Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 434 – 445

Procedia Computer Science

The Third Information Systems International Conference

A Secure Mobile App Solution Using Human Behavioral Context and Analytic Hierarchy Process

Salmah Mousbah Zeed Mohammed, Azizul Rahman Mohd, Manmeet Mahinderjit Singh

The School of Computer Sciences, University Sains Malaysia, Penang Malaysia

salmah.mousbah@gmail.com, azizul, manmeet@ usm.my

Abstract

Mobile devices have gained popularity worldwide. The mobile device flexibility has encouraged users to turn their mobile devices into primary hubs for storing information. This paper adopts the classical CW-Lite security models as the framework and the human behavioral patterns as the context. The selected behavioral aspects refer to mobile application and mobility, deployed as major characteristics that determine security control decisions. This proposed paper requires the application of human behavioral context on mobile phones. The solution involves the novel use of behavioral aspects to improve the security of mobile phones. Two important scenarios are incorporated: analytic hierarchy process (AHP) mobile application and AHP mobility. The proposed methodology is superior because it can detect the change in the user behavior in comparison with an intruder. The applied intelligent human behavioral context on the CW-Lite model shows the advantages of AHP in detecting the changes in the user behavior and in authenticating the identity of the main user. These advantages ensure reliability and security of the phone.

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)

Keywords: User authentication; CW-Lite security model; Analytic Hierarchy Process (AHP) for decision making

1. Introduction

With the widespread use of the mobile system and the continuous evolution of technology, the mobile device has been used for storing confidential data as well as for sending and receiving e-mails. Authentication ensures that access to the phone is given to an authorized individual. With the present technology, the integrity of passwords has been compromised because passwords are easily accessible and susceptible to unauthorized access. The most common method used for authentication is text password. Studies have shown that users tend to use short passwords for easy recollection [1].

The Appslock and Lock Timer applications require users to set a preferred password before such applications can be used. These applications have no capability of learning user behavior to perform automated system log-off and solely depend on passwords to access private information. Owing to this development, the analysis of human behavior in relation to mobile phones has received considerable interest, particularly in the areas of recording call logs, Bluetooth devices in proximity, cell tower IDs, application usage, and phone status. Location inferred from cell tower data [2] [3] can be recorded by mobiles. Phone operators offer the possibility of large-scale analysis of

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)
doi:10.1016/j.procs.2015.12.124

human mobility, including prediction of human mobility [4] or daily activity patterns of humans identification [5]. The present paper involves the novel use of behavioral aspects to improve mobile security. Studies of such nature are yet to exist in literature, which could have served as basis for comparison.

The aim of the paper is to consider the problems of user authentication within the mobile device based on individual behavioral patterns. The objectives are: 1) to apply human behavior context to mobile phones in recognizing the phone owner identity based on the mobile application and the location of the device, 2) to apply an analytic hierarchy process (AHP) in the decision making to detect the owner of the mobile phone and to compare different human behavior that form the basis for the decision to shut down the phone and the application or restrict item usage, and (3) to extend the architecture of CW-Lite model by incorporating human behavior context and AHP engine. This work is novel because human aspect has not been used in mobile app security. Owing to this reason, we focus only on two scenarios, namely, mobile application and mobility.

The rest of the paper is organized as follows: Section-II analyzes previous works related to mobile devices authentication and human behavior patterns, as well as the security model and the techniques of decision making. Section-III and Section-IV respectively discuss the research objectives of enhancement of the CW-Lite model and the proposed AHP model. Section-V discusses the process of the proposed AHP model. Section-VI contains the results of the experiments. The final section includes the summary of the work and suggestions for future work.

2. Related Studies

Authentication is the process of verification that validates a claimed identity by matching it to a known set of identities. When identifying a person, the system does not ascertain his or her identity [6]. According to Dinh et al. [7], mobile devices are rapidly becoming key computing platform in which the processes of transforming access to business and personal information require secure authentication. The essence of authenticating users on mobile phones is the enforcement of tighter security over physical access toward the mobile. An overview of human behavior context, CW-Lite model, and AHP is presented.

2.1. Human behavior context

Several studies have advanced security policy in technology environment with the use of the principle of human behavior. Brosso and Neve [8] reported that the implementation of human behavior analysis was significant in determining the basis of adaptive security in computer environment. However, another research adapted Skinner theory of operant conditioning behavior [9]. In the operant behavior, the environment is modified and generates consequences, thus it changes the likelihood of future similar occurrences. Nonetheless, operant conditioning is a mechanism for learning a new behavior.

2.2. CW-Lite model

The CW-Lite model [10] is selected in this study as the integrity guideline because of its stability and capacity to ensure that information within the mobile devices remains unchanged. Furthermore, the CW-Lite model can protect and measure the integrity of security-critical applications that run on mobile phones. Several studies have used CW-Lite as the basis for enforcing security policies. Muthukumaran et al. [11] conducted a study titled, "Protecting the Integrity of Trusted Applications in Mobile Phone Systems." In brief, the study focused on the development of a solution for protecting and measuring the integrity of security-critical applications that run on mobile phones.

