International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Location-based Access Control in Neighborhood Geosocial Network: a Case of Emergency Assistance

Syarulnaziah Anawar, Low Sheng Loong, Norharyati Harum, Zakiah Ayop, Erman Hamid

Abstract: ***To enforce safer virtual neighborhood environment, access control is essential to specify privileges or access rights to resources in neighborhood geosocial network applications. In the case of emergency circumstances, several concerns in implementing access control have been identified: (1) inefficient message sending to irrelevant recipients (2) location spoofing (3) gossip and rumors due to disclosing information to wrong audience. To address such potential risks, access control specifically tailored for neighborhood geosocial network is required. The objective of this paper is two-fold: First, to propose an access control using density-based and position-based location conditions for neighborhood geosocial network. Second, to design mySOS, a proof-of-concept prototype that incorporate the proposed access control to improve access control for emergency assistance in neighborhood geosocial network. To achieve the objectives, a combination of proposed self-organized segmentation algorithms (density-based) and resident engagement incentives (position-based) are implemented. This study contributes to a new way for access control that will determine user profile in accessing emergency assistance features in a neighborhood geosocial network application.***

Keywords: Access control, Privacy, Geosocial network, Emergency Assistance

I. INTRODUCTION

Neighborhood geosocial network is geosocial networking branches that allow user to communicate and share information virtually within a neighborhood or community. Typically, neighborhood geosocial network tracks current user location coordinates using location-aware features in users' mobile device. Location awareness will assist GPS self-check-in function to match users' home address and their current location.

One of the notable function in many neighborhood geosocial network applications is the emergency assistance function. A user may wish to use emergency assistance function to notify other application users in the case of crime, accident, medical needs. Therefore, access control is vital to specify privileges or access rights to applications' resources. In addition, access control may improve social distance and social quality in the virtual community.

This study has identified several concerns related to access control in geosocial network neighborhood. First, under emergency circumstances, sending updates to the whole neighborhood may not be efficient as the messages may be sent to a large number of irrelevant recipients who are not likely to respond [1] or do not expect to be alerted to emergencies. This may violate the privacy if the user intended to disclose such information to certain neighbors only. Second, without proper identity verification technique, a malicious user may cheat in their location declaration [2] and falsify as a group member in the existing neighborhood. Third, some users may be worried that their reputations will be affected because of gossip and rumors due to disclosing information to wrong audience [3]. To overcome such potential risks, the best way for the communities is to design access control specifically for neighborhood geosocial network.

The objective of this paper is two-fold: First, to propose a location-based access control using density-based and position-based location conditions for neighborhood geosocial network. Second, to design mySOS, a proof-of-concept that incorporate the proposed method to improve access control for emergency assistance in neighborhood geosocial network. This paper is organized as follows. Section 2 presents the literature review of this study. Next, section explains the prototyping methodology adopted for this study. In section 4, the design insight of the proposed location-based access control is presented. Next, we present system architecture and the proof-of-concept implementation of mySOS prototype in Section 5. Our work of this paper is summarized in the last section.

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.

* Correspondence Author

Syarulnaziah Anawar*, Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia. E-mail: syarulnaziah@utem.edu.my

Low Sheng Loong, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

Norharyati Harum, Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

Zakiah Ayop, Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

Erman Hamid, Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

II. LITERATURE REVIEW

In the past years, relationship-based access control (ReBAC) is a prominent model for managing access control of many research works in social network applications.

Fong [4] was among the first study that propose access control model based on relationship in Social network in 2009. The study presented Facebook-like social network access control, where members are given authorization to access resources according to their relationship with the resource owner. Another work by Carminati [5,6] presents access control for both users to users, and users to resources. The relationship is defined based on the type, depth, and trust level.

With the proliferation of location-based services, several studies have proposed inclusion of spatial and temporal dimension for access control in location-based application. For example, temporal dimension such as past check-in history is required in the access control policies proposed in [7]. [1] is one of the studies that extend access control in geosocial network. The study proposed protection model that considers user current location and spatial relations over people located in a certain neighborhood in geosocial computing system (GSCS). The drawback of the protection model [1] is that the model does not have proper identity verification technique, where the study assumed that users do not falsify their location declarations, i.e. location spoofing.

