# Vulnerabilities in Banking Transactions with Mobile Devices Android: A Systematic Literature Review

Pablo F. Ordoñez-Ordoñez[1,2(✉)], Domingo D. Herrera-Loaiza[1], and Roberth Figueroa-Diaz[1]

[1] Facultad de Energía, Universidad Nacional de Loja, Ave. Pío Jaramillo Alvarado, La Argelia, Loja, Ecuador
pfordonez@unl.edu.ec

[2] ETSI Sistemas Informáticos, Universidad Politécnica de Madrid, Calle Alan Turing s/n, 28031 Madrid, Spain

**Abstract.** This qualitative systematic literature review (SLR) corresponds to the search for vulnerabilities in banking transactions by means of ANDROID Intelligent mobile devices and the incidents in the users. In these devices there is leaking information that is captured by hackers and with it the dissatisfaction of users to ignore how to treat these insecurities. For this, initially of between 123 studies, 18 were selected according to the search criteria corresponding to the research questions in vulnerability and incidence, it was mainly found the bank Phishing, the injections of malware in mobile applications and to a large extent victims of bank fraud.

**Keywords:** Mobile applications · Banking transactions
Software vulnerabilities · Mobile vulnerabilities
Android vulnerabilities

## 1 Introduction

The use of the applications on mobile devices Android is extremely high for its popularity, that is why it is increasingly increase the people who use this type of devices for entertainment and as a tool of work [13,14,28]. When conducting mobile banking transactions, users are not aware that they may be victims of any of the insecurities in banking services indicated in [10], so this paper is a systematic literature review of the vulnerability in banking transactions with Android mobile applications, in order to know the current situation of research carried out according to the research questions:

- **RQ1:** What frequent vulnerabilities exist in banking transactions for Android mobile devices?
- **RQ2:** How do these vulnerabilities affect users?


M. Botto-Tobar et al. (Eds.): CITT 2018, CCIS 895, pp. 104–115, 2019.
https://doi.org/10.1007/978-3-030-05532-5_8

In addition, according to [4] there is a top 10 of vulnerabilities in the mobile platform that is of great importance as related work.

The SLR was based on the protocol of [5,12], where RQ1 and RQ2 were raised. These questions were considered in order to systematize the findings of studies with vulnerable impact on mobile device users when performing tasks such as: online payments, news review, games and entertainment in general.

In Sect. 2, the SLR is executed, the result of which is described in Table 2. On the basis of these results, Sect. 3 presents the most notable details and the synthesis argued and discussed in the 18 primary studies and Sect. 4 concludes as research questions the consequences of the review, and specific lines of research for the future.

## 2 Review Protocol Development

### 2.1 Research Identification

The criterion for the choice of search sources was based on web accessibility and the inclusion of search engines that allow to carry out advanced queries, in this way the following were used: IEEE library [1], SCOPUS Library [8], Google Scholar [2] and OWASP [3].

For the choice of keywords it was considered: research questions and keywords of previously reviewed articles: Vulnerability, mobile applications, Bank transactions, mobile vulnerabilities, Android vulnerabilities, mobile Banking, security

**Table 1.** Bibliographic sources and search strings.

| Search ID | String |
|---|---|
| B01 Scopus | ((An android based) AND (based mobile device) AND (device application) AND (Games and multimedia)) |
| B02 Scopus | ((forensic investigation) AND ('onedrive' OR 'box' OR 'googledrive' OR 'dropbox') AND (applications) AND (android) AND (ios)) |
| B04 Scopus | (title-abs-key (how current) AND title-abs-key (android) AND title-abs-key (malware seeks) AND title-abs-key (evade automated) AND title-abs-key (code analysis)) |
| B05 Scopus | (ALL (automatic detection) AND ALL (correction) AND ALL (visualization) AND ALL (security vulnerabilities) AND ALL (mobile apps)) |
| B06 OWASP | "owasp" + "mobile top 10" + "Vulnerabilities" + "vulnerabilidades" + "móviles" |
| B07 IEEE | "(((“Publication Title”: Security assessment) OR assessment of Mobile) AND Mobile Banking)" |
| B03 IEEE | ((((“Document Title”: Potential Vulnerability) AND Analysis) AND Mobile Banking) AND Applications) |
| B08 Google Scholar | "Systematic Literature Review:" + "Security Challenges of Mobile Banking" AND "Payments System" |
| B09 Google Scholar | "Examining" + "Security Risks" of "Mobile" + "Banking Applications" + "through Blog Mining" |

assessment, Potential Vulnerability, Banking applications, security risks, mobile device.

