International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 5, October 2022, pp. 5191~5203
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i5.pp5191-5203

Security and privacy recommendation of mobile app for Arabic speaking

Hameed Hussain Almubarak[1], Mohamed Khairallah Khouja[2], Ahmed Jedidi[3,4]
[1]Department of Computer Technology, Technical College of Dammam, Technical and Vocational Training Corporation, Sakaka, Saudi Arabia
[2]Department of Computer Science, Higher Institute of Technological Studies Mahdia, Hiboun, Tunisia
[3]Department of Computer Engineering, College of Engineering, Ahlia University, Manama, Bahrain
[4]Department of Electrical Engineering, National School of Engineering, Sfax University, Sfax, Tunisia

Article Info

Article history:

Received Aug 23, 2021
Revised May 18, 2022
Accepted Jun 14, 2022

Keywords:

Awareness
Mobile apps
Privacy
Recommender system
Security

ABSTRACT

There is an enormous number of mobile apps, leading users to be concerned about the security and privacy of their data. But few users are aware of what is meant by app permissions, which sometimes do not illustrate what kind of data is gathered. Therefore, users are still concerned about security risks and privacy, with little knowledge and experience of what security and privacy awareness. Users depend on ratings, which may be fake, or keep track of their sense to install an app, and an enormous number of users do not like to read reviews. To solve this issue, we propose a recommender system that reads users' reviews, and which exposes flaws, violations and third-party policies or the quality of a user's experience. In order to design and implement our recommender, we conduct a survey which supports two significant points: to detect the level of security and privacy awareness between users, and to gather new words into a dictionary of a recommender system, which assists to classify each review on the correct level, which can indeed reveal the scale of security and privacy in an app.

Corresponding Author:

Hameed Hussain Almubarak
Department of Computer technology, Dammam Technical College
Prince Mohammed Bin Fahad Branch Road، Al Firdaws, Dammam 32251, Saudi Arabia
Email: halmubarak@tvtc.gov.sa

1. INTRODUCTION

Currently the digital world has millions of mobile applications which interfere directly or indirectly to our personal's information such as location, name, and photos. The increase of numbers and diversities of apps lead to rise in synchronized way with threats, security risk and privacy issues which can impact the user data privacy. To evaluate the level of security and privacy, the users' reviews can be used to extract from their experiences to identify to what extent these applications security and privacy might be trusted. In addition, some of mobile apps provide information about their privacy and security level that can be use as index-helper in evaluation [1], [2]. On the other hand, the tricky matter that facing us is "Arabic language" is a semantic language with a complicated morphology, which is significantly different from the other popular languages, and thus to satisfy this large number of Arab users in terms of security and privacy on mobile apps we should take on consideration the special features of Arabic language.

Arab states are around 500 million people which they use Arabic language with different dialects beside classical one for instance Middle East and the dialects of the Maghreb, dialects of the Bedouin and the dialects of the people of cities and villages. In this case study we have been faced the dealing with reviews written in different Arab dialects. In many cases, one orthographic word in Arabic language comprises many

semantic and syntactic words. In addition of classical Arabic, there are two types of morphology: roots morphemes and affixes morphemes [1]. In this context, our work is to develop a privacy and security awareness recommender for the Arabic users in particularly. The recommender system be able to classify enormous of users' reviews in Arabic dialects, then it will determine the level of apps security and privacy [3], [4].

The rest of the article is structured as follows: the second section briefly presents the Arabic language specification. Also, it provides an overview of related work of recommender system in term of security and privacy. The third section illustrates the conducted survey results in objective to design our recommender with high performance. and the design assumptions adopted to establish the proposed system. The exhaustive methods for implementing the cluster selection mechanism and the trust system evaluation are provided in the fourth section. The fifth section analyses simulation results by highlighting the improvements achieved by the proposed protocol as compared to state-of-art techniques. Finally, we conclude the paper and highlights future work based on paper contributions.

2. RELATED WORK

There have been many studies deal with security and privacy by using a recommender system or survey. While, there still several issues with permissions in app and awareness of user about security and privacy. In this section, we present an overview for the Arabic language characteristics and present a survey result to solid our work.

2.1. The Arabic language: overview

The Arabic language is one of the most popular languages around the world and is commonly used on the internet and social media. It is considered one of the top six languages worldwide. Over 200 million people are native Arabic speakers, distributed over 20 countries [5].

Many researchers such as Perrin 2015 agreed that Unlike English language, characteristics of Arabic languages makes it is complex to developed in term of Corpora and some classifier tools, compared to the English language. Hence, it is stated that, in daily life and social media as well, the Arabic language is manifested in three forms: i) classical Arabic, the Holy Quran language, ii) modern standard Arabic (MSA), the formal Arabic used for professional purposes like books, media and education and which is easy to understand for all Arabs from different regions, and iii) dialectal Arabic (DA), the local dialects for Arabs which differ based on geographical regions, and which consists of four regions: i) Sudan and Egypt, ii) Lebanon, Syria, Jordan, and Palestine, iii) Gulf (Iraq, Kingdom of Saudi Arabia (KSA), United Arab Emirates (UAE), Kuwait, Qatar, Bahrain, and Yemen), and iv) Libya, Tunisia, Algeria, and Morocco [1]–[6].

2.2. Recommender systems

Social networks content is increasing steadily with a large amount of information like data, images, videos, contents, and documents that are shared on these networks which can be noisy and heterogeneous. Hence, this continuous huge increase in data needs to be organized and arranged in a way that allows users to extract the needful information easily. Previously, this demand could be achieved through recommender systems.

The field of recommender systems has its origins in the mid-1990s. Recommender system is an information filtering system that aims to solve the problem of information overload to users and suggest useful information to targeted users [7]–[9]. This is becoming increasingly important to e-commerce and social media sites. It helps to make decisions regarding products to buy and businesses to patronize.

Recommender systems (RSs) are built and developed based on users' textual reviews, ratings and comparative opinions [10]. There are four different approaches used in developing RSs, including content-based (CB) filtering, collaborative filtering (CF), hybrid-based (HB) filtering, and knowledge-based (KB) filtering. When using a CF or a HB filtering approach, RSs must gather information regarding the user in order to develop recommendations [9]–[11].

