GSTF Journal on Computing (JOC)
DOI: 10.5176/2251-3043_4.4.348
ISSN:2251 - 3043 ; Volume 5, Issue 1; 2016 pp. 21-28

Adaptive Behavioral Profiling for Identity Verification in Cloud Computing: A Model and Preliminary Analysis

Burhan Al-Bayati[1, 2], Nathan Clarke[1, 3], Paul Dowland[1]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]Computer Science Department, Science College, Diyala University, Diyala, Iraq
[3]Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia
burhan.al-bayati@plymouth.ac.uk

***Abstract*— In the past few years, cloud computing has become a new paradigm for hosting and delivering services over the Internet. Customers can directly access the resources (hardware and software) of cloud computing services over the Internet without the need to have specific knowledge about the resources. This flexibility has also made cloud services more vulnerable to potential attack. A key issue is that the cloud services rely upon a simple authentication login and remain accessible to users afterward for significant periods of time. This makes cloud computing services vulnerable to misuse. Well-known service providers including Dropbox (2012) and Apple (2014) have suffered from attacks, leading to sensitive information of their customers being exposed. As a result, there is a growing need for increasing the trust among end-users and cloud service providers and to be able to continuously monitor users to identify potential misuse. User behavior profiling is one technology that has been applied with various technologies/services to provide continuous re-authentication of a user transparently in order to monitor and improve the security of a system. This paper investigates the current state of the art in this approach and examines its applicability within cloud services. A preliminary experiment is undertaken using Dropbox log data to explore the feasibility of the approach within this type cloud service. The initial analysis of the proposed approach is very encouraging and provides the basis for proposing a novel multi-level behavioural profiling architecture.**

Keywords—Verification; continuous identity verification; transparent; behavior profiling; cloud computing services

I. Introduction

Cloud computing has become widely popular with it ranked as the first among the top 10 greatest global technology paradigms in recent years [1]. Google, Microsoft, Oracle, and Amazon are examples of the most popular cloud providers and service providers. The growth of this technology has made the number of worldwide subscribers of cloud services increase rapidly [2]. By using cloud computing services, customers can build and run projects, browse and buy products, send and receive email, store confidential information, transfer money, communicate with friends, and watch videos through web applications over the Internet; which give customers the flexibility, efficiency, cost effectiveness, easy deployment and on-demand services [3], [4]. As a result, many different commercial companies such as Netflix, eBay, Xerox, Etsy and Apple have decided to shift their products into cloud computing services by renting resources from Cloud Service Providers (CSP) [5], [6].

The Cloud Industry Forum (CIF) reported that 79% of UK businesses used at least one of the cloud computing services in 2014 [7]. Additionally, the money spent on cloud computing services has increased, U.S. businesses spent approximately $13 billion on cloud systems and managed hosting services in 2014 [8]. It was also reported that customers utilizing services that are supported by cloud services would spend more than $180 billion by 2018.

There is no doubt that the flexible and convenient facilities of cloud computing services have changed our daily lives (whether people are aware of it or not); however, the biggest barrier that hinders the development and widespread use of cloud computing services are the security issues [9]. These security issues cause challenges both commercially and technologically. Although many security mechanisms have been developed to reduce security related risks (e.g. being hacked), service providers and customers are still concerned about cybercrime and misuse of cloud services [10].

Dropbox, one of the most popular cloud services providers, faced hacking activities in 2012 where stolen usernames and passwords of many users from other websites were tested on Dropbox and the attacker was able to hack many of customers' accounts [11]. More recently, many Apple iCloud accounts were hacked (2014), resulting in personal photographs of the Apple customers, specifically celebrities, being leaked online. Apple claimed that there was no vulnerability in their online system; the accident was due to the hackers targeting and bypassing the authentication process of the Apple iCloud. It was reported that more than 20,000 passwords were stolen which caused the breaching of Apple's customers data [12].

It is clear from these incidents that cybercriminals can obtain access to sensitive information even though security controls were in place and dedicated security teams allocated. Therefore, it is important to build further security techniques to secure the cloud base system from being compromised. Being able to monitor user interactions and identify account misuse would significantly reduce the threat posed by hackers.

This paper investigates the current state of the art in the user behavior profiling and examines its applicability within cloud services. The paper continues to present a preliminary experiment by using Dropbox log data to explore the feasibility

of the approach within cloud services. The initial analysis of the proposed approach is very encouraging and provides the basis for proposing a novel multi-level behavioral profiling architecture.

II. Related work

A variety of studies have examined user behavior profiling from numerous perspectives, including marketing, intrusion detection, fraud detection, and authentication. The technique is utilized to verify a user by tracking and storing the previous user activities, creating a user profile template(s) based upon them, and then comparing current user activities with the historical behaviorial template in order to make appropriate decision of legitimate/illegitimate usage. This mechanism, therefore seeks to increase the security level after the login, by transparently re-authenticating users throughout the session. This leads to a continuous and non-intrusive authentication approach. Behavioral profiling has been published with different technologies, i.e. mobile phone system, network, computer system, and web browsing. In IDS literature, this is often referred to as anomaly detection' however, the focus upon the individual, rather than normal versus misuse profiles makes it more appropriate to the field of biometrics than IDS.

