depend on our ability to comprehend their privacy. We examine three months' worth of credit card data for 1.1 million individuals and demonstrate that 90% of individuals can be uniquely reidentified using only four spatiotemporal points. We demonstrate that the average increase in the risk of reidentification due to transaction price knowledge is 22%. In conclusion, we demonstrate that women are more recognisable in credit card metadata than males are, and that even data sets that include imprecise information at any or all of the dimensions offer minimal anonymity.

P. Hyman, "Cybercrime: How Serious Is It Really?," Commun. ACM, vol. 56, no. 3, March 2013, pp. 18–20.

In order to assure quality and accuracy and reduce the loss of health care funds, the European iWebCare project (FP6-2004-IST-4-028055) seeks to design and develop a flexible fraud detection web services platform that can support e-government processes of fraud detection and prevention. This paper describes the methodology used in this project, which includes developing an integrated fraud detection platform with an ontology-based rule engine and a data mining-based self-learning module, as well as introducing a fraud detection methodology that combines knowledge engineering and business process modeling.

"All your contacts are belong to us: Automated identity theft attacks on social networks," L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, Proc. 18th Int. Conf. World Wide Web (WWW), 2009, pp. 551–560.

The popularity of social networking sites has been rising steadily. Popular websites like Facebook have been reporting weekly growth rates of up to 3% (5). Millions of people have enrolled on various social networking sites, where they exchange photos, stay in touch, reconnect with long-lost acquaintances, and find new business relationships. In this study, we examine the ease with which a potential attacker may initiate automated crawling and identity theft assaults against many well-known social networking sites, therefore obtaining access to a substantial amount of private user data. The automated identity theft of active user accounts and the sending of friend invitations to the cloned victim's contacts constitute the first assault we describe. From the attacker's perspective, the goal is that the targeted people would just accept the friend request since they seem trustworthy. Through forging a friendship with a victim's connections, the attacker has access to the private information that the victim has shared. In our second, more sophisticated assault, we demonstrate that launching an automated, cross-site profile cloning attack is both practical and successful. With this approach, we may automatically contact the victim's friends who are enrolled on both networks and construct a forged profile in a network where the victim is not yet registered. Our real-user experiment results demonstrate the effectiveness and practicality of the automated assaults we provide.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Hand movement, orientation, and grip (HMOG), a collection of behavioral parameters to continually identify smartphone users, was presented by Sitova et al. [53]. Thermal imaging was utilized by Rajoub and Zwiggelaar [15] to track the thermal fluctuations in the periorbital area and investigate whether it might provide a discriminative signal for deceit detection. However, the majority of these biometric solutions need pricey gear, which makes them cumbersome and challenging to spread.

Abouelenien et al. [30] investigated a multimodal deception detection method that included many physiological, linguistic, and

thermal variables and was based on a unique dataset of 149 multimodal recordings. These pieces suggested that a user's activity patterns may serve as a representation of who they are. Many studies use the patterns of behavior of users to identify them. The development of behavior-based approaches came at a pivotal point and is useful for a variety of tasks, such as identifying and combating identity theft. User identifying and user profiling are the two stages that typically make up behavior-based user identification.

The technique of characterizing a user using behavioral data from their past is called user profiling. In order to determine the user profile, some works concentrate on statistical features like the mean, variance, median, or frequency of a variable. The challenge of identifying users by comparing the anonymous dataset's data histograms with the original dataset's histograms was examined by Naini et al. [55]. However, as various instances often have distinct features, it mostly depended on the expertise of professionals.

A behavior-based approach to detect breaches of certain high-profile accounts was put out by Egele et al. [7]. It did, however, need high-profile accounts, which were hard to come by.

Other studies found other characteristics to characterize user identification, including topic and regional distributions, tracing patterns, and user identity. In order to research online user behavior, Ruan et al. [32] gathered and examined user clickstreams from a popular OSN. In order to determine which users are active, Lesaege et al. [31] created a topic model that extended the LDA. A principal component analysis (PCA)-based method was introduced by Viswanath et al. [56] that effectively predicted the "like" behavior of typical Facebook users and distinguished notable departures from it as abnormal behaviors. An innovative method for gathering internet news articles and reporting on identity theft was suggested by Zaeem et al. [33]. The MKDE model was introduced by Lichman and Smyth [48] in order to precisely describe and forecast the spatial distribution of an individual's events.

Tsikerdekis and Zeadally [57] introduced an identity deception detection technique based on nonverbal behavior that works with a variety of social media platforms. The aforementioned techniques seldom considered using multidimensional behavior data and instead focused primarily on one dimension of the composite behavior. Sekara et al.'s investigation [58] of the intricate relationship between social and geographic behavior revealed that social behavior is highly predictable. It suggested that one's identity may be determined by composite behavior traits.

In order to forecast user behavior, Yin et al. [42] suggested a probabilistic generative model that combines the usage of spatiotemporal data with semantic information. POISED, a system that uses the variations in message propagation between benign and malicious on social networks to distinguish spam and other undesired information, was introduced by Nilizadeh et al. [49]. According to these research,

composite behavior traits may be useful for user identification.