2.3. An android permission control recommender system based on crowdsourcing

Mobile applications may be a concern to users due to risks of data security and privacy, because apps request many permissions which users do not fully understand, and apps do not disclose all information about the purposes of these permissions. Rustgi and Fung worked to improve a recommender system (DroidNet) by showing app permissions to the user, so that the user could agree or disagree to installing the app after seeing recommendations about the app [9]. This technique can reduce a user's concern around security and privacy. Moreover, DroidNet has a database which gathers all the user's permissions from the mobile and another database that is online. The significant point here is the linking between the two databases, which is immediately up to date. Also, DroidNet's recommendations are supported by expert users

who deal with apps. In sum, this paper illustrates that DroidNet is considered an effective recommender system that gives recommendations based on expert users and database [12]–[14].

3. SURVEY

The aim of the survey is to discover users' level of security and privacy awareness, and whether they have enough knowledge about security risk and privacy in mobile apps. Further, we attempt to gather words relevant to the description of security and privacy, which will use in the recommender system. It will be a good tool to help users know the level of security and privacy in an app, especially for those who prefer not to read reviews before downloading an app.

3.1. Result of survey

Findings of survey illustrates users' awareness around security and privacy, and which words are collected through survey. It extends to investigate how users deal with apps' privacy policy and third- party too, which really illustrates user's level of knowledge about security and privacy awareness. Firstly, we created the design of the questionnaires online using Google Drive. Then, it was distributed to many people who speak Arabic. There were 827 participants who responded to the survey through the internet; they are from 17 countries such as Saudi Arabia, Kuwait, Oman, Iraq, the United Kingdom (UK), and Turkey.

As shown in Figure 1, around 250 participants read the privacy policy of apps, while 577 of participants do not care about it. This shows how users who download apps still do not realize the significance of security and privacy. Also, other studies also found similar findings, such as the experiment in Universiti Sains Malaysia BYOD, 2017 where it was found that more than 50% of sharers do not read the guidelines of privacy [15].

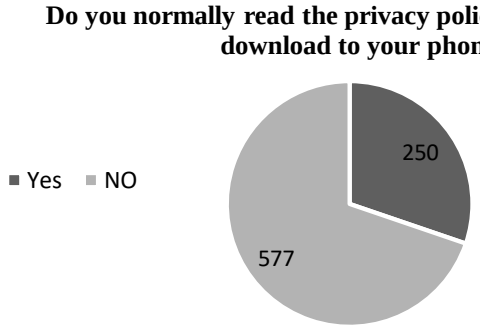


Figure 1. Users' lack of awareness about privacy policy when downloading an app

As shown in Figure 2, 617 participants prefer to use a recommender system before installing an app. Based on these answers, it is demonstrated that users realize the significance of a system of recommendations, even though 210 participants prefer not to use it. However, there are many recommender systems that focus on detecting permissions and showing them to a user; they can also show the scale of security and privacy on apps. Therefore, we work beside this survey to create a recommender system to support my aim about users' reviews. The result of the question of how important the recommender system can be obvious, as it can reduce security risk, and helps users to make the correct decision around installing apps [12], [16], [17].

The question shown in Figure 3 is significant in the survey because it allows the gathering of expressions and words about security and privacy awareness that can support my recommender system's dictionary. However, about 143 participants provided their comments, while 684 participants did not provide their views on any app after they downloaded it. There are 127 comments written by participants who said 'yes'; also, 16 comments came from participants who said 'no'. Therefore, there are 25 comments that are useful and usable in the dictionary. They include an enormous number of words (lexical and semantical) which involve the meaning of security and privacy awareness, as shown in Table 1 [18], [19].

Figure 4 illustrates the number of participants who provided their information when downloading an app. Further, around 300 participants provide their email, location and mobile number when they would like to install an app, while four participants provided everything to download an app. Figure 5 illustrates the number of participants who chose the factor 'security and privacy' as impacting on their decision before downloading an app (around 61.4%). In addition, the factor 'quality of app' affected exactly 58.8% of

participants' decisions before installing an app, which is slightly lower than security and privacy, and which shows how users have knowledge about protecting their sensitive data. Moreover, 'advertising' and 'ratings' can impact on users' decisions to download an app (42.6% and 44.7%, respectively). Of the participants, 17% are impacted by message errors (report bug). This question deeply shows the significance of security and privacy in users' awareness.

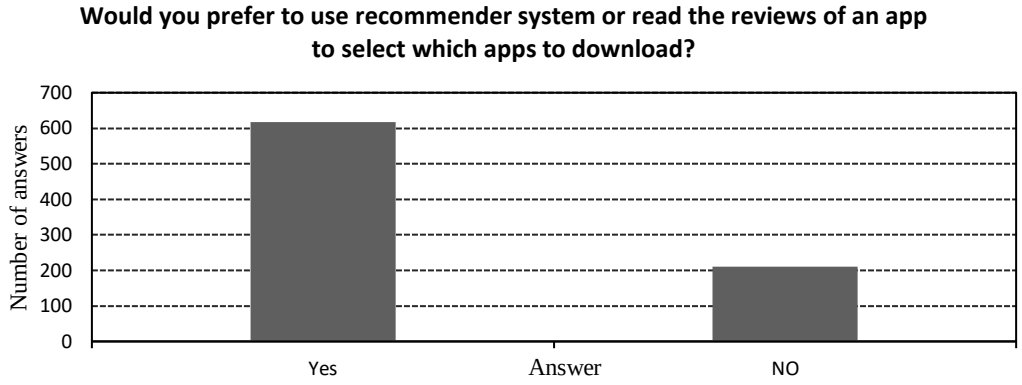


Figure 2. Needing the recommendation system

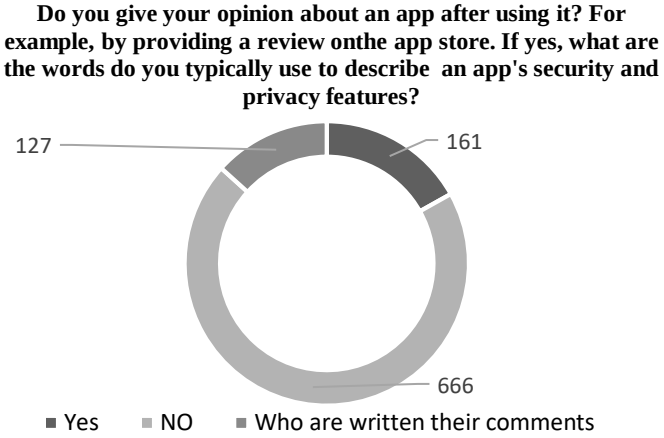


Figure 3. Six hundred and sixty-six participants did not write comments on the app