Around 1997, researchers started to study the possibility of applying user behavior profiling to support and provide a high-level security for mobile networks. The earliest research on mobile phones focused mainly on IDS and fraud detection based on identifying the user behavior activities during the interaction with mobile's services, such as calling and mobility [13]–[27]. However, more recent studies have focused on transparent authentication through modelling application usage to alleviate device misuse [28]–[33]. Much more information can be gathered from user activities while interacting with these applications (e.g. phone calls, GPS locations, SMSs, emails, websites visits, and calendar activities). These activities have been exploited to build an accurate behavioral profile which can be investigated to increase the accuracy level of the security system for the device or application itself.

From a client side (computer system) perspective, a number of researchers have focused on the generation of user behavior profiles from device usage and file access activities to detect any illegal access of the computer system [34–36]. Many features have been involved to build user behavior profiles in the computer system. For instance, the way in which a user interacts with their computer, which applications were used, how frequent a user is accessing their files and information and when, together with which websites were visited.

From a server side perspective, a number of studies have investigated the ability to build a user identifier by using user web surfing activities from numerous log files of websites [37], [38]. A user behavior profiling was based on spending time on various topics of the website, site names, number of pages, starting time and duration time of sessions.

From the aforementioned related work, most of these studies have utilized behavioral profiling with mobile, computer, web browsing which acquired various encouraging accuracy results. Table 1 shows the short summery of all related works that were mentioned previously.

Table 1: Rated behavioral profiling studies

	Author(s)	Activity	Client/Server	#Participants	Performance (%)	Purpose
1	[13]	Telephony	Server	600	DR=90, FALR=10	Fraud detection
2	[14]	Telephony	Server	110	DR=75,FALR=40	Fraud detection
3	[15]	Mobility	Server	400	DR=82.5,FALR=40	Fraud detection
		Telephony			DR=80,FALR=30	
4	[16]	Mobility	Server	None	DR=87.5	IDS
6	[17]	Mobility	Server	None	DR=87.5,FALR=15	IDS
7	[18]	Mobility	Server	None	DR=89,FALR=13	IDS
8	[19]	Mobility	Server	50	DR=50,FALR=50	IDS
9	[20]	Telephony	Server	5000	DR=80	Fraud detection
10	[21]	Telephony	Server	5000	DR=80	Fraud detection
11	[22]	Telephony	Server	5000	DR=80	Fraud detection
12	[23]	Telephony	Server	180	FAR=3	Fraud detection
13	[24]	Telephony	Server	300	DR=70	Fraud detection
14	[35]	Mobility	Server	100	DR=81	IDS
15	[26]	Mobility	Server	178	DR=94	IDS
16	[27]	Telephony	Server	94	DR=97	Fraud detection
17	[28]	Telephony, SMS, Browsing,Mobility	Client	50	DR=95	Authentication
18	[29]	Telephony, SMS, Browsing	Client	35	DR=98.5,EER=1.6	Authentication
19	[30]	Telephony, Device Usage, Bluetooth network scanning	Client	30	EER=13.5, 35.1,and 35.7	Authentication
20	[31]	Application, Telephony, SMS	Client	#76	EER=13.5, 2.2, 5.4	Authentication
21	[32]	Application Usage	Client	76	EER=9.8	Authentication
22	[33]	Text, App, Web and location	Client	200	EER=3	Authentication
23	[34]	Way of using PC	Client	21	EER= 7	Authentication
24	[35]	File access activity and network event	Client	8	DR=90, FAR=14, FRR=11	Authentication
25	[36]	File access activity	Client	18	FAR=1.1	Insider detection
26	[37]	Web Browsing	Server	100	DR=91	Identification
27	[38]	Web Browsing	Server	10	EER= 24	Authentication

*FALR=False Alarms Rate, EER=Equal Error Rate, DR=Detection Rate, TPR=True Positive Rate, FAR=False Accept Rate, FRR=False Reject Rate

The accuracy results in Table 1 show that behavioral profiling can be used to improve the user authentication. However, little research has been published on using this technique to improve the security of cloud computing services. The majority of these studies are merely theoretical without any practical experimental results which researchers cannot rely fully on them to develop a new technique–only one study was practical [39]. In [39] the authors introduced an approach to manage the challenges and limitations in traditional monitoring and intrusion detection techniques when switched to the cloud. They focused on auditing the security of cloud infrastructure service through monitoring the suspected change in the resources. Autonomic multi-agents and behavior analysis techniques are utilized for auditing an incident detection system, which is called Security Audit as a Service (SAaaS). This security service is placed inside VMs to collect and analyze the information of these VMs such as frequent

infrastructure changes. The aim of their study is to increase cloud security continuously and transparently by informing the users about the security incidents of data access and also increase the user's trust in cloud services. A normal behavior for VMs was generated such as the time of start, stop, and delete events of VMs. When these behaviors deviate from the historical behaviors, an alert can be generated and forwarded to the user. Additionally, tenants can access all information details to check status events of their services which were gathered by a security dashboard.