Searches were performed using logical operators: (AND) and (OR) and the following inclusion criteria were considered for the search:

- Include as relevant the existing publications from 2012 onwards, as a result of the exponential indication of the Use of mobile devices.
- Search results in the area of science and computation, by the close relationship of technical analysis for further mitigation.
- Documents in Spanish and English language.
- Search the Abstract of the article for keywords.

The Table 1 correspond to the search chains (B01...B09) in the different bibliographic sources.

### 2.2 Selection of Primary Studies

Once the results were obtained with the searches, the following criteria were established for the selection and evaluation of primary studies:

- In the summary, you should be aware of the vulnerabilities and/or incidents that occur in the Mobile devices with ANDROID operating system.
- The title must be related to the investigation.
- The document must respond to RQ1 and/or RQ2.
- The conclusion must have relevant information for the investigation.

### 2.3 Data Extraction

The Table 2 presents the relevant information for each of the selected articles (S01...S18) according to the search by pointing out elements such as: type of vulnerability (RQ1) and incidence (RQ2) as research questions, study/article title, and findings as Relevant conclusions. These are the results:

**Table 2.** Data extraction from the primary studies.

| Search ID - Source ID - Ref. Article title | |
|---|---|
| Vulnerability and/or incidence in users | Findings |
| B01 - S01 - [9] Games and multimedia implementation on heroic battle of surabaya: An android based mobile device application | |
| There is an impact on the change in lifestyle of mobile users for accessing information | The number of mobile users increases very rapidly. Interactive applications are developed that allow a better teaching especially in young people |

(*continued*)

**Table 2.** (*continued*)

| Search ID - Source ID - Ref. Article title | |
|---|---|
| Vulnerability and/or incidence in users | Findings |
| B02 - S02 - [7] Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices | |
| Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices Unsafe storage of information in the cloud<br>The credentials, the information accessed in the cloud through mobile devices, could be recovered in the internal memory of the device<br>The sessions and activities carried out in the cloud can be recovered in the backup | The information currently is stored in the cloud and is easily accessible by means of a mobile device, which could be recovered in the internal memory of the mobile device |
| B03 - S03 - [6] Potential Vulnerability Analysis of Mobile Banking Applications | |
| Potential vulnerabilities can be created from the permissions that the operating system grants to applications | Application developers generate vulnerabilities by default. Applications can generate vulnerabilities from permissions which could cause serious impacts on the system and applications<br>The applications generate vulnerabilities, due to the lack of knowledge of the developer |
| B04 - S04 - [27] How Current Android Malware Seeks to Evade Automated Code Analysis | |
| Attack campaigns specifically to the ANDROID platform, exploit the tapjacking vulnerability.<br>New Malware are detected as BadAccents | Malicious applications are spread through email and SMS messages.<br>It detects new malware like the Android/BadAccents family.<br>At present there are many campaigns of new threats to the ANDROID platform |
| B05 - S05 - [26] Automatic Detection, Correction, and Visualization of Security Vulnerabilities in Mobile Apps | |
| There is no confidentiality in sending data from mobile applications | The information that circulates from end to end is exposed to unauthorized observers<br>To increase confidentiality, remote servers are implemented to protect the data, using techniques such as Value-Similarity |

(*continued*)