Table 1. Dictionary's words

Dictionary (Words About Security and Privacy)				
Top	Above of Medium	Medium	Low	Very Low
أمن	تثق فيه	محسن	ليس أمن	الاحتيال
Secure	Trust it	Enhance	Not secure	fraud
قيود	سري	حسن	الاختراق	انتهاك
Restrictions	Secret	better	hack	Violation
مضمون	احترام حقوق	مستحسن	غير محمية	خطر
Guaranteed	Respect for rights	Recommended	Not protected	Dangerous
حماية	أمان	لأباس فيه	عيب	منتهك الخصوصية
Protect	Safe	Not bad	Flaw	Violate privacy
خاص	كلمة مرور	محدود	ليس أمان	ضعيف جدا
Private	Password	Limited	Not safe	Very weak
ثقة	المصادقة	غير معقد	بدون قيود	تسرب البيانات
Confidence	Authentication	Uncomplex	Without Restrictions	Data leak
معتمد	سرية	أذونات أقل	ضار	سرقة الفيزا
A certified	Secrecy	Fewer permissions	Harm	Theft of the credit card

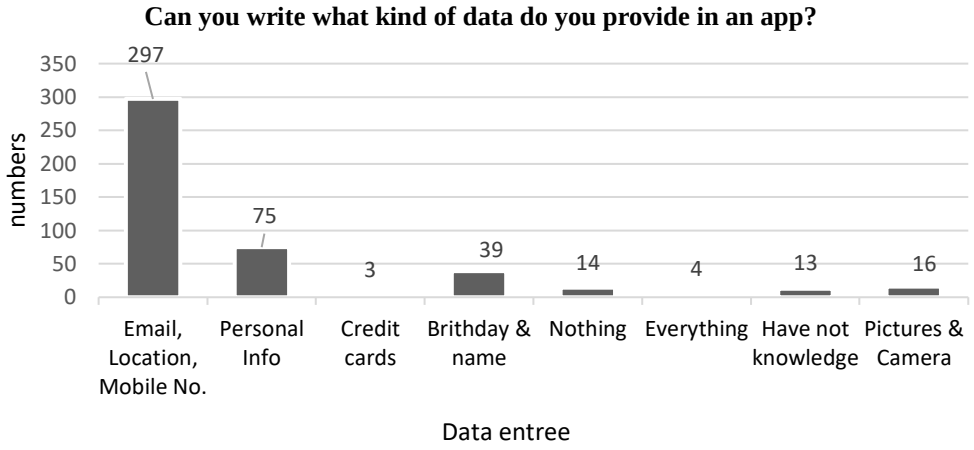


Figure 4. Factors affecting decision to download

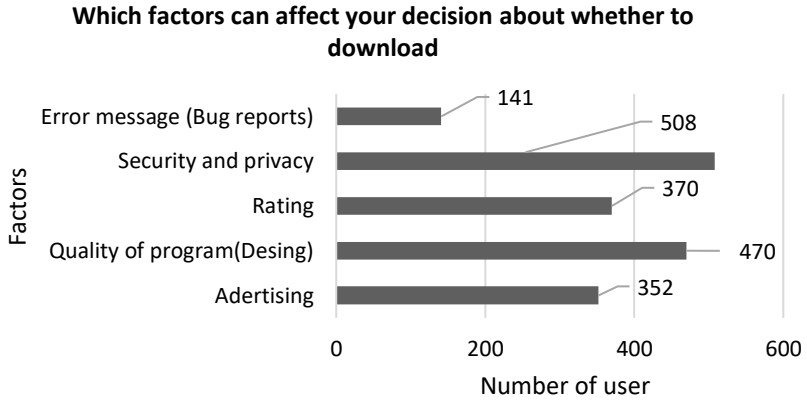


Figure 5. Security and privacy are the highest affective

3.2. Survey discussion

There are two significant parts of survey: i) to gather words for recommender system's dictionary and ii) to discover level of users' security and privacy awareness by their answers in the survey. Firstly, in Figure 3 and Table 1, it is demonstrated how participants do not care about reviews, which we believe includes sensitive words about security and privacy. Few participants provide words about security and privacy, but this is a slightly weak result. In addition, Figure 5 provides some information that participants provide to apps before downloading them. Therefore, many users still struggle with apps that request they insert their information before installing them, and which sometimes extend the request to include sensitive data which is then saved, such as credit card information. These questions reflect users' low awareness.

Secondly, Figures 1 to 4 involve specific questions about security and privacy, which we can use to dramatically determine users' level of awareness. Figure 1 illustrates users' unawareness about privacy policies, but they do have knowledge that the issue of their data is serious, so they select to use a recommender system to avoid leaking their data or at least reduce threats, as shown in Figure 2. Moreover, Figure 5 shows that security and privacy are a priority for users.

4. RECOMMENDER SYSTEM FOR SECURITY AND PRIVACY

It acts as reader where it reads users' reviews and assists them to pay attention to level of security and privacy in apps before they download them. That allows users to take an obvious decision about app if they want to install it or not. Also, recommender system can assist the users to prevent effectively what is considered as threat or violation to their security and privacy or "unexpected data collection practices" [17], [20].

4.1. Users' reviews

We select users' reviews from Google Play; this allowed to gather many words to illustrate the level of security and privacy. To build a recommender system requires an enormous number of words (lexical or semantical). Therefore, we gathered 1,354 comments from these groups (21 games, 16 education apps, 20 shopping apps and 10 social media apps) which were relevant to security and privacy. The aim of this work is to fully understand the context of users' reviews and collect each word relevant to security and privacy. Therefore, we can increase the words (lexically and semantically) in the recommender system's dictionary, which helps it to classify and evaluate each review for an app.

4.2. Dictionary

The dictionary includes lexical and semantic words. I classify the words based on their relevance about security and privacy. In addition, I attempt to insert each word into as correct a place as possible in the dictionary based on whether the word is close to a security expression or privacy expression. After that, I attempt to weigh the word about which level it will be (where five is strong and one is weak) as shown in Tables 2 and 3.