2.3. Analytic Hierarchy Process (AHP)

AHP was introduced by Saaty [12]. AHP is an effective tool for dealing with complex decision making by aiding the decision maker in setting priorities and making the best decision. The systematic decision-making method includes qualitative and quantitative techniques [12]. AHP is also a structured technique for organizing and analyzing complex decisions based on mathematics and psychology [13]. It has been extensively used for a long time in numerous fields. AHP reduces complex decisions to a series of pairwise comparisons and synthesized results, thus helping capture both the subjective and objective aspects of a decision. Moreover, AHP incorporates a useful technique for checking the consistency of the evaluations of the decision makers, hence reducing bias in the decision-making process.

3. Methodology

In this section, the research objectives are presented. The primary aim of this research work is to combine the human behavioral aspect with mobile phones to detect occurrence of any change in user behavior and recognize the owner of the mobile device for security. The idea behind the proposed secure intelligent mobile solution is the use of human behavioral context. Analyzing and understanding the behavior of the user can be performed based on the mobile application and location stored in the database/cloud. If the current behavior is completely different from the previous behavior sorted in the database, the proposed AHP model can decide to shut down the mobile and the application or restrict access. The enhancement done on the CW-Lite model is presented next.

3.1. Enhancement of the CW-Lite model

We propose to apply a human behavioral context on the CW-Lite model to detect the changes in the user behavior through which the owner of the mobile device can be recognized, as shown on the left side of Figure 1.

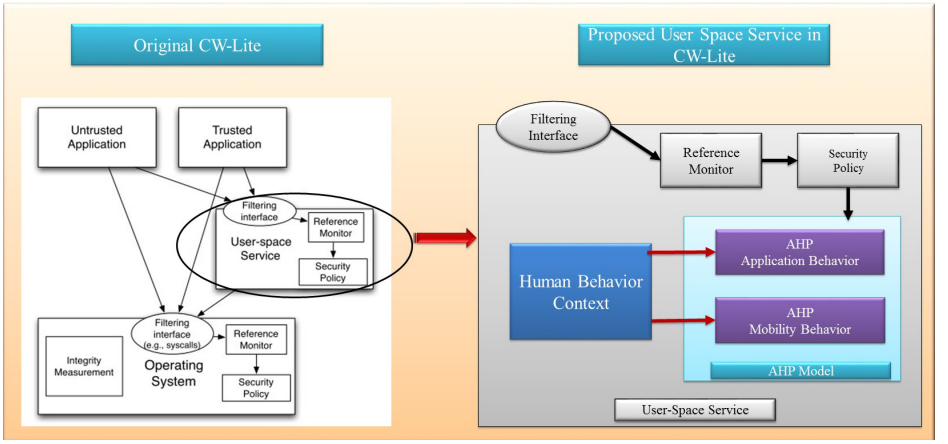

Figure 1: Enhancement of the CW-Lite model authentication policy model

Based on the AHP model, the proposed model aims to regulate the integrity of information flow between two objects, namely, the operating system and the user space services. These objects are illustrated in Figure 1. The details of the enhancement model are explained in the next section.

3.1.1. Internal work flow

The architecture of the proposed intelligent human behavior context is presented in this section. The architecture comprises the main component, which is the proposed AHP model. Figure 2 shows the internal structure of the proposed intelligent human behavior context.

The modification on CW-Lite is on the user space. The purpose of reference monitoring is to enforce access control, where the sensors collect the patterns of execution and usage of mobile application as well as capture the coordinates of the place where the users are located. After receiving inputs from the sensors of the mobile application and coordinates of the location, these inputs are kept in the database. Thereafter, the AHP engine calculates both scenarios to detect if any changes occurred in the user behavior based on the principles of AHP. Subsequently, the output of the AHP value is passed on to the operating system. The comparison of the current AHP value of both scenarios with the previous AHP value in the database is performed through filtering. Based on the result, AHP makes a decision. In case the AHP value shows that the current behavior is outside the normal boundary of the user behavior, an alarm will be sent to the security of CW-Lite to shut down the phone or the application or restrict access to the phone. The model is designed to detect an abnormality (intruder) immediately. However in this work, the data set for seven days was collected and analyzed using AHP. Thus, the user pattern can easily be revealed and easily differentiated by the intruder. This convergence can be immediately seen from the captured boundaries for both the user and intruder, which is based on the boundary of the user using basic standard deviation analysis with consistency index (CI), random index (RI), and consistency ratio (CR).