However, this work has several problems. Firstly, although SAaaS is based on the use of multi-agents of sensors for collecting different events, the security policies of these sensors are received from Security Service Level Agreement (SSLA). Therefore, the security policy of the sensor is still dependent on rules that are pre-defined by SSLA, which means the detection range will be limited to the known attacks. Moreover, using a large number of agents (e.g. initiating agent, killing agent, and moving agent) might lead to increase the communication traffic between the agents and the computational become overhead [40]. In addition, the prototype is not yet validated for scalable environments because if tenants need to add new services or ask to protect from a specific type of attack, a problem may occur with autonomous agents. The reason for this problem is the configuration and development of these agents which is achieved at the beginning of the VM lifecycle. Therefore, there is a need to add global solutions for improving cloud security.

III. Behavior Profiling for Continuous Identity Verification in Cloud Computing Services

As there is an increase in the use of cloud computing services, there is a growing need for building trust between users and cloud providers. One of the main problems that lead to less confidence in cloud computing services is that they remain accessible after the initial login, making them vulnerable to misuse – particularly as the nature of the login is all too frequently abused. As seen in the related work, behavioral profiling has been utilized with various technologies transparently to protect their systems from different types of attack. Therefore, behavioral profiling could be utilized to increase the security level of cloud computing

Additionally, Microsoft and Google are examples of having multiple levels of cloud services (SaaS, PaaS, and IaaS), meaning a user can have different services within and between cloud service models. For example, a user can have an IaaS with Microsoft as a provider and the same user can utilize one or more SaaS services such as OneDrive and Microsoft office. These cloud service/application providers subsequently have access to a wider range of behavioural characteristics with which to model and develop a strong behavioral profile of the user. Therefore, an intelligent identity verification system is proposed that provides a multi-instance behavioral profiling model. The intelligent system needs to be operable in a modular fashion which means the system can effectively turn off/on the behavioural monitoring of services dependent on whether a single profile (service) is available or more. An advantageof the multi-instance system is that it provides a constructive capability where strong a strong behavioural profile on one service can offset a weaker profile on another. It can also be used to assist in the capturing and processing of initial training data to allow new service monitoring. In this way, the proposed system can improve the accuracy result and become more transparent.

Fig. 1 shows the novel architecture of user verification in cloud service provider based on different levels of user behavior profiles.

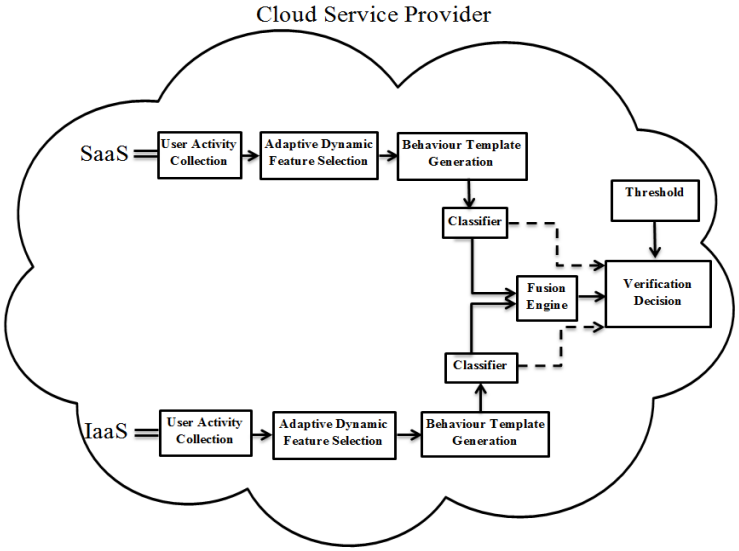

Fig. 1. A Novel Architecture of User Verification in the Cloud Service Provider

An outline description of the components is provided below:

- **User Activity Collection:** The main task of data collection process is to perform the collection and pre-processing of the user interaction data. All the required activities will be pre-processed to ensure privacy and stored in a database any normalization processes have been undertaken.
- **Adaptive Dynamic Feature Selection**: This is a key process which can apply an intelligent extraction model to create unique features from the collected dataset. Behavioural-based features tend to be particular noisy in terms of discriminative features. As such, this component will focus specifically on identifying a suitable set of features on a per user basis (rather than a more typical generic feature set for all users). The focus upon the user will enable a more robust classification system. A variety of features can be generated from user log file of user cloud services such as time, date of accessing, type of event, the name of application, CPU and memory usage, and the way of interaction with services. These selected features will be stored in a database (template). Moreover, the system should adapt easily to new conditions, evolving the features utilised.
- **Profile Template Generating**: In this process the data (samples) will be converted into a behavioural template which can further be utilized by classifiers. Templates can be created to store the new style of the samples.