**Table 2.** (*continued*)

| Search ID - Source ID - Ref. Article title | |
|---|---|
| Vulnerability and/or incidence in users | Findings |
| B06 - S06 - [25] Weak Server Side Controls | |
| The weakness of controls on the server allows cybercriminals to scan open ports, applications, exploiting vulnerabilities through the injection of malicious code<br>XSS Cross-Site Scripting Vulnerabilities, generated from the API, web service or web server applications are exploited through a mobile device | Attackers to find a vulnerability inject malicious code to perpetrate its purpose that is the theft of information from users<br>Vulnerabilities are exploited through a mobile device, the same one that feeds malicious entries to the server, to violate them, this can produce unexpected sequences of events |
| B06 - S07 - [19] Insecure Data Storage | |
| Insecurity in Data Storage, when the user loses his mobile device, attacks can be made to access this medium using the EXPLOITS | Users losing their mobile device for any reason can be victims of attack through malware |
| B06 - S08 - [20] Insufficient Transport Layer Protection | |
| Insufficient Protection in the Transport Layer, as there is no encryption | Data encryption protocols must be used in the transport layer, with SSL/TLS |
| B06 - S09 - [24] Unintended Data Leakage | |
| Unintended Data Fugue, when developing mobile applications you can not control the security of the other systems that are going to interact or hardware with which you will interact so you can lose data | Developers must be trained so that each time they code new applications, they can take action on the possible leaks of information that may occur |
| B06 - S10 - [22] Poor Authorization and Authentication | |
| Poor Authentication and Authorization, due to the lack of security tokens, information can be lost, for example with the well-known "you want to save your password" [22] | You should not be confident at the moment that an application asks if you want to save or remember passwords, this can be displeasing to know that they are capturing the passwords |
| B06 - S11 - [16] Broken Cryptography | |
| Broken Cryptography, using proprietary data encryption algorithms may have holes through which attackers may violate a mobile application | Sometimes the methods of encryption of information (data) become an almost obsolete practice |

(*continued*)

**Table 2.** (*continued*)

| Search ID - Source ID - Ref. Article title | |
|---|---|
| Vulnerability and/or incidence in users | Findings |
| B06 - S12 - [17] Client Side Injection | |
| Lateral Injection Client, mainly occurs in ROOT users since having super user permissions can access files and leave doors open | Users who are not experts or do not know about the privileges that can be activated on their ANDROID devices are vulnerable in terms of information theft perpetrated by CYBER CRIMINALS |
| B06 - S13 - [23] Security Decisions Via Untrusted Inputs | |
| Security decisions that are not trusted via entries, mobile applications when interacting with other applications that are not trusted are vulnerable since there are some processes that may contain malware | Mobile applications should interact only with trusted applications that pass through a certified filter |
| B06 - S14 - [18] Improper Session Handling | |
| Inadequate Management of the session, it happens when we do not close the session for example when we leave open a session in some social network or electronic banking account among others | The naive users are those who are most subject to this vulnerability because they do not know the topic of login when being connected to the internet |
| B06 - S15 - [21] Lack of Binary Protections | |
| Lack of protection at the binary level, through reverse engineering can obtain confidential information from attackers, this happens when a programmer has not been the full author of the application | Developers must have absolute control of their application because otherwise they can be victims of attack by computer criminals |
| B07 - S16 - [15] Security assessment of Mobile- Banking | |
| SMARTPHONES are gaining use in front of the PCs, this does not cause much admiration due to the great benefits that the smart phones give | It is basically code injections on mobile devices that are not managed correctly by the user |
| Denial of Distributed Service (DDoS), services are not accessed by their legitimate users | It occurs due to easy access to stolen devices, taking into account the level of security that the device owns |
| Mobile malware, potentially affects the majority of users who do not have the necessary knowledge to mitigate this vulnerability | When developing an application the data is usually exchanged between client-server |
| Threats from third-party applications are dangerous when interacting with systems other than ANDROID without due security | Interaction with third-party applications, in which the code of other developers is not well known |

(*continued*)