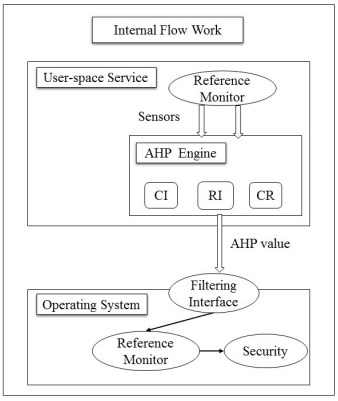

Figure 2: Intelligent human behavior-based mobile security architecture

3.2. AHP model

We apply the AHP model in the CW-Lite model because the former has the ability to decide the change in user behavior based on the inputs of the sensor of the human behavior context. The latter provides the security of user authentication and determines whether the phone will be locked. The AHP for mobile application and mobility takes the inputs from the human behavior context in user-space services of the sensors stored in the database. We next focus on the two main parts of the proposed AHP model structure, namely, AHP mobile application behavior and AHP mobility behavior. These parts are explained in the following sections.

3.2.1. AHP mobile application

The AHP mobile application behavior structure determines the changes in the user behavior based on the mobile application. The importance of the criteria (cell broadband, Wi-Fi network, and 3G network), is evaluated in relation to the goal. These criteria are used for this purpose because most of the applications employed by the users utilize these types of network to access the mobile application. The alternatives for AHP mobile application behavior include WhatsApp, Viber, Wechat, Facebook, SMS, and Call/Voice. We utilize the methods of the applications and propose a hierarchy of application for AHP mobile application behavior, as shown in Figure 3.

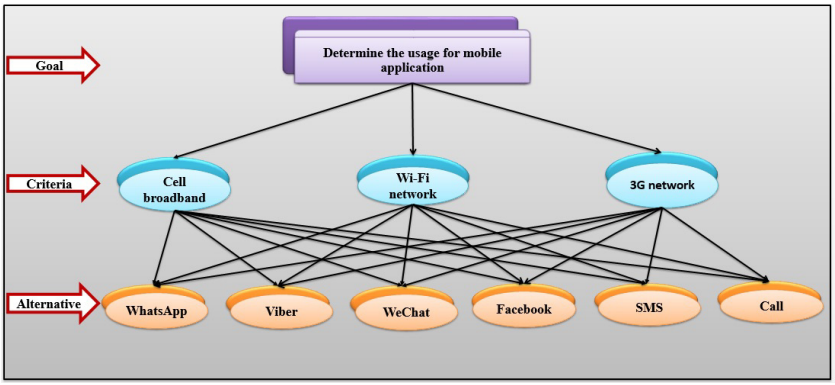

Figure 3: The proposed AHP mobile application hierarchy

The lines that connect the goal to each criterion mean that the criteria must be compared in a pairwise manner based on their importance with respect to the goal. Similarly, the lines that connect each criterion to the alternatives mean that the alternatives are compared in a pairwise manner based on the preference for a certain criterion.

3.2.2. AHP mobility

The AHP mobility behavior aims to determine the changes in the user behavior based on mobility and importance of the criteria, such as location, day, and time, which are evaluated in relation to the goal. These criteria are utilized based on the location at daytime and nighttime. The alternatives are Cell A, B, C, and D. We utilize their method and propose a hierarchy of mobility for AHP mobility behavior, as shown in Figure 4.

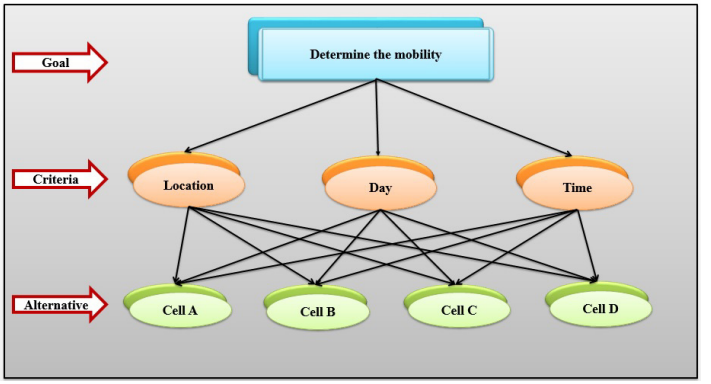

Figure 4: The proposed AHP mobility hierarchy

The lines that connect the goal to each criterion mean that the criteria must be compared in a pairwise based on their importance with respect to the goal. Similarly, the lines that connect each criterion to the alternatives mean that the alternatives are compared in a pairwise manner based on which the preference for a certain criterion.

4. AHP Model Usage on Proposed Intelligent Human Behavior Context

A schematic of the methodology is shown in Figure 5. We consider the evaluation in terms of performance metrics and product characteristics The process proposed for determining the usage for mobile application and mobility comprises the following flowchart. Because the limitation of the paper, so the main steps of AHP was used as Sharma [14].

5. Results and Discussion

The user behavior-based experiment was continuously run for a seven-day period in two different scenarios, but with the same simulation setup. The seven-day period is chosen in this experiment only to identify and locate the changes in the behavioral pattern between two different users. The amount of calculation needed by AHP is huge.