Table 2. Recommender system's dictionary-privacy

Privacy				
5	4	3	2	1
السرية	سياسة ذات معايير عالية	سياسة غير واضحة	استغلال	تسرب البيانات
Confidentiality	High standards police	Unclear policy	Exploit	Data leak
خاص	أذونات أقل	طلب أذونات	بدون قيود	منتهك الخصوصية
Private	Less permissions	Request Permissions	Without Restrictions	Violate privacy
نزاهة	حفظ البيانات	رسالة إعلانية	رسائل خاطئة	الاحتيال
integrity	Save Data	Advertising message	Error messages	Fraud
أو غير مسموح غير مصرح	احترام حقوق	مقبول أو مرضي	الوصول للبيانات	إعلانات إباحية
Not Allowed	Respect for rights	Satisfaction	Access to Data	Porn ads
خصوصية	حجب أو منع الوصول للبيانات	سياسة الخصوصية متغيرة	طلب تصريح	طرف ثالث
Privacy	Prevent Access to data	privacy policy changeable	Request Authorization	Third Party

Table 3. Recommender system's dictionary- security

Security				
5	4	3	2	1
أمن	تثق فيه	محسن	ليس أمن	غير محمي
Secure	Trust it	Enhance	Not secure	Not protected
حماية	كلمة مرور	حسن	ليس أمان	الاختراق
Protect	password	better	Not safe	Hack
معتمد	سري	مستحسن	عيب أو خلل	لا يمكن اثق فيه
A certified	Secret	Recommended	Flaw	Do not Trust it
الأمن عالي	أمان	محدود	غير مشفر	غير معتمد
High security	Safe	Limited	Not encrypted	Without certification
مشفر	أمانة	غير محدث	يمكن اختراقه	يمكن كسر كلمة المرور
Encrypted	integrity	not up to date	vulnerable	Crack

4.3. Recommender system's diagram

"A recommender system is algorithm whose aim is to provide the most relevant information to a user by discovering patterns in a dataset." (Dictionary and Recommendation system), machinimas of recommender system as presented in Figure 6. The diagram describes the different steps we took to build my learning model and its implementation by the recommendation application. These steps are briefly described:

- Reviews collection process: This consists of collecting reviews from the open-source Google Play Store platform using Google Play Scraper. The collected data set contains 954,684 reviews obtained from 2,816 apps. I chose the last 500 reviews in Arabic for each app, if there are any. This data set will be cleaned and then harvested to create the classifier's training features.
- Pre-processing of reviews: This is the stage of preparing reviews to create the training data, it mainly comprises the following processing: i) Tokenization: tokenizing a review amount to separating it into tokens, that is to say into distinct words or symbols. From a review we extract a vector of tokens, ii) lexical standardization: in the Arabic language some characters can be written in several ways, this step will allow them to be standardized, iii) english words remover: some reviews contain in addition to words in Arabic other words containing Latin characters, a function will take care of them, and iii) remove stop words: stop words are words that are so common that it is unnecessary to index them or use them in learning.

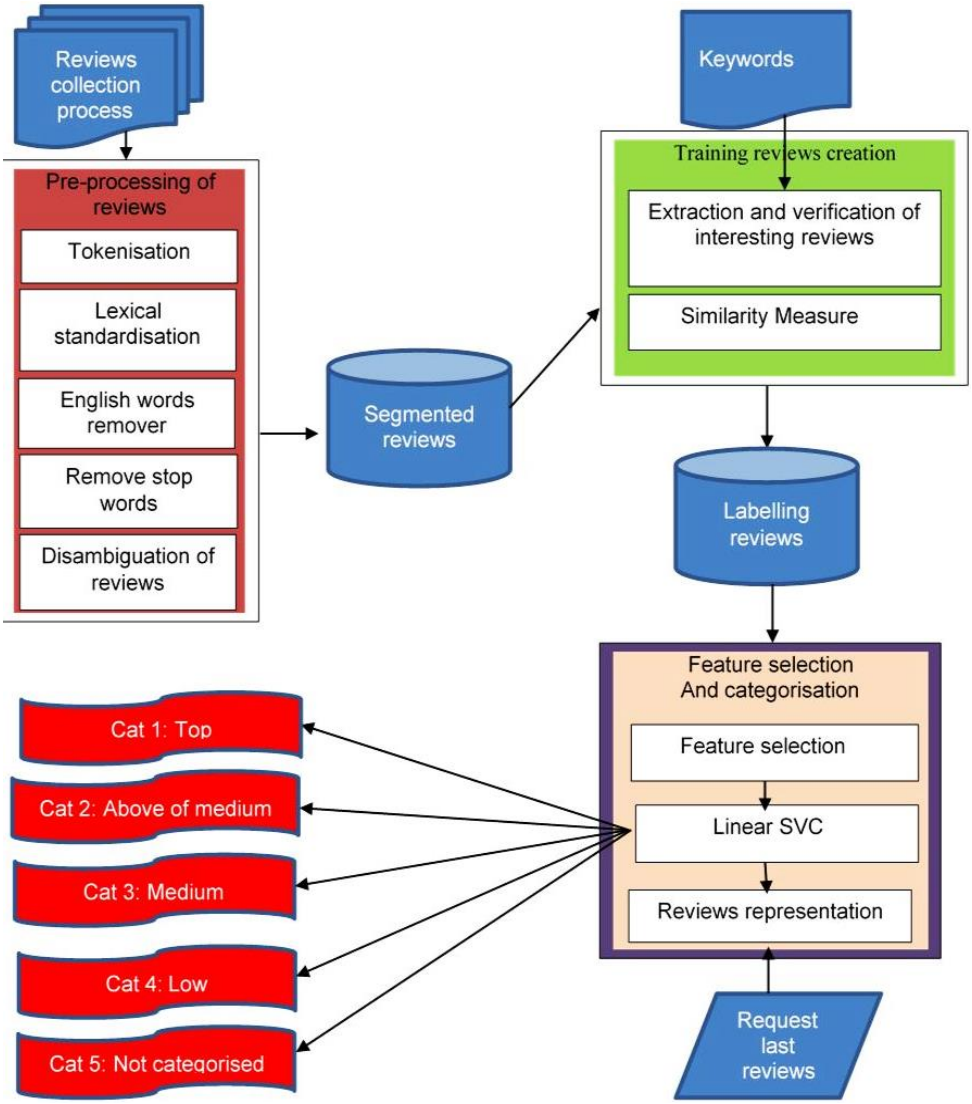


Figure 6. Recommender system's diagram

Disambiguation of reviews: functions will try to detect and delete certain reviews that do not provide any textual information (repetition of the same characters, set of images and emoji ...)