**Table 2.** (*continued*)

| Search ID - Source ID - Ref. Article title | |
|---|---|
| Vulnerability and/or incidence in users | Findings |
| TCP-IP Spoofing, which is based on replacing an IP address with a false one | There are authentication patterns that are considered insecure, this is the case of the IP address change |
| Rear access doors, here malicious codes are captured that do not allow the proper functioning of the algorithm | Sometimes the methods of encryption of information (data) become an almost obsolete practice |
| Manipulation, users follow an inappropriate sequence in their SMARTPHONE re-directing it to another application | Access to unreliable applications by users, in which their data is vulnerable and very prone to theft |
| Exploits, is a vulnerability very well known by computer scientists but little for common users | Insecurity of communication between processes, easily the user can be redirected to another environment through false advertising, games etc. |
| Social engineering and Trojans are very common to violate access to mobile devices | Handling very weak information, a Trojan can easily be introduced to a device, as well as taking information through social engineering to naive users [15] |
| B08 - S17 - [11] Systematic Literature Review: Security Challenges of Mobile Banking and Payments System | |
| The improper use of the APIs, produces an insecurity in the operating system | Users and applications can have full control of mobile devices, as there is no control of priorities in the management of processes |
| B09 - S18 - [10] Examining Security Risks of Mobile Banking Applications through Blog Mining | |
| Banking Phishing, perhaps one of the most common perpetrated by cybercriminals | A fraud by cloning pages or applications, very well planned by hackers |
| WIFI networks without encryption, currently there are applications capable of easily breaching a WIFI network | Poor configuration in network equipment causes unsafe networks, even in the same homes being a gateway to cybercriminals |
| Vulnerabilities of mobile banking applications, with the development of fake ANDROID mobile applications hackers can impersonate original applications for false | Reverse engineering application in banking applications [10] |

### 2.4 Data Synthesis

Table 3 shows the searches that generated 123 articles, of which 72 coincidences were recorded, where the number of articles reviewed was 51, of which 18 articles were selected according to the aforementioned search criteria.

**Table 3.** Summary of reviewed studies.

| Sources | Found | Coincidences | Revised | Selected |
|---|---|---|---|---|
| SCOPUS | 41 | 32 | 09 | 04 |
| IEEE | 47 | 28 | 19 | 02 |
| OWASP | 11 | 0 | 10 | 10 |
| GOOGLE SCHOLAR | 24 | 12 | 12 | 02 |
| Totals | 123 | 72 | 51 | 18 |

## 3 Discussion

What reflects [S01] is the unbridled increase of mobile users for its great features to perform online tasks (payments or purchases, transactions, news, games, etc.) and with this the change in the routine of users that has affected positive and negative way worldwide in terms of health education, history and many other factors that are already known by users. [S02] mentions the growing development of smartphones and with it the use that users give them to perform online tasks, specifically banking transactions, also points out some types of vulnerabilities to which users are exposed as the distributed denial of service attack (DDOS) called the third highest threat according to the FBI, in which the attacker plays the role of network for the scanning of open ports and thereby perpetrate the theft of information, also mention is made of other vulnerabilities such as malware (malicious software), Spoofing of TCP-IP in which the pirate gets access to the phone in an unauthorized way, backdoors installed by the same developers, modifications in applications, pieces of spy code (exploits) and the knowledge of social engineering with banking Trojans. Because of the lack of security in the servers, attackers can make contact with unencrypted data; it also mentions some protocols used by smartphones for information security, there are also some encryption algorithms that are used in the mobile data flow and a security method for banking systems in which authentication and the authorization. In [S03] it is clearly understood the vulnerability that exists when using different clouds to manage user information, it is referred to four (OneDrive, Box, GoogleDrive and Dropbox) that when used in different ANDROID and IOS devices, is It is easy to retrieve information using forensic techniques based on this article in the NIST 10 forensic guide and Martini's four-step forensic framework, demonstrating how you can retrieve information from mobile devices depending on your operating system version (ANDROID version 2.2. 2 and IOS

version 4.3.5), this information is recorded in different files of the internal memory of the phone independently if it is restored to the device for later recovery, showing a complete history of task management performed by the user in that moment.

Regarding the permissions that the user gives to the ANDROID applications, [S04] finds: the normal, the dangerous, the signature and the system, of which the dangerous category is the one associated to the banking applications in which users could naively give permission without knowing the risk they run when their data are intercepted by attackers. In short, there are different types of licenses that users can give to ANDROID mobile applications, each allows with a degree of danger in terms of leakage that can be caused by misuse of them, causing severe damage when installed. Harmful applications in smart devices. Likewise, it is mentioned in [S05] the great ability that hackers have to introduce themselves to smartphones using sophisticated techniques (up to ANDROID version 4.4) for the theft of information, for this they use the so-called attack of tapjacking that is exploited by the Android/BadAccents, consists of the superposition of cloned windows that appear on the screen of the device, and that ask to enter personal data for an update required by the operating system in order to obtain super user permissions (ROOT), it is worth mentioning that they introduce this malware to the SMARTPHONES by means of text messages making fun of the security of servers with intersection of messages or voice calls.