The main concept applied in this work is for the model to collect behavioral data and to quantify them using AHP for each user profile to be determined. These scenarios are used to detect if any change in the user behavior occurs. The first scenario is related to the user behavior towards the mobile application. Whereas, the second scenario is related to user behavior on mobility.

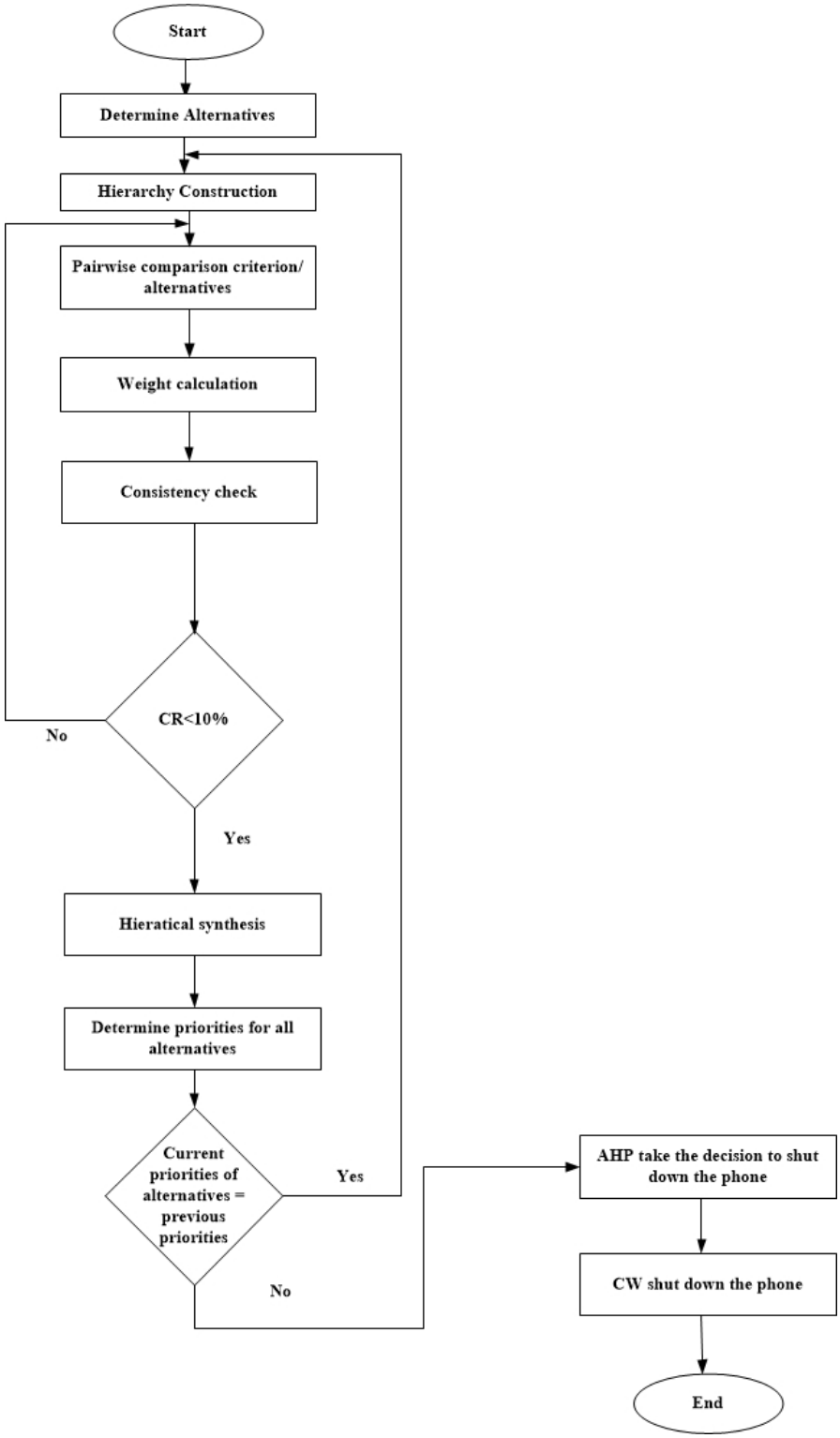

Figure 5: Flow diagram of the proposed intelligent human behavior-based mobile security platform

5.1. User Mobile Application Usage Results Using AHP

The first scenario of the AHP is the determination of the user behavior based on the mobile application. The performance hierarchy for the mobile application determines the relative weights of AHP using pairwise comparison. On the first day, pairwise comparison creates alternatives with respect to the three criteria.