In geosocial network application, geolocation-based authentication is commonly used to detect malicious users and location spoofing [8]. User access may be denied in the occurrence of mismatch of user location during login request. Such implementation can be seen in [9], where location verification technique is employed to identify malicious users using parsing method to compare user current location with the origin of login request. Several other verification schemes have also been proposed in [10]-[12]. However, these works focus on detecting location spoofing in social network application only, making it less suitable for neighborhood geosocial network application.

This paper presents an alternative access control tailored for neighborhood geosocial network. The proposed technique is based on two location-based conditions proposed in access control model for location-based services [13], namely density and position-based conditions. Density-based condition refers to the condition on relationship among multiple users, while position-based condition refers to the condition on the user location.

III. METHODOLOGY

This study is conducted following prototyping model, which consists of six phases; requirement gathering, quick design, building prototype, customer evaluation, refining prototype and engineer product. The activity flow of each phases is illustrates in Figure 1.

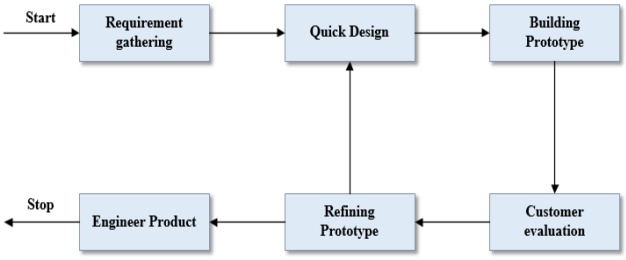


Fig. 1.Prototyping model

This paper only discusses activities up to phase 3. The activities in each phase are described in Table 1.

Table- I: Description of methodology

Phase	Activities
Requirement Gathering	• Identify required hardware and software (Intel XDK, Web Browser, Cordova, Smartphone, modem). • Identify modules/functions need to be embedded in the prototype
Quick Design	• Determine design of access control according to density-based (self-organized segmentation) and position-based (residence engagement incentives). The discussion is elaborated in Section 4. • Determine the design of the prototype based on hardware, software, modules and function of the emergency assistance application. The discussion is elaborated in Section 5.
Building Prototype	• Build proof of concept prototype based on determined design • The access control functionality testing is explained in Section 6.

IV. DESIGN OF PRIVACY CONTROL METHOD

This section presented the design flow of the proposed location-based access control that involves two main phases and the details of each phases.

A. Design Flow

The design flow for the proposed location-based access control is shown in Figure 2. The access control is designed in two phases according to location-based conditions; density-based and position-based:

- *Density-based:* This phase evaluates optimal number of residents currently in neighborhood. This study used our previously improved self-organized segmentation algorithms to cluster the users based on Dunbar number to improve social distance and quality in the geosocial network application. For a more detailed explanation of our self-organized segmentation algorithms, see [14].
- *Position-based:* This phase evaluates status of a resident who is located within neighborhood area to avoid location spoofing problem. This study used our proposed resident engagement incentives as authorization scheme against malicious users.