Multi-samples might be generated for each user to improve the decision of the system.

- **Classifier**: An adaptive classifier(s) should be selected based on the nature of features or the number of these features because some classifiers can deal with a huge number of features better than others. Multi-algorithmic approaches will be implemented for each service to achieve a better performance.
- **Fusion Engine**: This engine will decide whether the system will rely on a single behavioral profile or multi-instance to make a decision. If the user has a single service (SaaS or IaaS), the engine can switch *off* one of these services and will depend fully on a single instance to make a decision. However, if the user has more than one service, the engine can switch *on* the multi-instance to make a final decision.
- **Verification Decision**: This is the component of the proposed system where the decision is made. Firstly, it can manage the score(s) that come(s) from classifier(s); if the score(s) is/are equal or closer to the specified threshold, the current user can be considered as a legitimate user; otherwise, a number of flags can be set before making a final decision. An intelligent decision support system will monitor both the output of the classifieds but also appreciate the context within which those samples were created. In doing so, a more reliable and confident decision can be made.

IV. PRELIMINARY ANALYSIS OF USER BEHAVIORAL PROFILING IN CLOUD COMPUTING SERVICES

As discussed in the related work, behavioral profiling have been utilized with different technologies such as mobile phone, web application, and computer system. This study presents a feasibility study of using the behavioral profiling technique to verify individuals within the cloud computing environment. The main aim of this study is to investigate the possibility of extracting unique features from the user interactions with various cloud services. Upon the creation of the features, user behavior profiles can then be generated which will be subsequently applied to provide continuous verification to ensure the legitimacy of the current user.

Whilst several popular cloud computing services could be chosen for a preliminary analysis, Dropbox was selected as it is one of the most widely used as a cloud storage service with more than 300 million registered customers in 2014 [41]. The following sections will discuss several features and then analyze their effectiveness towards the verification of a user. The purpose of this analysis was not to perform a full verification experiment but to provide an analysis of the potential feasibility of using cloud service log data to create behavioural profiles. As such, a limited number of participants (6) were invited to take part. A total of 3 months of log data was captured and extracted. Of particularly interest in the analysis are the intra- and inter-classes variances, which measure the similarity of users' samples and between users respectively. Ideally, the intra-class variance needs to be small with the inter-class variance large[42].

A. Data Collection

Due to the privacy and security concerns, it would be challenging to get a workable dataset from cloud computing service providers. Also, to the best of the author's knowledge, no public dataset on user's activities within cloud computing is available. These activities were collected by opening Dropbox accounts using a web browser followed by click on 'events' option and then highlighting and copying the required activities thereby pasted into a Microsoft Excel file. Therefore, the collected data contains real user activities that were recorded by the Dropbox service. Also, the data has been anonymized to protect the participants' privacy. Fig. 2 illustrates a sample of user activities with the dataset.

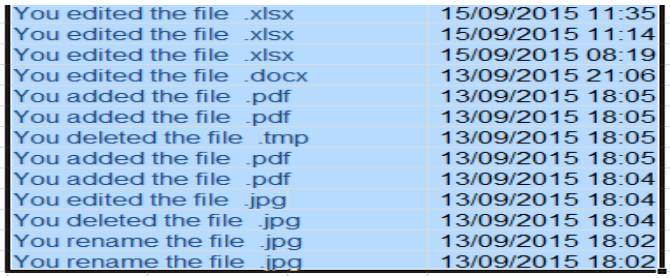

Fig. 2. User Activity with Dropbox

A number of activities were collected from historical usage of Dropbox users, such as add, delete, edit, move, and rename the file types being used, including documents, images, movies; andthe time and date stamp. All of these have the potential to be used towards the generation of the user behavioral profile. Table 1 below shows some of the main user activities which were extracted from the above figure.

Table 2: User Dropbox Activities

Activity	File Type	Time and Date Stamp
Edit	xlsx	15/09/2015 11:35
Edit	xlsx	15/09/2015 11:14
Edit	xlsx	15/09/2015 08:19
Edit	docx	13/09/2015 21:06
Add	pdf	13/09/2015 18:05
Add	pdf	13/09/2015 18:05
Delete	tmp	13/09/2015 18:05
Add	tmp	13/09/2015 18:05
Add	pdf	13/09/2015 18:04
Add	pdf	13/09/2015 18:04
Edit	jpg	13/09/2015 18:04
Delete	jpg	13/09/2015 18:04
Rename	jpg	13/09/2015 18:02

From Table 2, there are many approaches that can be used to investigate the variability of the extracted features. For example, some users access their Dropbox's accounts to read, or rename, or download files, whereas others might mostly edit, or upload files to their accounts. Moreover, these files can contain a variety of extensions (e.g. pdf, doc, xls, and jpg) which users might work with specific types of files. The date, time, and duration of the accessing might also be another factor can be used to discriminate the users from others. For example, when an impostor accesses other user's account, he/she may choose different types of operations which the owner might not use, or the date and time of accessing the account might be

different, such as detecting files after 12PM on Sunday, while the legitimate user might not utilize his/her Dropbox account at that time. Various users' activities within Dropbox can be investigated to discriminate between authorized and unauthorized users through positive and negative user behaviors that can be observed while interacting with the service.