The six alternatives are compared with each criterion, as shown in Table 1. The specialists made 15 pairwise judgments among the six alternatives (WhatsApp, Viber, WeChat, Facebook, SMS, and Call), with respect to their criteria (Cell broadband, Wi-Fi network, and 3G network). For example, (WhatsApp:Viber) = (20:20) = (1:1), where 20 refers to the number of times the application is opened per day. After the construction of the pairwise comparison matrix, the weights of each element in the matrix are retrieved. The comparison results and the weights of the six alternatives are shown in Table 1. The principle vector, which can be interpreted as the relative importance usage of each of the alternative, was computed.

Pairwise comparison of the three criteria (Cell broadband, Wi-Fi network, and 3G network) was conducted with respect to the goal (determine the usage for mobile application). The comparison and weights results are shown in Table 2.

The final stage of the AHP mobile application is the computation of the contribution of each alternative to the overall goal. The overall priority for each alternative is obtained by summing the product of the weights of the criteria and the contribution of the alternative with respect to that criterion. As a result, the final weights and ranking of the alternatives with respect to the goal were obtained. The results are shown in Table 3.

First day		WhatsApp	Viber	WeChat	Facebook	SMS	Call	Priority Vector
Cell broadband	Whatsapp	1	1	1/2	1/2	2	3	0.172
	Viber	1	1	2	1/2	2	3	0.199
	WeChat	2	1/5	1	1/3	1/2	1	0.123
	Facebook	2	2	3	1	1	2	0.256
	SMS	1/2	1/2	2	1	1	4	0.176
	Call	1/3	1/3	1	1/2	1/4	1	0.075
		WhatsApp	Viber	WeChat	Facebook	SMS	Call	Priority Vector
Wi-Fi network	Whatsapp	1	1/2	1/3	2	1/2	1/3	0.096
	Viber	2	1	1/2	2	1	3	0.193
	WeChat	3	2	1	3	1/2	3	0.250
	Facebook	1/2	1/2	1/3	1	1/3	2	0.094
	SMS	2	1	2	3	1	3	0.265
	Call	3	1/3	1/3	1/2	1/3	1	0.102
		WhatsApp	Viber	WeChat	Facebook	SMS	Call	Priority Vector
3G network	Whatsapp	1	1/2	1/7	2	1/2	1/3	0.079
	Viber	2	1	2	4	1	3	0.259
	WeChat	7	1/2	1	3	1/2	3	0.235
	Facebook	1/2	1/4	1/3	1	1/6	1	0.059
	SMS	2	1	2	6	1	2	0.261
	Call	3	1/3	1/3	1	1/2	1	0.106

Table 1: Pairwise comparison matrix for the alternatives

	Cell broadband	Wi-Fi network	3G network	Priority Vector
Cell broadband	1	3	2	0.517
Wi-Fi network	1/3	1	1/4	0.124
3G network	1/2	4	1	0.359

Table 2: Pairwise comparison matrix for criteria

	Cell broadband	Wi-Fi network	3G network	Overall Priority Vector
Whatsapp	0.172	0.096	0.079	0.129
Viber	0.199	0.193	0.259	0.219
WeChat	0.123	0.250	0.235	0.179
Facebook	0.256	0.094	0.059	0.165
SMS	0.176	0.256	0.261	0.218
Call	0.075	0.120	0.106	0.089

Table 3: Priority matrix for assessment of performance

CR was used to estimate directly the consistency of pairwise comparison. If the CR is less than 0.1, the comparison is acceptable. All CR values for this application are lower than 0.1. Therefore, all the judgments are consistent.

Similarly, the experiments are conducted during the rest of the days. The average for the seven days for the criteria is shown in Table 4, and Table 5 for the alternatives.

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Average
Cell broadband	0.517	0.635	0.236	0.139	0.663	0.517	0.171	**0.411**
Wi-Fi network	0.124	0.078	0.082	0.088	0.058	0.124	0.750	0.186
3G network	0.359	0.287	0.682	0.773	0.278	0.359	0.078	0.402

Table 4: The average of priority matrix for criteria

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Average
Whatsapp	0.129	0.091	0.126	0.162	0.113	0.118	0.198	0.134
Viber	0.219	0.164	0.157	0.051	0.042	0.075	0.233	0.134
WeChat	0.179	0.169	0.136	0.160	0.090	0.172	0.158	0.152
Facebook	0.165	0.193	0.308	0.300	0.285	0.196	0.164	0.230
SMS	0.218	0.215	0.210	0.250	0.418	0.366	0.342	**0.288**
Call	0.089	0.167	0.064	0.076	0.050	0.073	0.040	0.079

Table 5: The average of priority matrix for alternative

To determine the most frequently used mobile application by a user, AHP is applied to make the decision based on overall priorities, as shown in Table 5. The results for SMS, Facebook, WeChat, Viber, WhatsApp, and Call indicate that SMS is the most used application; thus, it is shown in **bold** font.