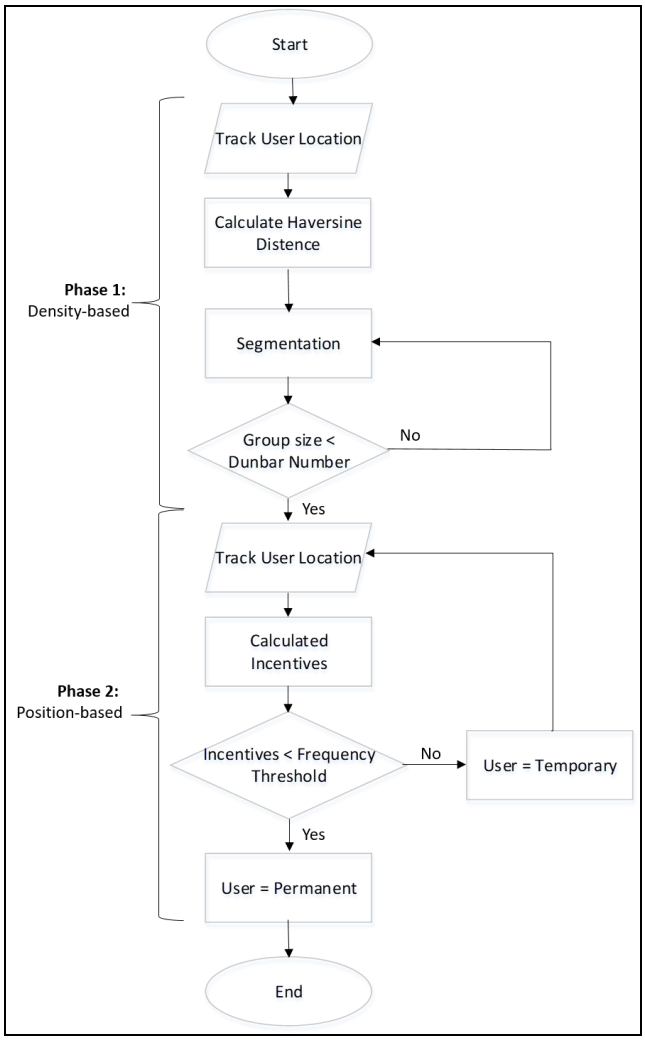


Fig. 2.Design flow for the proposed location-based access control

B. Phase 1: Density-based

In phase 1, this study implements improved self-organized segmentation algorithms to group the neighborhood into clusters. The improved algorithms extend previous work by Shi [15],[16] that utilized DBSCAN algorithms [17] for clustering in a geosocial network. In the improved algorithms, distance between residents is calculated using Haversine formula [18] due to higher accuracy for great-circle distance. Next, the neighborhood segmentation is done by defining a threshold value for two important parameters to self-organize the segment density, namely Eps and MinPts. Eps is the minimum distance between neighbors and MinPts is the minimum number of neighbors to form a neighborhood. Note that these two parameters were previously defined. In the context of the study, Eps is the radius of house area and the width of roads, which is set to 2.75 meter width length. On the other hand, MinPts parameter is set to 2 based on the recommendation Simmel's studies of dyad [19].

In addition, the proposed algorithms improve the concern of social connectivity by implementing cluster re-segmentation using Dunbar's number. This is particularly important, as current neighborhood segmentation technique did not take into account of social connectivity between neighbors. The determination of group size of a cluster and re-segmentation of a cluster is shown in Figure 3.

Algorithm 1: Cluster_size (cluster_data)

For C_i in clustered data set
  If C_i size $C > 150$
    add C_i to list
  End
End
Return list
End // cluster_size

Fig. 3.Determination of cluster group size [14]

Where,
C = Cluster group size
C_i = Cluster data set

Each cluster should not exceed certain group size to maintain social distance and quality within the community [20]. Thus, the proposed algorithm 1 applies Dunbar's Number to maintain a mean group size of 150 peoples and re-segment cluster group size that is larger than 150 peoples as shown in Fig 3.

Next, inverse Haversine formula is implemented to form a rectangle border instead of in arbitrary shape for equal cluster segmentation. To form the rectangle border, the algorithms determine the number of slice by dividing the total points for oversize segment with 150. Oversize cluster is re-segment as specified in Figure 4.

Algorithm 2: Segmentation (over_size_cluster)

If $DLat > DLng$
 Distance segmented area, $DSeg = DLat / S$
 New Cluster List,
 $NList = inverse\_haver\sin e(NLat, SLat, DSeg)$
Else
 Distance segmented area, $DSeg = DLng / S$
 New Cluster List,
 $NList = inverse\_haver\sin e(WLng, ELng, DSeg)$
End
Return *NList*
End // *segmentation*

Fig. 4.Determination of rectangle border for arbitrary shape cluster [14]

Where,
$NLat$ = Most North of Latitude point
$SLat$ = Most South of Latitude point
$WLng$ = Most West of Longitude point
$ELng$ = Most East of Longitude point
Distance of Latitude, $DLat = NLat - SLat$
Distance of Longitude, $DLng = WLng - ELng$
Number of slice, S = Total point for over-size / 150

C. Phase 2: Position-based

In phase 2, this study proposes a new authorization scheme called resident engagement incentives that will be used to determine residents' status through their successful self-check-in record. In the context of this study, resident engagement incentives is an accumulated point system that use mobile phone GPS to track user location. During registration, user needs to state their home address. To identify resident status, a combination of successful self-check-in track record and minimum amount of threshold frequency is needed to upgrade the user profile. In the context of this study, the threshold frequency is set to 182 days based on determination of residence status for individuals in Malaysia according to Income Tax Act 1967 (ITA 1967) Section 7 and subsection 7(1B).

There are two user profiles namely: temporary residence and permanent residence. User with cumulative incentives point less than threshold value is categorized as temporary resident whereas user with high cumulative incentives point that surpass the threshold value is categorized as permanent resident. User with temporary resident status indicates that the user has not been verified in the neighborhood.