- Segmented reviews: The result of the pre-processing phase is a data set containing all the reviews cleaned up and ready for the labelling phase.
- Keywords: it is the set of words constituting the dictionary.
- Training reviews creation: This is the labelling phase; it consists of assigning each review a label defining its class from 0 to 5 where 0 is the class of reviews not concerning the topic (security or privacy) and the other classes from 1 to 5 from very low to top. This is done according to the dictionary classification of keywords.
- Labelling reviews: It is all the reviews labelled and ready for training.
- Feature selection and categorization: This is the classification stage where after extraction of the features, the classification algorithm by LinearSVC is applied to build two models, one for security and the other for privacy, this model is exported into the web application that collects the online reviews (request last reviews) and apply the model to decide which class corresponds to the review.

The remaining sentences are called 'not categorized reviews' (class 0). We define the representative reviews as what contains pre-defined keywords of the category in its content. Nevertheless, there exist error reviews in the representative reviews, which we will eliminate. As similar words tend to appear in similar contexts, we compute the similarity by using contextual information. This step is done twice, one for security classes and the other for privacy as shown respectively in the Figures 7 and 8.

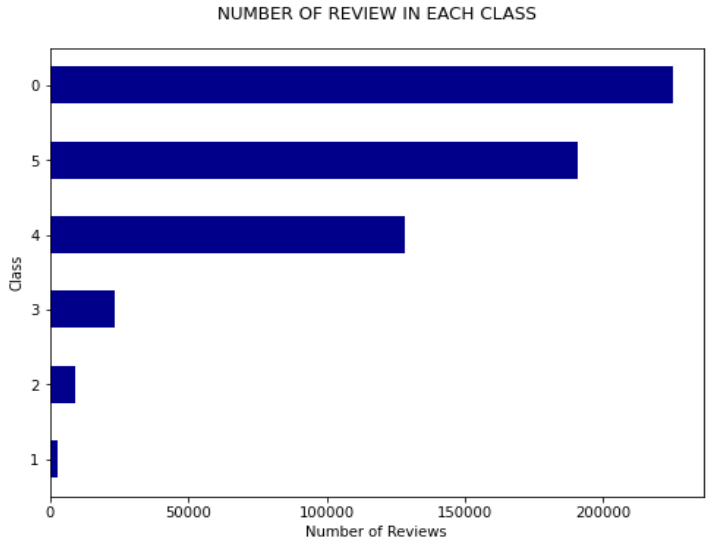


Figure 7. Number of users for the security class

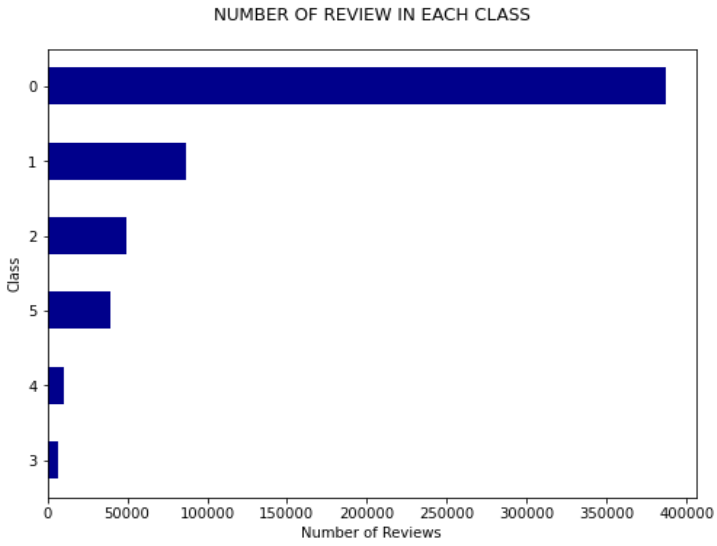


Figure 8. Number of users for the privacy class

4.3.1. Unbalanced data

Learning from imbalanced data is a difficult task since most learning systems are not prepared to cope with a large difference between the number of cases belonging to each class. Researchers have reported difficulties to learn from imbalanced data sets in several domains [20]. To overcome these difficulties, two main solutions are proposed in the literature: one is based on the adaptation of learning algorithms and the other on the modification of the size of the data in order to make them balanced. we opted for the second strategy which generally offers three alternatives:

- Under-sampling: this method aims to balance the data set by eliminating examples of the majority class.
- Over-sampling: this method replicates examples of the minority class in order to achieve a more balanced distribution, by data duplication or self-generation of new data synthetic minority oversampling technique (SMOTE).
- A combination of over- and under-sampling.

Given the difficulty of applying over-sampling, we opted for under-sampling by trying to balance the data according to the minority class and by performing the performance tests to find the ideal size for the other classes. Technically we worked with 'imbalanced-learn application programming interface (API'1),

which provides the necessary methods to perform under-sampling in several ways, but we opted for the random under-sampling technique by fixing the size of the samples of each class according to the test's performance.

4.3.2. Feature extraction

The reviews must be parsed to remove words, known as tokenization. Then, the words need to be encoded as integers or floating-point values for use as input to a machine-learning algorithm, known as feature extraction (or vectorization). For this step we used the '*TfidfVectorizer*' 2 method which converts a collection of raw documents to a matrix of TF-IDF features. The term frequency/inverse document frequency (TF/IDF) model learns a vocabulary from all of the documents, then models each document by calculating a numerical statistic for each word of the document that reflects how important the word is to the document.

Note that this method comes with options to limit the number of features by setting a '*max_features*' option by ignoring terms that have a document frequency strictly lower than the '*min_df*' threshold and/or by ignoring terms that have a document frequency strictly higher than the '*max_df*' threshold and ignoring the stop words. Given the specificity of the Arabic language and the presence of double and triple words in the dictionary of keywords, we defined the parameter '*ngram_range*' to the tuple (1,3), the lower and upper boundary of the range of n-values for different n-grams to be extracted. All values of n such that 1<=n<=3 will be used.

This method consists of representing the reviews by n-grams. The n-gram is a sequence of n consecutive words (in our case). It consists of splitting the text into several sequences of n words by moving with a window of one word. This technique has several advantages. The n-grams automatically capture the roots of the most frequent words without going through the step of searching for lexical roots; these spaces are considered, independent of the language. In fact, not taking them into account introduces noise.