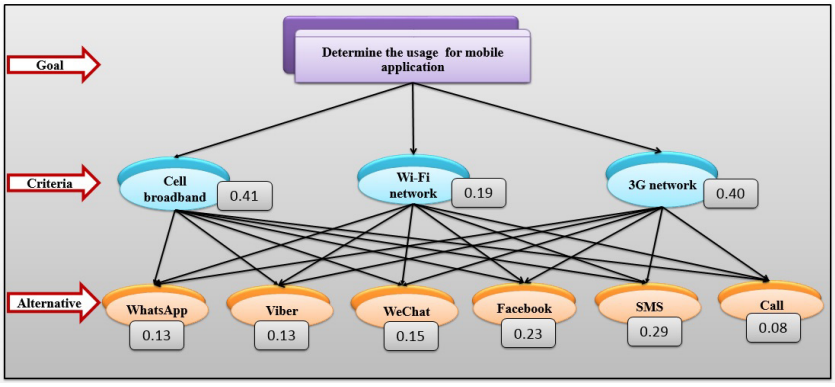

Figure 6: The hierarchy of AHP mobile application for the main user

AHP is applied to determine the priority values for the three types of connection (criteria) to the mobile application. To determine the overall priority values for the alternatives, the most used applications are ranked based on each mobile application: SMS (29%), Facebook (23%), WeChat (15%), Viber (13%), WhatsApp (13%), and Call (8%). The AHP hierarchy is shown in Figure 6.

5.2. User Mobility Results Using AHP

The decision for AHP mobility involves the location mostly visited by the user, which is highlighted **bold** font in Table 6. The average determines the location most visited compared with the other locations. The calculation for this scenario is similar to the AHP mobile application scenario. According to the overall priorities of the following Cell C, A, B, and D, Cell C is the location most visited by the user.

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Average
Cell A	0.301	0.230	0.264	0.283	0.394	0.449	0.464	0.341
Cell B	0.092	0.076	0.085	0.358	0.177	0.127	0.137	0.150
Cell C	0.495	0.625	0.555	0.186	0.347	0.343	0.329	**0.411**
Cell D	0.112	0.069	0.097	0.171	0.081	0.081	0.069	0.097

Table 6: The average of priority matrix for alternative

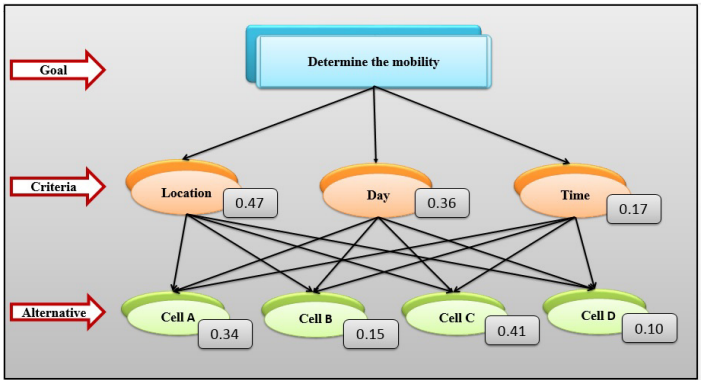

Figure 7: The hierarchy of AHP mobility for the main user

Figure 7 shows the ranking of the priority values for the criteria, as well as the ranking of the alternatives based on the most visited location, which is considered within an overall priority value to have followed the AHP ranking of each location visited: Cell C (41%), A (34%), B (16%), and D (10%).

5.3. Main User Behavior Deviation Toward Mobile Applications

Figure 8 shows the behavior of the main user during the observation conducted for seven days. Based on the results, the most used application during the seven days of observation is SMS. However, during the observation on the second, third, and fourth days, Facebook was the most used application.

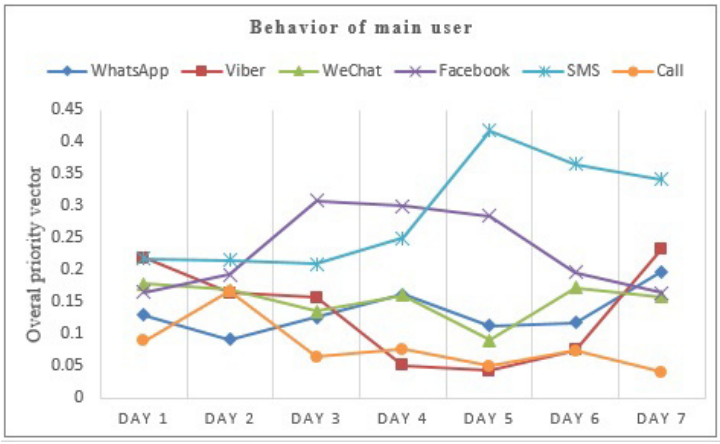

Figure 8: The behavior of the user base on mobile application

The behavior of the main user in relation to the use of certain applications, such as WhatsApp, changes from one day to another, even though such behavior remains in the same boundary area. Based on the results received for the SMS application, the behavior of the user is similar during the first four days; however, a huge change occurs when the usage of SMS application increases. This situation occurs as the behavior of the user changes. With continuous observation, however, the behavior starts to deviate from conditioned practices. This result can be attributed to the normal behavior of the user.