Referring to this guideline, this study proposes Equation (1) to determine the residence status for neighborhood geosocial application. A GPS check-in of a user *i* is the day in which the user stays at his or her own living place. A user GPS coordinates will be recorded on that particular day if the GPS coordinates match with the user home address coordinates. *Ai* is the check-in date in which the GPS coordinates are recorded for the user *i*. *F* is defined as the threshold frequency for accumulated days of user GPS record.

$$a_i = \frac{|A_i|}{F}, a \in (0,1) \qquad (1)$$

V. PROOF OF CONCEPT

This section described the proof of concept implementation of the proposed location-based access control in mySOS application.

A. System Architecture

mySOS is a neighborhood geosocial network application which is initiated as a social platform in a neighborhood or community in Malaysia. The application offers several features for its users that include social messaging, emergency assistance, and local event organizer. mySOS is developed for Android mobile user and an open database web platform.

Figure 5 shows mySOS system architecture and registration process. The application can be accessed from any computer connected to the Internet using a standard browser for web-based application, or from an Android phone for better portability, ubiquity and connectivity. During registration, a resident should provide relevant personal information and home address to ensure accurate geographic coordinates of his or her living place, and provide trusted neighbor and emergency contact to enable emergency assistance function. First time users will be recorded as temporary resident in the database and will be given limited access to the application features. Once the user exceed the minimum resident engagement incentives, the user will be verified as permanent resident and will be given full access to the application features.

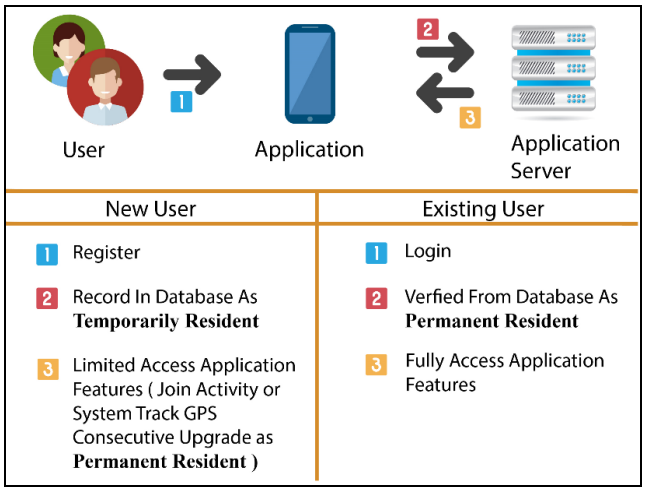


Fig. 5.System architecture

B. Application Design and Functionality

The interface of the application is designed using Dobble, a free social network application template for educational purposes [21]. In this paper, the discussion of the application design and functionality is limited to the emergency assistance feature only. In mySOS, the emergency assistance feature can be used to alert nearby neighbors in the case of emergency.

We developed *emergency post* and *neighbor SOS* functions to effectively send alert message to nearby neighborhood in the case of emergency:

- *Emergency post:* User can submit an emergency post with message and the application will automatically capture user current geolocation coordinates and embed it into to the message. Figure 6 shows the example of how to emergency post is implemented.
- *Neighbor SOS:* User can click on a SOS button when feel distress. Once the SOS button is activated, the application will automatically create an emergency post with current geolocation coordinates, send Short Message Service (SMS) to nearby neighbors and emergency contact, and call emergency contact number based on user registration information. In the application, the neighbor SOS button is placed at down right corner in each of the application page. The placement is important for user convenience during emergency circumstances.

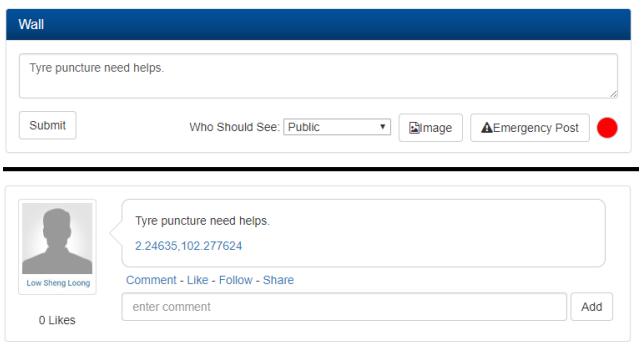


Fig. 6.Emergency post

VI. IMPLEMENTATION OF ACCESS CONTROL

This section demonstrates the implementation of the proposed location-based access control in both emergency post and neighbor SOS functions for different resident status; temporary and permanent resident.