4.3.3. Classification

The classification of texts includes a choice of learning technique (or classifier). Some of the most commonly used learning methods include: naive Bayes, support vector machine, k-near neighbors and decision trees. Usually, the choice of classifier is based on the end goal to be achieved. If the end goal is, for example, to provide an explanation or a rationale that will then be presented to a decision-maker or expert, then methods that produce understandable models such as decision trees are preferred. But it remains difficult to replace tests to know which classifier is appropriate for which situation. In our case we tested three learning techniques namely:

- Random Forest Classifier3 (random forest classifier): 'Random forests are a combination of tree predictors such that each tree depends on the values of a random vector sampled independently and with the same distribution for all trees in the forest. The generalization error for forests converges as. to a limit as the number of trees in the forest becomes large' [21], [22].
- Linear SVC4 (linear support vector classification): this is a faster implementation of support vector classification (SVC) for the case of a linear kernel. LinearSVC implements the 'one-vs-the-rest' multi-class strategy.
- Multinomial NB5 (naive Bayes classifier for multinomial models): this implements the naive Bayes algorithm for multinomially distributed data, and is one of the two classic naive Bayes variants used in text classification (where the data are typically represented as word vector counts, although TF-IDF vectors are also known to work well in practice).

5. TEST AND EVALUATION OF TRAINING PROCESS

The experimental evaluation of classifiers is the last step in the indexing process. It usually attempts to assess the effectiveness of a classifier, namely its ability to make classification decisions. There are numerous measures for this, each highlighting a particular property of the system. I retained the following, most widely used measures: i) recall, which is synonymous with the true acceptance rate, ii) precision, which measures the rate of correct answers among positive answers, iii) the F1-score, which synthesizes the first two, and iv) accuracy, which represents the number of correctly predicted data out of all the data. Consider the following appointments [23].

- TP (true positive); i.e. the number of documents correctly attributed to a class,
- FN (false negative); i.e. the number of documents incorrectly attributed to a class,
- FP (false positive); i.e. the number of incorrectly rejected documents assigned to a class, and
- TN (true negative); i.e. the number of correctly rejected documents attributed to a class.

$$recall = TPTP+FN \quad (1)$$

$$precision = \frac{TP}{TP+FP} \quad (2)$$

$$f1-score = 2 \times \frac{recall \times precision}{recall+} \quad (3)$$

$$accuracy = \frac{TP+TN}{TotalSample} \quad (4)$$

Equations to compute the recall and the precision [24], [25]. An experimental comparative study between these three classifiers was carried out and the different performance scores are indicated in Table 4 for the security and privacy model. Considering the previous comparisons, the model based on linearSVC was generated and exported to the application (website).

Table 4. Result of experiment

Models		Performance			
	Security/Privacy	Recall (weighted avg)	Precision (weighted avg)	F1-score (weighted avg)	Accuracy
LinearSVC	Security	0.88	0.89	0.88	0.88
	Privacy	0.87	0.88	0.87	0.87
Random Forest	Security	0.77	0.82	0.77	0.77
	Privacy	0.81	0.82	0.80	0.81
MultinomialNB	Security	0.66	0.79	0.68	0.66
	Privacy	0.60	0.79	0.63	0.60

5.2. Challenges

Several challenges were met throughout this work. The first concerns the collection of reviews and the extraction of the keywords constituting the dictionary. Therefore, we wrote a python script using Google Play Scraper to extract reviews from the Google Play Store, which allowed to automate this collection. After studying the result, we noticed some problems, such as the fact that reviews are generally written using very varied dialects depending on the region, with no respect for lexical or grammatical rules of the Arabic language, which forced to rule out any sort of classic pre-processing on these reviews. The most delicate step was the labelling of the reviews because this step is crucial to learning and is usually carried out by an expert and requires a huge amount of time, but our choice was to automate it using the term-matching technique.

The second challenge concerned understanding the machine-learning world, with all the details concerning supervised and unsupervised learning, classification algorithms, how to work with unbalanced data, how to evaluate a classifier and how to generate a model that we could integrate in our recommender system. The third challenge was the creation of the website which should highlight our machine-learning model and take advantage of the results obtained. The choice was to use a python framework trained in web development which was capable of using models generated natively. After a comparison between Django and Flask, our choice was fixed on the latter.

6. RECOMMENDER SYSTEM'S WEB SITE

A website is considered the interface of the recommender system, which allows users to check the level of security and privacy of an app. The website involves two parts, as shown in Figure 9. The two parts are; i) keyword part: where the main word of the app is entered that the user wants to search for and ii) search button: to make search Engine work to find all apps that have related to the main word.

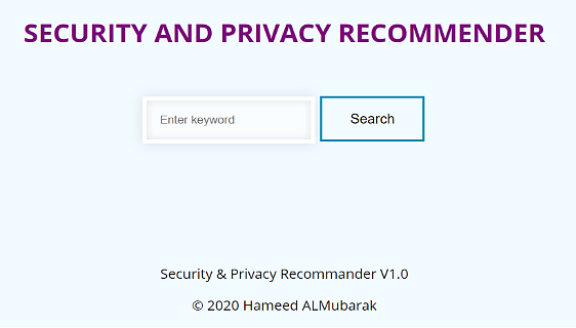


Figure 9. Interface of the recommender system

Users can search for any application they would like to make sure it is safe and will protect their data. Here, I applied a simple experiment on the web engine to search for the social media section. First, we selected the IMO app to check the level of security and privacy on it. In the second step, the recommender system will gather all applications that have links with this keyword (IMO), as shown in Figure 10.