5.4. Main User Behavior Deviation Based on Mobility

The results in Figure 9 show a change in the main user behavior from one day to the next in a span of seven days. Based on these results, the location of the user is similar. The results show that the most visited location is Cell C in the first four days of observation. However, during the remaining days, the user focuses on Cell A, where the highest application usage occurs. These behavioral changes are normal for the observed user.

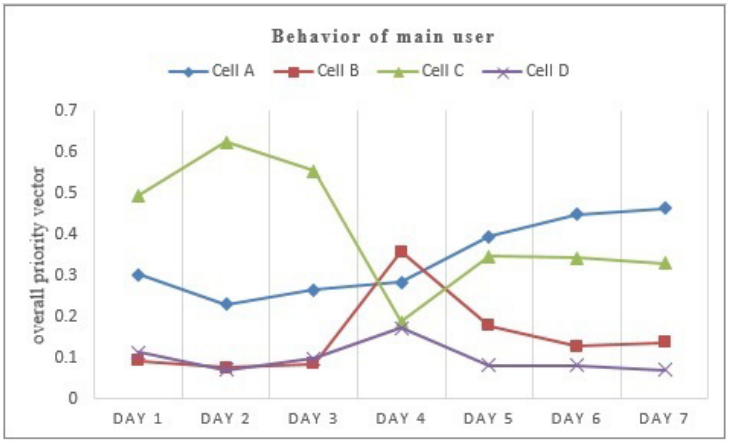

Figure 9: Seven days observation results on user behavior based on mobility

The effect of the behavior of intruders can be investigated in cases of stolen phones to identify the change in user behavior using the proposed scenarios of AHP. Based on the result shown in Figure 10, the boundary of the main user behavior in using mobile application is based on the calculated standard deviation. The figure shows the upper and lower points for each application based on the average.

Any full value inside the boundary indicates the main user behavior. However, the value can represent that of the intruder although this scenario is not detected in this paper because the value within the interval is full. Thus, checking other applications to detect if the behavior is different is important. This scenario is performed using six mobile applications and three are beyond the boundary, where the AHP detected 50% of the changes in behavioral aspect. If the second scenario of AHP mobility is detected with vast differences in behavior, a final decision will be made by AHP by considering the entity as an intruder.

Based on Figure 10, the full values of the user are outside the interval when these applications are used, except for three values identified as values of the intruder. This result is significant to the AHP mobile application scenario.

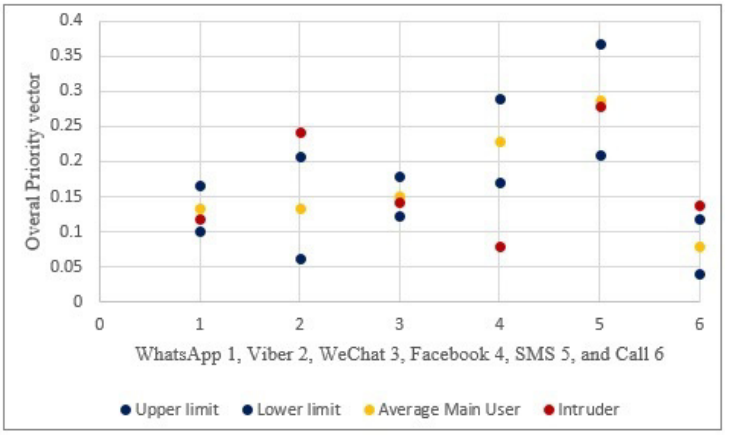

Figure 10: The range usage of each mobile application and compare with intruder

For the AHP mobility scenario, Figure 11 shows that the value of the location visited by the user is fully outside the interval of the location most visited by the main user except for one location. This observation can only mean that the user is an intruder. The calculated standard shows the ability of AHP to detect the intruder and provide accurate results. AHP makes the decision by comparing both scenarios to detect the difference between the behaviors of the users. AHP decides whether to shut down the phone or the application or to restrict access to the phone based on the changed behavior. AHP sends the decision to the CW-Lite model, which consequently terminates the phone or the application or restrict access to the phone based on relevant data.