Disadvantages

The LDA model does not perform well in either dataset, which suggests that the quality of the data has a significant impact on the model's performance.

2) When comparing the Yelp dataset to the Foursquare dataset, the CF-KDE and LDA models perform poorly; however, the fused model [17] notices an unexpected reversion.

3) A combined model that utilizes the relative anomalous score The model based on the logarithmic anomalous score Sl is outperformed by Sr.

4) The joint model is in fact better than the fused model (i.e., JOINT-SR, the joint model in the system's subsequent material all relate to the joint model based on Sr).

Proposed System

In this paper, we provide a method for identifying identity theft that makes use of multidimensional behavioral data, which may not be adequate in every dimension. We choose the online social network (OSN) as a representative situation based on these features, where the majority of users' activities are coarsely recorded [39]. Users' behaviors in the Internet age are a mixture of their social, offline, online, and perceptual/cognitive activities. Numerous applications, including offline check-ins in location-based services (LBSs), online tip-posting in instant messaging services, and social relationship-building in online social services, may gather behavioral data. As a result, we base the design of our technique on the composite behaviors of users across these categories.

Because of the challenges of data collection, user privacy requirements, and the fact that some users have multiple behavioral records, the user behavioral data in OSNs that can be used for online identity theft detection are frequently too low-quality or restricted to build qualified behavioral models. Our focus is on demonstrating that multidimensional behavioral data may be used to create a high-quality (quick-responding, resilient, and effective) behavioral model, even when the data is severely lacking in each dimension.

Advantages

In order to properly use coarse behavioral data, we suggest a joint model called CBM that can capture both online and offline elements of a user's composite behavior.

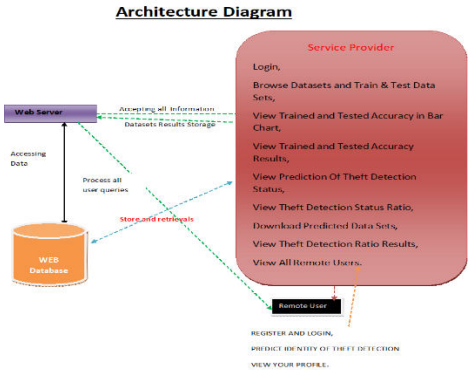
2) To achieve real-time identity theft detection, we develop a relative anomalous score Sr to quantify the frequency of recurrence of each composite behavior.

3) We conduct tests on two real-world datasets to show that CBM works. The results demonstrate how well our model works in comparison to the current models and how responsive it is.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

IV. SYSTEM DESIGN

System Architecture



V. MODULES

Service Provider

The Service Provider must provide a valid user name and password to log in to this module. Following a successful login, one may do a number of tasks, including Look Through Datasets and Test & Training Data Sets, See the results of trained and tested accuracy, see the ratio of theft detection status to the prediction of the status, view the trained and tested accuracy in a bar chart, download the predicted data sets, View All Remote Users and Theft Detection Ratio Results.

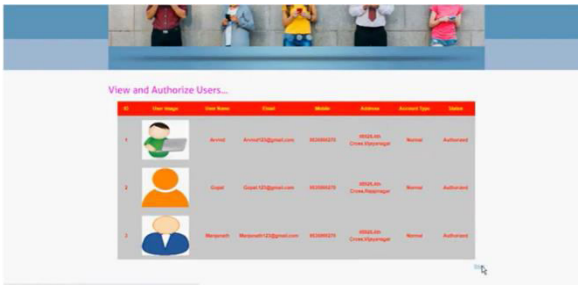
View and Authorize Users

The administrator may see a list of all enrolled users in this module. The administrator may see user information here, including name, email address, and address, and they can also approve people.

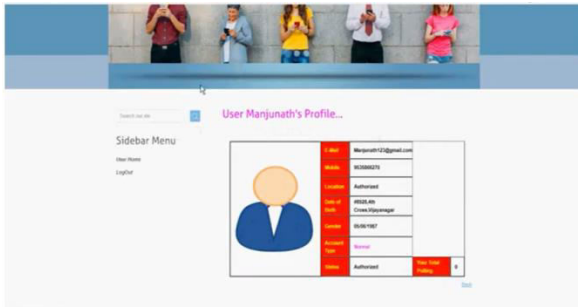
Remote User

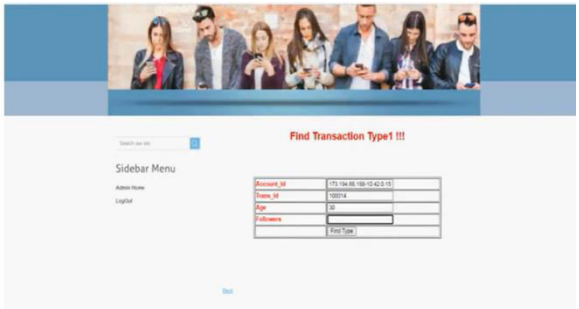
There are n numbers of users present in this module. Prior to beginning any actions, the user must register. The user's information is saved in the database when they register. Upon successful registration, he must use his permitted user name and password to log in. Upon successful login, the user may do several tasks such as registering and logging in, predicting the identity of theft detection, and seeing their profile.