A. Emergency Post Function

In this application, a user with temporary resident status does not have an access to the emergency post function on their wall as shown in Figure 7. The temporary resident is deemed untrusted in the community, and they can only send normal message to their wall and the message will not be notified to other users.

Fig. 7.Emergency post for temporary resident

On the contrary, a user with permanent resident status may opt to submit normal post or emergency post. Normal and emergency post is indicated using different color: red for emergency post and green for normal post as shown in Figure 8. The emergency post message content will be appended with user current geolocation coordinates. All nearby neighbors within the same cluster ID will receive notification from the user as shown in Figure 9. The geolocation coordinates are included as a URL link that links to smartphone navigation application such as Google Maps to ease user navigation.

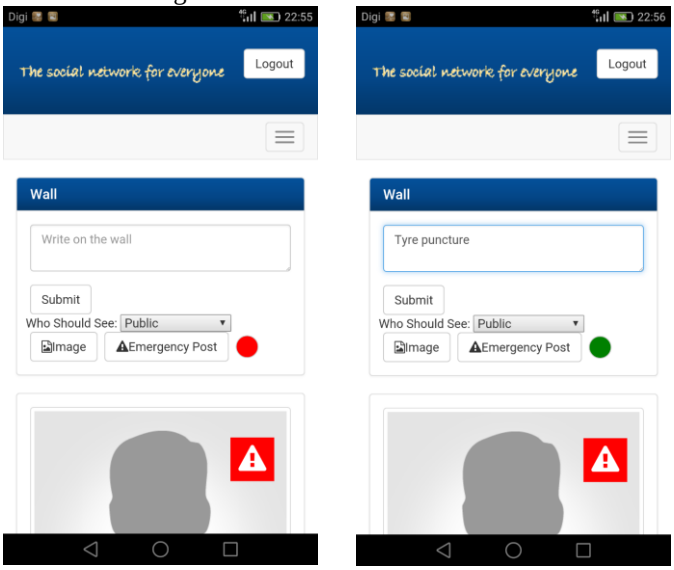


Fig. 8.Emergency post for permanent resident

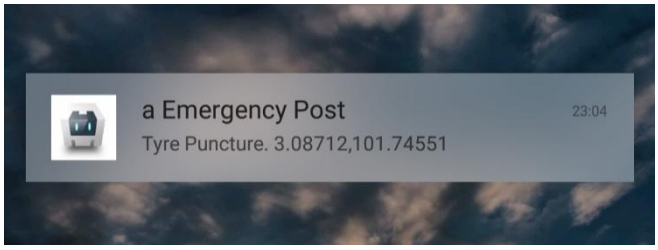


Fig. 9.Alert notification for emergency post

B. Neighbor SOS Function

In this application, a user with temporary resident status has limited access to the neighbor SOS function. When the temporary resident activates the SOS button, the application will automatically send Short Message Service (SMS) and create a call to their emergency contact only (see Figure 10).

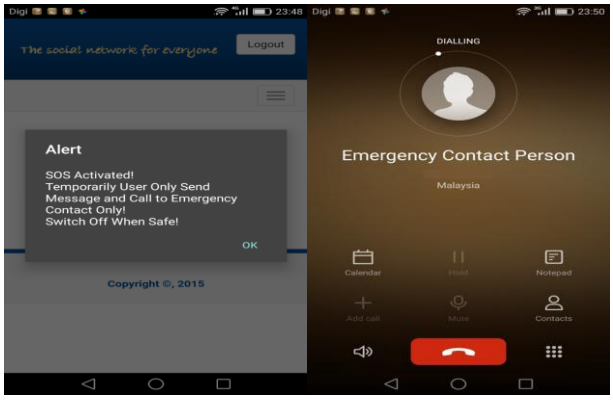


Fig. 10. Neighbor SOS for temporary resident

Figure 11 and Figure 12 illustrate the implementation of access control in neighbor SOS function for permanent resident. When a user with permanent resident status activates their SOS button, the application will automatically send Short Message Service (SMS) and create a call to their emergency contact and all nearby neighbors within the same cluster ID. The geolocation coordinates are included in the alert notification.