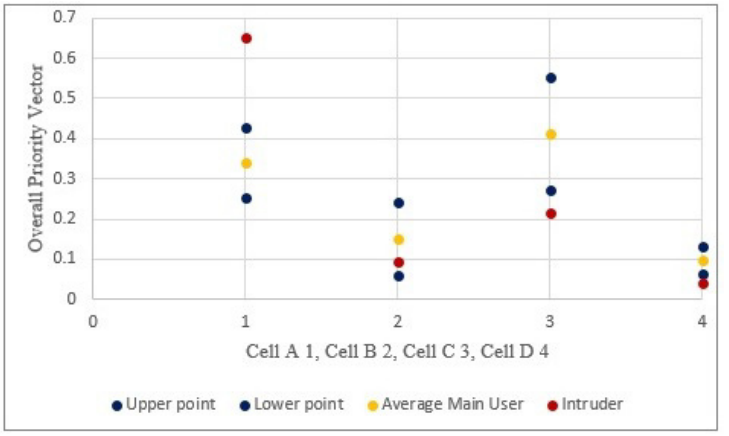

Figure 11: The range usage for visited each location and compare with intruder

The confidence levels that AHP can immediately detect behavioral changes based on the boundary of results are

identified in Figures 10 and 11. The number of contexts of the model determines the quantity of details about the user and different boundaries the user will have. The proposed model must have rich details and accurate information about the user.

The tradeoffs of having more context about the user behavior is the richer detection and profiling, which means that the model can detect with high confidence between an intruder and a main user, as shown in Figures 10 and 11, and based on the seven-day data collection and with much larger data set, that is, with 98% confidence level. The method can identify an intruder from a normal/main user with 100% confidence. The seven-day period is chosen in this experiment only to identify and locate the changes in the behavioral pattern between two different users. The amount of calculation needed by AHP is huge; hence, the data collection is done only within seven days. This research is preliminary; in the future, however, data will be collected until a 95% confidence is achieved.

6. Conclusion

This paper presented a method that successfully incorporated the human behavioral aspect with mobile phones to detect occurrence of any change in user behavior and recognize the owner of the mobile device to ensure the security of the data in the phone.

Based on the implementation and analysis of the results from the two scenarios of AHP mobile application and AHP mobility, the proposed AHP model could effectively detect the changes in human behavior. Thus, the proposed AHP could fulfill the objectives of the research. The applied intelligent human behavioral context on the CW-Lite model showed the advantages of AHP in detecting the changes in the user behavior and in authenticating the identity of the main user. These advantages ensured reliability, data security, and security of the phone.

This paper demonstrates the applicability of AHP to the detection of the changes in user behavior toward providing secure phone settings, as well avoiding damages to the rightful owner. Overall, we will involve dynamic-based applications to record the type of applications in the future.

References

[1] Z. Liu, Y. Hong, D. Pi, A large-scale study of web password habits of chinese network users, Journal of Software 9 (2) (2014) 293–297.
[2] T. Liu, P. Bahl, I. Chlamtac, Mobility modeling, location tracking, and trajectory prediction in wireless atm networks, Selected Areas in Communications, IEEE Journal on 16 (6) (1998) 922–936.
[3] R. Bajaj, S. L. Ranaweera, D. P. Agrawal, Gps: location-tracking technology, Computer 35 (4) (2002) 92–94.
[4] C. Song, Z. Qu, N. Blumm, A.-L. Barabási, Limits of predictability in human mobility, Science 327 (5968) (2010) 1018–1021.
[5] S. Phithakkitnukoon, T. Horanont, G. Di Lorenzo, R. Shibasaki, C. Ratti, Activity-aware map: Identifying human daily activity pattern using mobile phone data, in: Human Behavior Understanding, Springer, 2010, pp. 14–25.
[6] J. Bigun, J. Fiérrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, Combining biometric evidence for person authentication, in: Advanced Studies in Biometrics, Springer, 2005, pp. 1–18.
[7] H. T. Dinh, C. Lee, D. Niyato, P. Wang, A survey of mobile cloud computing: architecture, applications, and approaches, Wireless communications and mobile computing 13 (18) (2013) 1587–1611.
[8] I. Brosso, A. La Neve, Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security, INTECH Open Access Publisher, 2012.
[9] D. Barnes-Holmes, Y. Barnes-Holmes, V. Cullinan, Relational frame theory and skinner's verbal behavior: A possible synthesis, The Behavior Analyst 23 (1) (2000) 69.
[10] U. Shankar, T. Jaeger, R. Sailer, Toward automated information-flow integrity verification for security-critical applications., in: NDSS, 2006.
[11] D. Muthukumaran, J. Schiffman, M. Hassan, A. Sawani, V. Rao, T. Jaeger, Protecting the integrity of trusted applications in mobile phone systems, Security and Communication Networks 4 (6) (2011) 633–650.
[12] T. Saaty, The analytic hierarchy process (ahp) for decision making, in: Kobe, Japan, 1980.
[13] Y. Y. Jusoh, K. Chamili, N. C. Pa, J. H. Yahaya, Open source software selection using an analytical hierarchy process (ahp), American Journal of Software Engineering and Applications 3 (6) (2014) 83–89.
[14] M. J. Sharma, I. Moon, H. Bae, Analytic hierarchy process to assess and optimize distribution network, Applied Mathematics and Computation 202 (1) (2008) 256–265.