In [S06] we detail the access that mobile applications have to the different types of data that the user has installed on their smartphone as very private information (bank accounts, passwords etc.). An application called ASTRAEA that is responsible for the mitigation of vulnerabilities in information leakage, which has its own security proxy, which makes the flow of data according to the application very secure by examining the information that passes from the end to the extreme.

At work [S17] the use of smart phones worldwide is highlighted, due to their banking services among others, which in turn classifies threats as broad, from telephone to telephone, and online, on the other hand that most malware is on google and the Android platform. Consequently, it explains that mobile users increase day by day so they can enter at any time the mobile banking to perform various tasks, this leads to the attackers to invent new methods (more sophisticated Trojans and malware in general as the forms to introduce them to the SMARTPHONES) in order to circumvent the security of said banking entities, likewise recommend the updates due to their equipment.

The authors of [S18] emphasize security in mobile applications and for this they refer to a study based on mining BLOG (method blog mining) that is about the search for blogs that contain information on security applications of banking mobile, encountering many coincidences such as threats and vulnerabilities (trojans, rootkits and viruses), phishing as insecure Wi-Fi networks; and with these a range of countermeasures such as data encryption, antivirus application updates, among others. They also talk about some malwares like: Zitmo, Banker, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream and Keyloggers.

Regarding threats from third-party applications they secretly alter a banking application, so the author recommends the constant updating of applications from reliable sources, another huge vulnerability found is the famous phishing that deals with fraudulent applications (application clones)), unencrypted WIFI networks in popular places which allows the attacker to violate these networks due to its weak security and reverse engineering. For their part, they recommend integrating mobile security based on biometrics as well as intelligent technology based on monitoring in mobile banking applications.

## 4 Conclusion and Future Work

With the growing development of smart terminals (SMARTPHONES) and its extensive benefits to the user to improve the lifestyle, a number of vulnerabilities arise for both mobile platforms and operating systems in general, so that the desire for computer criminals steal confidential information from users, who for different reasons do not use their smartphone properly.

As mobile vulnerabilities are mitigated in different versions of the Android operating system, the attacker is at the forefront to take advantage of the minimum flaw that is in the current versions and thus act deliberately and especially violate banking applications.

The systematic review allowed to know the frequent vulnerabilities in the banking transactions by Android mobile devices, usually the user is not aware of what they happen, the ones that stand out are: Banking Phishing, Trojans and injections, unsafe storage in the cloud, campaigns to violate the ANDROID platform, insufficient protection when circulating data, insecurity in servers, lack of protection in the transport layer, involuntary data leakage, poor authentication and authorization, broken cryptography, ROOT users.

With respect to the incidence of use of banking transactions with smartphones in users, the increase in technology has partly facilitated their way of life due to the great benefits that smartphones have generated in their daily performance, the change in routine of users who use SMARTPHONES, has had a positive and largely negative impact, simply because they do not know deeply the good use of these smartphones and therefore are the victims of many bank frauds and information leakage.

Consequently, future work is needed to establish models of trust in mobile transactions and person-mobile research that minimizes the effects of the user when data security is concerned. Also, that from these results are generated recommendations for the mitigation of these incidents.

## References

1. Google Scholar. https://scholar.google.com/
2. IEEE Xplore Digital Library. https://ieeexplore.ieee.org/Xplore/home.jsp
3. OWASP. https://www.owasp.org/index.php?search=&title=Special%3ASearch&go=Go