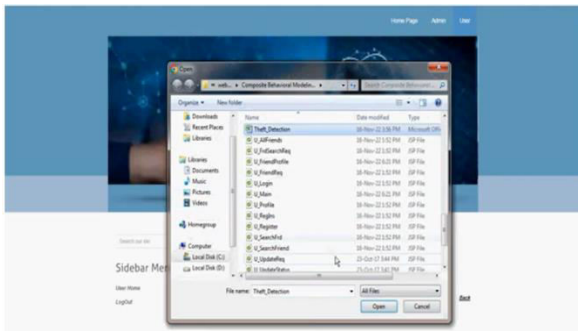
VI. RESULTS

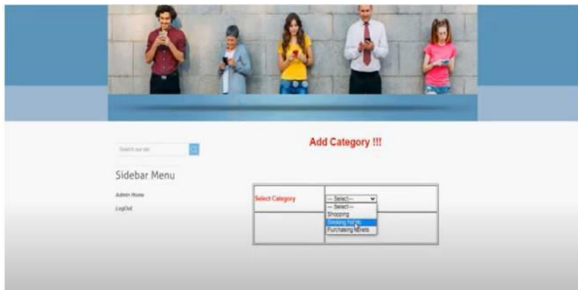


International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362









VII. CONCLUSION

We examine if it is possible to employ high-quality behavioural data rather than low-quality behavioural data to create an efficient behavioural model for user identification in OSNs. We combine online and offline behaviours to produce a thorough probabilistic generative model by fully using the complementary effect among the multifaceted activities of OSN users. Extensive trials on real-world OSN datasets demonstrate the combined model's overall success in detecting identity theft in OSNs in terms of detection effectiveness, reaction latency, and resilience. In particular, the joint model performs noticeably better than the current fused model.

Our behavior-based approach's primary goal is to identify identity thieves once the account's access control has been compromised. Then, combining our

approach with other tried-and-true tactics to more effectively prevent identity theft is simple and promising.

REFERENCES

[1] J. Onaolapo, E. Mariconti, and G. Stringhini, "What happens after you are pwnd: Understanding the use of leaked Webmail credentials in the wild," in *Proc. Internet Meas. Conf.*, Nov. 2016, pp. 65–79.

[2] A. Mohan, "A medical domain collaborative anomaly detection framework for identifying medical identity theft," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, May 2014, pp. 428–435.

[3] Y.-A. de Montjoye, L. Radaelli, V. K. Singh, and A. S. Pentland, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221, pp. 536–539, Jan. 2015.

[4] P. Hyman, "Cybercrime: It's serious, but exactly how serious?" *Commun. ACM*, vol. 56, no. 3, pp. 18–20, Mar. 2013.

[5] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *Proc. 18th Int. Conf. World Wide Web (WWW)*, 2009, pp. 551–560.

[6] J. Lynch, "Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks," *Berkeley Technol. Law J.*, vol. 20, no. 1, pp. 259–300, 2005.

[7] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 4, pp. 447–460, Jul. 2017.

[8] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory," *J. Res. Crime Delinquency*, vol. 47, no. 3, pp. 267–296, Aug. 2010.

[9] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 447–462.

[10] H. Li *et al.*, "Bimodal distribution and co-bursting in review spam detection," in *Proc. 26th Int. Conf. World Wide Web*, Apr. 2017, pp. 1063–1072.

[11] A. M. Marshall and B. C. Tompsett, "Identity theft in an online world," *Comput. Law Secur. Rev.*, vol. 21, no. 2, pp. 128–137, Jan. 2005.

[12] B. Schneier, "Two-factor authentication: Too little, too late," *Commun.ACM*, vol. 48, no. 4, p. 136, Apr. 2005.

[13] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1618–1629, Jul. 2016.

[14] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric recognition in automated border control: A survey," *ACM Comput. Surv.*, vol. 49, no. 2, p. 24, 2016.

[15] B. A. Rajoub and R. Zwiggelaar, "Thermal facial analysis for deception detection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 1015–1023, Jun. 2014.

[16] M. M. Waldrop, "How to hack the hackers: The human side of cybercrime," *Nature*, vol. 533, no. 7602, pp. 164–167, May 2016.

[17] C. Wang, B. Yang, J. Cui, and C. Wang, "Fusing behavioral projection models for identity theft detection in online social networks," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 4, pp. 637–648, Aug. 2019.

[18] C. Shen, Y. Li, Y. Chen, X. Guan, and R. A. Maxion, "Performance analysis of multi-motion sensor behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 48–62, Jan. 2018.

[19] C. Wang and H. Zhu, "Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services," *IEEE Trans. Dependable Secure Comput.*, early access, May 4, 2020, doi: 10.1109/TDSC.2020.2991872.

[20] H. Zheng *et al.*, "Smoke screener or straight shooter: Detecting elite sybil attacks in user-review social networks," in *Proc. 25th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2018, pp. 259–300.