Additionally, it can be difficult to build user behavior profiles from one or two interactions within a day of usage. Therefore, there is a need to know the number of these interactions/activities for the users. Table 3 below contains 14439 activities amongst the six users over the three-month duration.

Table 3: Dropbox events

Activity	Frequency
Add	4,683
Edit	8,876
Delete	496
Rename	291
Move	93
File Types	14439

B. Descriptive Statistics on Inter and Intra-Classes Variance

The preliminary feature analysis implemented a descriptive statistic approach to analyze and extract unique patterns to discriminate individuals presented by the dataset [43]. Selecting an effective or an optimum set of features is a critical and significantly important process because it will subsequently affect pattern classification and the performance of the system [44]. Based on the available dataset, two types of aspects have been considered in this analytical study on Dropbox: user events and file types.

In order to see the similarities and differences of usage amongst users, Table 15 shows the mean and standard deviation of events and file types for each user which was collected for 90 days of the user daily usage.

Table 4: Descriptive statistics of selected features

		Events		File Types						
Users		Add	Edit	jpg	pdf	doc	xls	m	asv	lyx
1	Mean	26.84	x	25.82	x	x	x	x	x	x
	Stdev.	16.62	x	16.32	x	x	x	x	x	x
2	Mean	4.16	14.11	x	4.21	12.09	x	x	x	x
	Stdev.	4.61	9.72	x	3.94	9.19	x	x	x	x
3	Mean	x	75.01	x	x	x	x	59.66	10.25	33.14
	Stdev.	x	64.36	x	x	x	x	58.87	9.42	34.70
4	Mean	x	5.01	x	x	x	4.49	x	x	x
	Stdev.	x	4.49	x	x	x	4.39	x	x	x
5	Mean	4 . 8	7.58	x	x	7.05	4.65	x	x	x
	Stdev	4.25	6.29	x	x	5.89	4.70	x	x	x
6	Mean	9.32	x	8.30	x	x	x	x	x	x
	Stdev.	6.62	x	6.16	x	x	x	x	x	x

From an inter-classes variance perspective, Table 4 shows that User 1, User 2, User 5, and User 6 shared the 'Add' event. However, there are considerable differences between these users. For instance, the mean and standard deviation of User 1 and User 6 are different which could provide a degree of discrimination for a classifier to distinguish them. Moreover, User 1 and User 6 shared the same file type (jpg), but also the mean and standard deviation are considerably different. A concern exists with User 2 and 5 because they have identical mean and standard deviation of using 'Add' event.

However, analyzing other features reveals users 2 and 5 have different mean and standard deviation for file type (doc) as well as each user used a different file type and different frequency. User 2 has a unique usage for file type (pdf). Therefore, these users can be recognized easily based on these two features. Similarly, User 2, User 3, User 4, and User 5 have also shared the 'Edit' event, but User 2 and User 3 are different from other in the average usage. Additionally, User 3 deals with a variety of file types (m, asv, and lyx) which are different from all other users.

The analysis does show a potential problem with User 4 and User 5 because they have quite close usage of event type (Edit) and file type (xls) which will affect accuracy of system decision. This problem of similarity of usage between User 4 and User 5 can be managed however when looking across the range of actions and file types. However, there is a significant difference in the use of useful especially type (.doc) with User 4 not using them at all.

Upon further analysis across the 90-day period, the figures below can also show clearly the all aspects which have discussed previously about the inter-class variance.