4. Sobre OWASP. https://www.owasp.org/index.php/Sobre_OWASP
5. Centro Cochrane Iberoamericano: Manual Cochrane de Revisiones Sistemáticas de Intervenciones, versión 5.1.0 (2011)
6. Cho, T., Kim, Y., Han, S., Seo, S.H.: Potential vulnerability analysis of mobile banking applications. In: 2013 International Conference on ICT Convergence (ICTC), pp. 1114–1115, October 2013. https://doi.org/10.1109/ICTC.2013.6675570
7. Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., Choo, K.K.R.: Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Aust. J. Forensic Sci. **48**(6), 615–642 (2016). https://doi.org/10.1080/00450618.2015.1110620
8. Elsevier B.V.: Scopus. https://www.scopus.com/home.uri
9. Handojo, A., Lim, R., Andjarwirawan, J., Sunaryo, S.: Games and multimedia implementation on heroic battle of surabaya: an android based mobile device application. In: Pasila, F., Tanoto, Y., Lim, R., Santoso, M., Pah, N.D. (eds.) Proceedings of Second International Conference on Electrical Systems, Technology and Information 2015 (ICESTI 2015). LNEE, vol. 365, pp. 619–629. Springer, Singapore (2016). https://doi.org/10.1007/978-981-287-988-2_69
10. He, W., Tian, X., Shen, J.: Examining security risks of mobile banking applications through blog mining. In: MAICS, pp. 103–108 (2015)
11. Islam, S.: Systematic literature review: security challenges of mobile banking and payments system. Int. J. u-and e-Serv. Sci. Technol. **7**(6), 107–116 (2014)
12. Kitchenham, B.: Procedures for performing systematic reviews (2004)
13. Liang, C.: Subjective norms and customer adoption of mobile banking: Taiwan and vietnam. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 1577–1585, January 2016. https://doi.org/10.1109/HICSS.2016.199
14. Njenga, K., Ndlovu, S.: On privacy calculus and underlying consumer concerns influencing mobile banking subscriptions. In: Information Security for South Africa (ISSA), pp. 1–9. IEEE (2012)
15. Nosrati, L., Bidgoli, A.M.: Security assessment of mobile- banking. In: 2015 International Conference and Workshop on Computing and Communication (IEMCON), pp. 1–5, October 2015. https://doi.org/10.1109/IEMCON.2015.7344489
16. OWASP: Broken Cryptography - Mobile Top 10 2014–M6. https://www.owasp.org/index.php/Mobile_Top_10_2014-M6
17. OWASP: Client Side Injection - Mobile Top 10 2014–M7. https://www.owasp.org/index.php/Mobile_Top_10_2014-M7
18. OWASP: Improper Session Handling - Mobile Top 10 2014–M9. https://www.owasp.org/index.php/Mobile_Top_10_2014-M9
19. OWASP: Insecure Data Storage - Mobile Top 10 2014–M2. https://www.owasp.org/index.php/Mobile_Top_10_2014-M2
20. OWASP: Insufficient Transport Layer Protection - Mobile Top 10 2014–M3. https://www.owasp.org/index.php/Mobile_Top_10_2014-M3
21. OWASP: Lack of Binary Protections - Mobile Top 10 2014–M10. https://www.owasp.org/index.php/Mobile_Top_10_2014-M10
22. OWASP: Poor Authorization and Authentication - Mobile Top 10 2014–M5. https://www.owasp.org/index.php/Mobile_Top_10_2014-M5
23. OWASP: Security Decisions Via Untrusted Inputs - Mobile Top 10 2014–M8. https://www.owasp.org/index.php/Mobile_Top_10_2014-M8
24. OWASP: Unintended Data Leakage - Mobile Top 10 2014–M4. https://www.owasp.org/index.php/Mobile_Top_10_2014-M4

25. OWASP: Weak Server Side Control - Mobile Top 10 2014–M1. https://www.owasp.org/index.php/Mobile_Top_10_2014-M1
26. Pistoia, M., Tripp, O., Ferrara, P., Centonze, P.: Automatic detection, correction, and visualization of security vulnerabilities in mobile apps. In: Proceedings of the 3rd International Workshop on Mobile Development Lifecycle, MobileDeLi 2015, New York, NY, USA, pp. 35–36 (2015). https://doi.org/10.1145/2846661.2846667
27. Rasthofer, S., Asrar, I., Huber, S., Bodden, E.: How current Android malware seeks to evade automated code analysis. In: Akram, R.N., Jajodia, S. (eds.) WISTP 2015. LNCS, vol. 9311, pp. 187–202. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24018-3_12
28. Sugiono, E., Asnar, Y., Liem, I.: Android security assessment based on reported vulnerability. In: 2014 International Conference on Data and Software Engineering (ICODSE), pp. 1–6, November 2014. https://doi.org/10.1109/ICODSE.2014.7062686