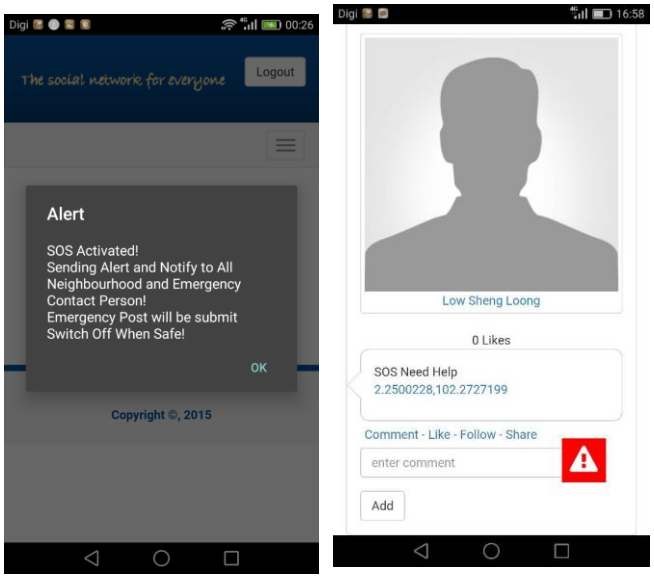


Fig. 11. Neighbor SOS for permanent resident

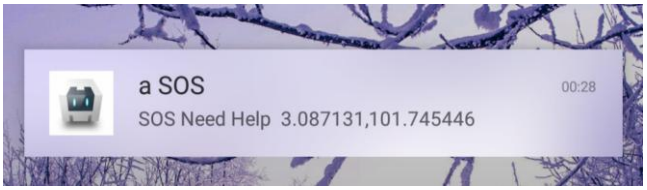


Fig. 12. Alert notification for Neighbor SOS

VII. CONCLUSION

In conclusion, this study proposed a new location-based access control using density and position-based location conditions for neighborhood geosocial network application. The access control is designed using a combination of self-organized segmentation and resident engagement incentives techniques. A proof-of-concept prototype for emergency assistance has been developed to incorporate the proposed access control in order to determine user profile: temporary or permanent. The proposed access control has achieved promising results that can determine residence status in a virtual neighborhood or virtual community. This study contributes to a new way for user authorization in a geosocial network neighborhood application.

Future extension of current work will include participants' involvement parameters: daily-devoted time, and number of daily task; as part of the resident engagement incentives in determining resident status for geosocial neighborhood application.

ACKNOWLEDGMENT

A high appreciation to Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) for supporting the work done in this paper.