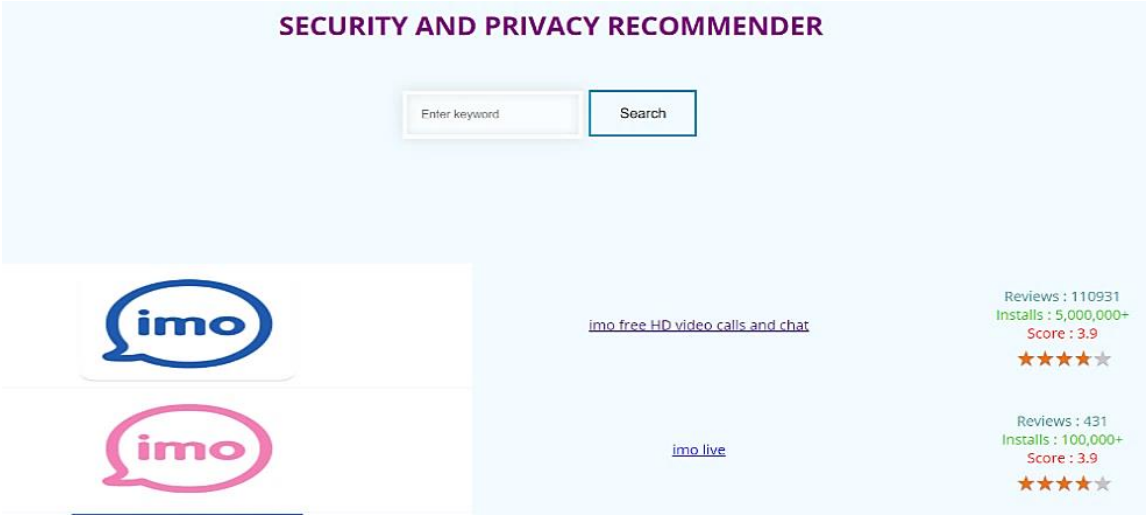


Figure 10. Result of the recommender system's search

Here, the recommender illustrates three parts for each app: number of reviews, number of users who downloaded the app, and Google score. Next, I clicked on the first app to show the results of the recommendation, which demonstrated four features, as shown in Figure 11. The three parts are;

- Google's score of the app, which comes from users
- The recommender's result which includes two parts: i) The most predicted class, which shows the most class, repeated after processing and ii) The mean, which computes all reviews found in the class, and divides it by the number of these classes.
- Relevant Reviews: 639, which the recommender system gathered to give this score to the app.

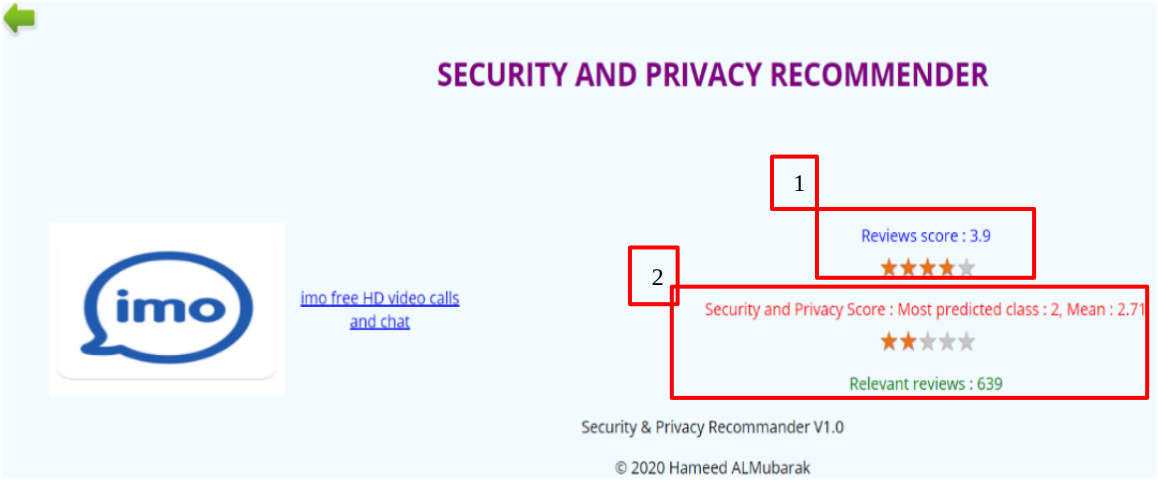


Figure 11. The recommender's result for social media

The mean computes all reviews found in the class and divides it by the number of these classes. Here is a simple example, to clarify:

Security: class1=4, class2=51, class3=89, class4=46, class5=23.
Privacy: class1=129, class2=162, class3=2, class4=63, class5=70.
- Most predicted class = 2 (213 reviews)
- Mean= (4*1+51*2+89*3+46*4+23*5 + 129*1+162*2+2*3+63*4+70*5)/639= 2.71
- Relevant reviews➔ 639

Note**:** The recommender system's result also shows the number of reviews related to security and privacy. It collects only 2,000 reviews. However, we can modify the number of gathered reviews, but it affects the time taken for the recommender system to process the reviews.
Q: What is the correlation between most predicted class and mean?
A: When the results for the predicted class and the mean are the same or close, this means that the recommender system has given the user an accurate score about the app's level of security and privacy, but if there is a gap between the results, the user should follow the most predicted class because there are many reviews that are unobvious (noise review).

7. CONCLUSION

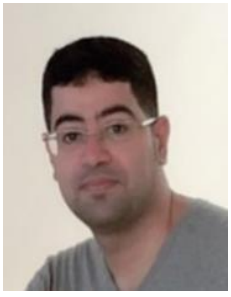
In the first part of our study regarding the level of users' awareness about security and privacy, participants still struggle with the enormous number of apps and their requests. Also, participants do not make it a priority to read an app's reviews, which would probably allow them to discover the security risks and threats to their data; they can also affect a user's awareness, so users' awareness currently is acceptable when compared to previous research where users' awareness was low when dealing with smartphones. The second part of our study is the recommender system, the fundamental concern of which is about an app's reviews and which classifies them to five levels based on relevant reviews about security and privacy. Therefore, the recommender system dramatically worked on an app's reviews to gather all relevant reviews about security and privacy and then showed the level of security and privacy of the app and mean value of the app. The recommender system has largely achieved the aim of study, regardless of the difference between the most predicted class and the mean value in some of the apps' results, while the predicted class correctly evaluates the level of security and privacy of an app. As a result, the recommender system of reviews can play a main role in discovering the threats to privacy and security risk by apps. There are some limitations; in the survey: I did not obtain enough comments, which assists to fully understand words of security and privacy. In addition, in implementing recommender system: the limitation comes from the google API which limits the loading of reviews to 40 for each app. In future, recommender system can be extended to figure out any permissions violations of privacy. Regarding the application, we plan to improve it by manually revising the labelling phase and adding other reviews from the app store, which will necessarily improve the learning model and add the possibility of searching from other stores.