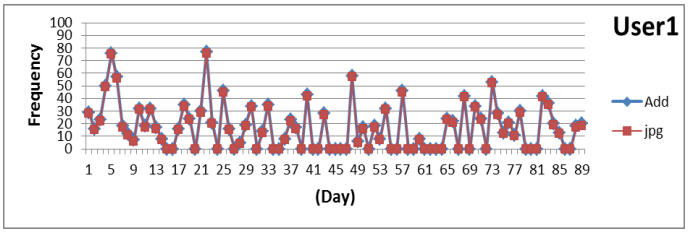

Fig. 3. Daily usage of User 1

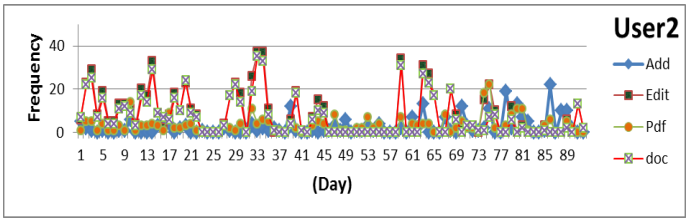

Fig. 4. Daily usage of User 2

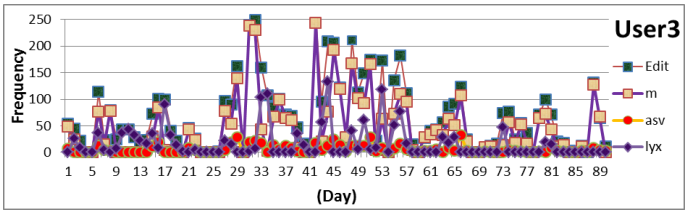

Fig. 5. Daily usage of User 3

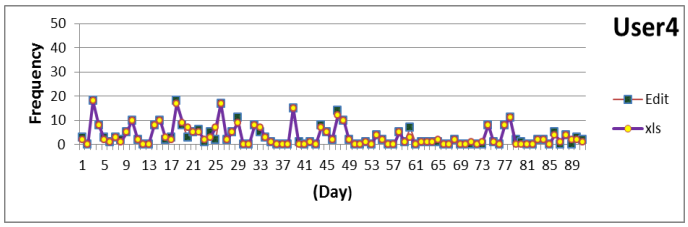

Fig. 6. Daily usage of User 4

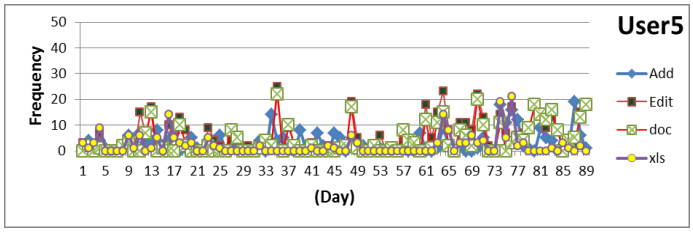

Fig. 7. Daily usage of User 5

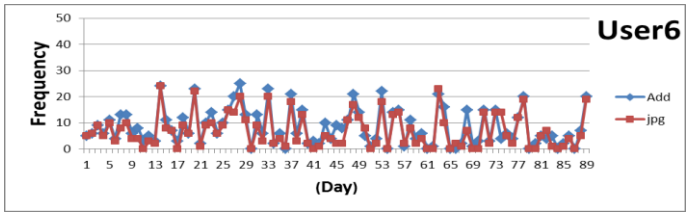

Fig. 8. Daily usage of User 6

Additionally, the above figures also illustrate the pattern of similarity usage for each user (intra-classes variance). For example, Fig. 3 and Fig. 8 shows that although User 1 has slightly unstable usage, it can be recognized through his/her frequency of usage which is stable between "10-60" for the event and file type; whereas User 6 which has a similar usage with User1 can be recognized by range "5-10".

Additionally, Fig. 5 demonstrated that User 3 has a different frequency of usage over the three months. However, this user can be recognized through file types because he/she does not share file types (m, asv, and lyx) with all other users. More importantly in this case, an adaptive behavioral profile can be built for this user as User 3 has a similar usage over the first and third month, but the average of usage of the second month was increased. Therefore, the usage might increase or decrease base on the user usage. Moreover, an adaptive feature selection can also increase the accuracy of a classifier because the activity of users might be changeable over time.

Fig. 4 demonstrates that User 2 has some attributes were not comparable over the selected period such as the 'Add' event and file type (pdf), whereas others were stable such as the 'Edit' event and file type (doc). However, Fig. 6 shows that the similarity of User 4 usage remained quite consistent over the chosen period which can be helped to build an efficient profile. Similarly, Fig. 7 illustrated that the User 5 has also comparable pattern of usage for events and file types.

V. Discussion

From the above analysis, inter and intra classes variance are apparent. Each user has different activity (behavior) on Dropbox from other users and the similarity patterns of usage over the chosen period for the most users were a quite stable. Therefore, an efficient user behavior profiles could be generated for cloud users which will play a significant role in discriminating users. As a result, the behavioral profiling technique could be employed to verify the legitimate user and improve the security level of cloud computing services. However, there is a range of further issues might face this technique which needs to be resolved in order for the proposed system to operate effectively.

Firstly, the main problem with the behavioral profiling techniques is the stability; users might change their behaviors over time which might affect the accuracy of a system. For instance, User 2, 3 and 5 have unstable frequencies of usage which will make a classification more challenging. This type of problem the proposed system can solve by the dynamic adaptive features through renewing templates on a continual basis. As a result, the most recent users' activities can be involved which will increase the accuracy decision of the proposed system. However, this is not an easy task because the renewing template might include the illegitimate usage which an impostor might be accepted by the system over time as the genuine user. The multi-instance approach will aid in providing an additional protection measure against the capture of illegitimate usage.

The similarity of usage among users could be another problem. Therefore, the system should take into account to select more other features or multi-instances (i.e. more than one pattern from the same user in different times) for each user which can increase the degree of the discrimination between the users and reduce the violation to the system by other users or attackers. All these factors will lead to a reduction in the error rate (EER) and increase the accuracy of system decision which needs to be considered in our proposed system.