REFERENCES

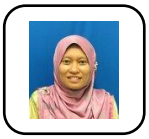
1. E. Tarameshloo and P.W. Fong, "Access control models for geo-social computing systems," *19th ACM Symposium on Access Control Models and Technologies*, June 2014, pp. 115-126.
2. B. Debatin, J.P. Lovejoy, A.K. Horn and B.N. Hughes, "Facebook and online privacy: Attitudes, behaviors, and unintended consequences," *Journal of Computer-mediated Communication*, Vol. 15 (No. 1), 2009, pp. 83-108.
3. C. Gates, "Access control requirements for web 2.0 security and privacy," *Web 2.0 Security and Privacy Workshop*, 2007.
4. P.W. Fong, M. Anwar and Z. Zhao, "A privacy preservation model for facebook-style social network systems," *European Symposium on Research in Computer Security*, September 2009, pp. 303-320.
5. B. Carminati and E. Ferrari, "Enforcing relationships privacy through collaborative access control in web-based social networks," *5th International Conference on Collaborative Computing: Networking*, Applications and Worksharing, November 2009, pp. 1-9.
6. B. Carminati, E. Ferrari and A. Perego, "Enforcing access control in web-based social networks," *ACM Transactions on Information and System Security*, Vol. 13 (No. 1), 2009, p. 6.
7. P.W. Fong, P. Mehregan and R. Krishnan, "Relational abstraction in community-based secure collaboration," *ACM SIGSAC Conference on Computer & Communications Security*, November 2013, pp. 585-598.
8. A.C. Hsu and I. Ray, "Specification and enforcement of location-aware attribute-based access control for online social networks," *ACM International Workshop on Attribute Based Access Control*, March 2016, pp. 25-34.
9. S.O. Oluoch, "Improving Password Security Using Location-Based Intelligence," *International Journal of Scientific and Research Publications*, Vol. 4 (No. 2), 2014, pp. 1-4.
10. W. He, X. Liu and M. Ren, "Location cheating: A security challenge to location-based social network services," *31st International Conference on Distributed Computing Systems*, June 2011, pp. 740-749.
11. V.K. Nguyen, *Authentication of smartphone user using RSSI geolocation*, Naval Postgraduate School Monterey, California, 2014.
12. B. Zhao and D.Z. Sui, "True lies in geospatial big data: Detecting location spoofing in social media," *Annals of GIS*, Vol. 23 (No. 1), 2017, pp. 1-14.
13. C.A. Ardagna, M. Cremonini, S.D.C. di Vimercati, and P. Samarati, "Access control in location-based services," *Privacy in Location-Based Applications*, 2009, pp. 106-126.
14. L.S. Loong, S. Anawar, Z. Ayop, M.R. Baharon and E. Hamid, "Self-organized Population Segmentation for Geosocial Network Neighborhood," *International Journal Of Advanced Computer Science And Applications*, Vol. 9 (No. 9), 2018, pp. 230-235.
15. J. Shi, N. Mamoulis, D. Wu, and D.W. Cheung, "Density-based place clustering in geo-social networks," *ACM SIGMOD international conference on Management of data*, June 2014, pp. 99-110.
16. D. Wu, J. Shi, and N. Mamoulis, "Density-Based Place Clustering Using Geo-Social Network Data," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16 (No. 5), 2018, pp. 838-851.
17. R.W. Sinnott, "Virtues of the Haversine," *Sky Telesc.*, Vol. 68, 1984, p.159.
18. R.L. Moreland, "Are dyads really groups?," *Small Group Research*, Vol. 41 (No. 2), 2010, pp. 251-267.
19. R. Dunbar, *How many friends does one person need? Dunbar's number and other evolutionary quirks*, London: Faber & Faber, 2010.
20. D. Walter (2015). "*fresh5447*", [Online]. Available: https://github.com/fresh5447/bootstrap-social-network-template.

AUTHORS PROFILE

Syarulnaziah Anawar holds her Bachelor of Information Technology from UUM, Msc in Computer Science from UPM, and PhD in Computer Science from UiTM, Malaysia. She is currently a Senior Lecturer at the Department of Computer and Communication System, Faculty of Information and Communication Technology, UTeM. She is a member of the Information Security, Digital Forensic, and Computer Networking (INSFORNET) research group. Her research interests include human-centered computing, participatory sensing, mobile health, usable security, and societal impact of IoT. You can contact her at email syarulnaziah@utem.edu.my.

Low Sheng Loong is a graduated student from University Teknikal Malaysia Melaka (2018). He holds his Degree in Computer Networking. His research interest is in computer system and networking. You can contact him at email lsloong1012@gmail.com.

Norharyati Harum holds her Bachelor in Engineering (2003), MSc. in Engineering (2005) and PhD in Engineering (2012) from Keio University, Japan. She has experience working in R & D Department of Next Generation Mobile Communication at Panasonic Japan (2005-2009).. She is currently a senior lecturer at the Department of Computer and Communication System, Faculty of Information and Communication Technology, UTeM. Her interests in research area are Internet of Things, Wireless Sensor Network, Next Generation Mobile Communication and Signal Processing.



Zakiah Ayop holds her Bsc Computer Science from UTM, Msc in Computer Science from UPM, Malaysia. She is a senior lecturer at the Department of Computer and Communication System, Faculty of Information and Communication Technology, UTeM, Malaysia. She is a member of the Information Security, Digital Forensic, and Computer Networking research group. Her research interest is Quality of Information (QoI), Internet of Things (IoT) and Distributed Computing and Networking. You can connect with Zakiah at zakiah@utem.edu.my.

Erman Hamid is a Senior Lecturer at the Department of Computer and Communication System, Faculty of Information and Communication Technology, UTeM. With a qualification in Bachelor Of Information Technology (Hons) (Multimedia) from Universiti Utara Malaysia (UUM), he started working in Entrepreneurs Development Institute before joining Kolej Yayasan Melaka, both as a Lecturer. His teaching subjects are related to Computer Networking, Multimedia and Information Technology. After persuing his Master In Information Technology (Computer Science) at Universiti Kebangsaan Malaysia (UKM), he joins Universiti Teknikal Malaysia Melaka (UTeM) as a Lecturer. His research interest includes Network Management, Network Visualization and Internet of Things (IoT)