REFERENCES

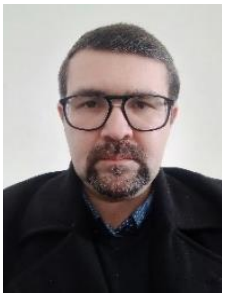
[1] H. Almuhimedi *et al.*, "Your location has been shared 5,398 times!," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Apr. 2015, pp. 787–796., doi: 10.1145/2702123.2702210.
[2] G. E. Batista, A. L. C. Bazzan, and M.-C. Monard, "Balancing training data for automated annotation of keywords: a case study," *Journal of artificial intelligence research*, vol. 3, no. 2, pp. 15–20, 2003
[3] H. Ko, S. Lee, Y. Park, and A. Choi, "A survey of recommendation systems: Recommendation models, techniques, and application fields," *Electronics*, vol. 11, no. 1, Jan. 2022, doi: 10.3390/electronics11010141.
[4] B. H. Jones and A. G. Chin, "On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time," *International Journal of Information Management*, vol. 35, no. 5, pp. 561–571, Oct. 2015, doi: 10.1016/j.ijinfomgt.2015.06.003.
[5] S. Shorman and M. Al-Shoqran, "Analytical study to review of Arabic language learning using internet websites," *International Journal of Computer Science and Information Technology*, vol. 11, no. 02, pp. 37–44, Apr. 2019, doi: 10.5121/ijcsit.2019.11204.
[6] T. Alanzi, "A review of mobile applications available in the app and Google play stores used during the COVID-19 outbreak," *Journal of Multidisciplinary Healthcare*, vol. 14, pp. 45–57, Jan. 2021, doi: 10.2147/JMDH.S285014.
[7] A. Perrin, *Social media usage: 2005–2015*. Pew Internet & American Life Project, Washington DC, 2015.
[8] I. Portugal, P. Alencar, and D. Cowan, "The use of machine learning algorithms in recommender systems: a systematic review," *Expert Systems with Applications*, vol. 97, pp. 205–227, May 2018, doi: 10.1016/j.eswa.2017.12.020.
[9] P. Rustgi and C. Fung, "Demo: DroidNet - an android permission control recommendation system based on crowdsourcing," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 737–738.
[10] A. Balapour, H. R. Nikkhah, and R. Sabherwal, "Mobile application security: role of perceived privacy as the predictor of security perceptions," *International Journal of Information Management*, vol. 52, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.102063.
[11] A. Shoufan and S. Alameri, "Natural Language processing for dialectical Arabic: a survey," in *Proceedings of the Second Workshop on Arabic Natural Language Processing*, 2015, pp. 36–48., doi: 10.18653/v1/W15-3205.
[12] F. Ricci, L. Rokach, and B. Shapira, "Recommender systems: introduction and challenges," in *Recommender Systems Handbook*, Boston, MA: Springer US, 2015, pp. 1–34., doi: 10.1007/978-1-4899-7637-6_1.
[13] K. Kowsari, K. Jafari Meimandi, M. Heidarysafa, S. Mendu, L. Barnes, and D. Brown, "Text classification algorithms: a survey,"

Information, vol. 10, no. 4, Apr. 2019, doi: 10.3390/info10040150.
[14] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers and Security*, vol. 34, pp. 47–66, May 2013, doi: 10.1016/j.cose.2012.11.004.
[15] M. Koyuncu and T. Pusatli, "Security awareness level of smartphone users: an exploratory case study," *Mobile Information Systems*, vol. 2019, pp. 1–11, May 2019, doi: 10.1155/2019/2786913.
[16] B. Liu *et al.*, "Follow my recommendations: a personalized privacy assistant for mobile app permission," in *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016, pp. 27–41.
[17] M. Mahinderjit, C. Wai, and Z. Zulkefli, "Security and privacy risks awareness for bring your own device (BYOD) paradigm," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 2, pp. 53–62, 2017, doi: 10.14569/IJACSA.2017.080208.
[18] Y. Sun, A. K. C. Wong, and M. S. Kamel, "Classification of imbalanced data: a review," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 23, no. 04, pp. 687–719, Jun. 2009, doi: 10.1142/S0218001409007326.
[19] R. Zafarani and H. Liu, "Connecting users across social media sites," in *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, Aug. 2013, pp. 41–49., doi: 10.1145/2487575.2487648.
[20] L. Brieman, "Random forests," *Machine Learning*, vol. 45, pp. 5–32, 2001, doi: 10.1023/A:1010933404324.
[21] Z. Benenson, F. Gassmann, and L. Reinfelder, "Android and iOS users' differences concerning security and privacy," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems on - CHI EA '13*, 2013, p. 817., doi: 10.1145/2468356.2468502.
[22] X. Liang, J. Tian, X. Ding, and G. Wang, "A risk and similarity aware application recommender system," *Journal of Computing and Information Technology*, vol. 23, no. 4, pp. 303–315, 2015, doi: 10.2498/cit.1002537.
[23] B. Markelj and I. Bernik, "Safe use of mobile devices arises from knowing the threats," *Journal of Information Security and Applications*, vol. 20, pp. 84–89, Feb. 2015, doi: 10.1016/j.jisa.2014.11.001.
[24] A. Anandhan, L. Shuib, M. A. Ismail, and G. Mujtaba, "Social media recommender systems: review and open research issues," *IEEE Access*, vol. 6, pp. 15608–15628, 2018, doi: 10.1109/ACCESS.2018.2810062.
[25] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, Aug. 2014, pp. 951–960., doi: 10.1145/2623330.2623705.

BIOGRAPHIES OF AUTHORS



Hameed Hussain Almubarak received the master degree in network and security in 2020 from University of Kent. He educates many courses in computer and networks security and he have been working in the Technology College at Dammam for 20 years. Moreover, he worked on some researches. He can be contacted at email: halmubarak@tvtc.gov.sa.



Mohamed Khairallah Khouja received the Master degree in computer science from Monastir University, Tunisia, and Operations Research Combinatorics Optimization from Joseph Fourier University and National Polytechnic Institute of Grenoble, France. He is a Technologue at the Department of Computer Science, Higher Institute of Technological Studies Mahdia, Tunisia, he is interested in areas related to artificial intelligence, machine learning, deep learning and data science. He can be contacted at email: mohamedkhairallah.khouja@mahdia.r-iset.tn.

Ahmed Jedidi received Ph.D. degree in System of Computer Engineering in 2012 at the National School of Engineering Sfax University Tunisia. Also, he is a member in the laboratory "Computer & Embedded Systems" University of Sfax, Tunisia. The line of research focuses on the detection, localization and estimation of crosstalk in all-optical networks (AONs), the embedded system performance, optical network communication and Wireless sensor network. Besides, he has a number of research papers published in international journals and conferences. He has more than 10 years' experience in teaching in various universities in Tunisia and Saudi Arabia. Particular, he teaching computer and network courses. He can be contacted at email: ajedidi@ahlia.edu.bh.