Scalability is another consideration – whilst it has been shown that a level of discrimination exists between 6 users, can the same be said for large number of users. One aspect to offset this problem is through the use of classifier which will handle the data in a multidimensional space (rather than two dimensions when performing descriptive statistics). However, further work will need to undertaken focussing upon measuring the equivalent feature spaces available in this approach.

From an end-user perspective, privacy is a key factor which should be considered in any system deals with user information. In our system, data collection and user samples must be achieved in a manner that minimizes the risk of misuse of the information. Therefore, the architecture of the system must be appropriately designed to make sure the opportunity of accessing the user information is only possible by authorized individuals. However, whilst the system will be built in the cloud service provider side where which the user information already exists, the aspect of privacy would raise less concern.

VI Conclusions and Future Work

As there are an increasing number of cloud-computing services, there is an increasing level of concern with regards to the misuse of these services. Therefore, there is a need to provide a universal solution that will ensure Cloud

Application/Service Providers have additional approaches to detect and monitor misuse to better protect their end-users.

This paper has proposed a multi-instance behavioral profiling framework and discussed its core components and operation. The framework is able to provide continuous identity verification in cloud computing services through monitoring user application activities.

The results from the experimental analysis were encouraging, demonstrating that users' interactions with their cloud service are indeed discriminatory. However, further work needs to be undertaken to measure the discriminative value of the feature set.

To focus on increasing the number of participants and the volume of data to acquire a larger and more reliable dataset; and, to identify the dynamic and adaptive feature selection algorithm to aid in maximising performance.

REFERENCES

[1] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.

[2] Forbes, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2015," 2015. [Online]. Available: http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/. [Accessed: 27-Apr-2015].

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," Natl. Inst. Stand. Technol. Inf. Technol. Lab., vol. 145, p. 7, 2011.

[4] A. Prasanth, M. Bajpei, V. Shrivastava, and R. G. Mishra, Cloud Computing : A Survey of Associated Services Cloud Computing : A Survey of Associated Services, vol. 13. 2015.

[5] SmartDataCollective, "Companies Who Have Moved to the Cloud | SmartData Collective," 2013. [Online]. Available: http://smartdatacollective.com/gilallouche/145341/7-well-known-companies-have-moved-cloud. [Accessed: 27-Apr-2015].

[6] ebay inc, "BREAKING: eBay and Microsoft Announce Cloud Computing Agreement #WPC10 - eBay InceBay Inc," 2010. [Online]. Available: http://blog.ebay.com/breaking-ebay-and-microsoft-announce-cloud-computing-agreement-wpc10/. [Accessed: 27-Apr-2015].

[7] Data Clarity Limited, "Cloud computing is moving into mainstream businesses," 2015. [Online]. Available: www.clarity365.co.uk. [Accessed: 13-Apr-2015].

[8] L. T. Stephane Come, CTO, "LCS Technologies Projects Top Five Tech Trends to Watch in 2015 - THE SARTA BLOG," 2015. [Online]. Available: http://sarta.org/blog/lcs-technologies-projects-top-five-tech-trends-to-watch-in-2015/. [Accessed: 13-Apr-2015].

[9] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," Commun. Surv. Tutorials, IEEE, vol. 15, no. 2, pp. 843–859, 2013.

[10] T. Chou, "Security threats on Cloud Computing vulnerabilities," Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 3, pp. 79–88, 2013.

[11] S. Gupta, P. Kumar, and A. Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment," Int. J. Distrib. Sens. Networks, vol. 2013, no. 2, pp. 1–12, 2013.

[12] U. Gupta, "Survey on security issues in file management in cloud computing environment," vol. 2, no. 11, p. 5, 2015.

[13] J. Moreau Y., Verrelst, H., Vandewalle, "Detection of Mobile Phone Fraud Using Supervised Neural Networks: a First Propotype," in International Conference on Artificial Neural Networks. Springer Berlin Heidelberg, 1997.

[14] P. Burge and J. Shawe-Taylor, "Detecting Cellular Fraud Using Adaptive Prototypes," in Proc of AI Approaches to Fraud Detection and Risk Management, 1997, pp. 9–13.

[15] D. Samfat and R. Molva, "IDAMN: an intrusion detection architecture for mobile networks," IEEE J. Sel. Areas Commun., vol. 15, no. 7, pp. 1373–1380, 1997.

[16] R. Buschkes, D. Kesdogan, and P. Reichl, "How to increase security in mobile networks by anomaly detection," in Proceedings 14th Annual Computer Security Applications Conference (Cat. No.98EX217), 1998.

[17] B. Sun, F. Yu, K. Wu, and V. C. M. Leung, "Mobility-based anomaly detection in cellular mobile networks," Proc. 2004 ACM Work. Wirel. Secur. - WiSe '04, p. 61, 2004.

[18] Z. W. R. Y. F. Sun B; Chen, "Towards adaptive anomaly detection in cellular mobile networks," in CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006., 2006, vol. 2, pp. 666–670.

[19] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," WiMob'2005), IEEE Int. Conf. Wirel. Mob. Comput. Netw. Commun. 2005., vol. 2, pp. 17–24, 2005.

[20] C. S. Hilas and J. N. Sahalos, "User Profiling for Fraud Detection in Telecommunication Networks," in 5th International Conference on Technology and Automation, 2005.

[21] C. Hilas and J. Sahalos, "An application of decision trees for rule extraction towards telecommunications fraud detection," Lect. Notes Comput. Sci., vol. 4693, no. 2, pp. 1112–1121, 2007.

[22] C. Hilas, S. Kazarlis, I. Rekanos, and P. Mastorocostas, "A genetic programming approach to telecommunications fraud detection and classification," Proc. 2014 Int. Conf. Circuits, Syst. Signal Process. Commun. Comput., pp. 77–83, 2014.

[23] F. Ogwueleka, "Fraud Detection In Mobile Communications Networks Using User Profiling And Classification Techniques," J. Sci. Technol., vol. 29, no. 3, pp. 31–42, 2009.

[24] S. Qayyum, S. Mansoor, A. Khalid, Z. Halim, and A. R. Baig, "Fraudulent call detection for mobile networks," 2010 Int. Conf. Inf. Emerg. Technol., pp. 1–5, 2010.

[25] S. Yazji, R. P. Dick, P. Scheuermann, and G. Trajcevski, "Protecting Private Data on Mobile Systems based on Spatio-temporal Analysis," 2011.

[26] S. Yazji, P. Scheuermann, R. P. Dick, G. Trajcevski, and R. Jin, "Efficient location aware intrusion detection to protect mobile devices," Pers. Ubiquitous Comput., vol. 18, no. 1, pp. 143–162, 2014.

[27] S. Subudhi and S. Panigrahi, "Quarter-Sphere Support Vector Machine for Fraud Detection in Mobile Telecommunication Networks," Procedia Comput. Sci., vol. 48, no. Iccc, pp. 353–359, 2015.

[28] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6531 LNCS, pp. 99–113, 2011.

[29] M. P. Dimitrios Damopoulos, Sofia A. Menesidou, Georgios Kambourakis and N. C. and S. Gritzalis, "Evaluation of anomaly- based IDS for mobile devices using machine learning classifiers," Secur. Commun. Networks, vol. 5, no. 1, pp. 3–14, 2012.

[30] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling on mobile devices," Proc. - EST 2010 - 2010 Int. Conf. Emerg. Secur. Technol. ROBOSEC 2010 - Robot. Secur. LAB-RS 2010 - Learn. Adapt. Behav. Robot. Syst., no. 2010, pp. 77–82, 2010.

[31] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Misuse Detection for Mobile Devices Using Behaviour Profiling," Int. J. Cyber Warf. Terror., vol. 1, no. 1, pp. 41–53, 2011.

[32] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," Int. J. Inf. Secur., vol. 13, no. 3, pp. 229–244, 2014.

[33] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active Authentication on Mobile Devices via Stylometry , Application

Usage , Web Browsing , and GPS Location," pp. 1–10, 2015.

[34] A. Aupy and N. Clarke, "User Authentication by Service Utilisation Profiling," Adv. Netw. Commun. Eng. 2, p. 18, 2005.

[35] S. Yazji, X. Chen, R. P. Dick, and P. Scheuermann, "Implicit user re-authentication for mobile devices," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5585 LNCS, pp. 325–339, 2009.

[36] M. Ben Salem and S. J. Stolfo, "Modeling user search behavior for masquerade detection," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6961 LNCS, pp. 181–200, 2011.

[37] Y. Yang, "Web user behavioral profiling for user identification," Decis. Support Syst., vol. 49, no. 3, pp. 261–271, 2010.

[38] M. Abramson and D. Aha, "User Authentication from Web Browsing Behavior," Twenty-Sixth Int. FLAIRS Conf., pp. 268–273, 2013.

[39] F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke, "An agent based business aware incident detection system for cloud environments," J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, p. 9, 2012.

[40] I. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," Computers, vol. 3, no. 1, pp. 1–35, 2014.

[41] Statista, "• Dropbox number of registered users 2011-2014 | Statistic," 2015. [Online]. Available: http://www.statista.com/statistics/261820/number-of-registered-dropbox-users/. [Accessed: 14-Apr-2015].

[42] J. Daugman, "Face and Gesture Recognition: Overview," Pattern Anal. Mach. Intell. IEEE Trans., vol. 19, no. 7, pp. 675–676, 1997.

[43] R. Sallehuddin, S. Ibrahim, A. M. Zain, and A. H. Elmi, "Detecting SIM box fraud by using support vector machine and artificial neural network," J. Teknol., vol. 74, no. 1, pp. 137–149, 2015.

[44] M. H. Nguyen and F. de la Torre, "Optimal feature selection for support vector machines," Pattern Recognit., vol. 43, no. 3, pp. 584–591, 2010.