FBYOD: A Fuzzy Logic-based System for Safe BYOD Adoption

Paulo Roberto Uhlig[1], Luiz Nacamura Junior[2]

Programa de Pos-Graduação em Computação Aplicada Universidade Tecnológica Federal do Paraná – UTFPR
Curitiba, Brazil

Abstract *— Smartphones are commonly used equipment for personal purposes and well as for work-oriented activities. There is a growing number of companies that adopt the policy of allowing their users to use their own equipment to perform personal and work activities. This policy, called Bring Your Own Device (BYOD), offers advantages such as reducing costs in the acquisition of equipment by the company, increased mobility and productivity. However, the adoption of BYOD offers risks because these devices may have customizable security configurations that are too permissive and also store highly relevant information. In this way, the customizable security settings of the smartphone's operating system can directly impact the security of the device and as a result, data theft and financial loss can occur. Thus, the individual assessment of the security impact that each custom configuration represents together with the quantification of the data stored in the mobile device, may provide a degree of security impact that that equipment presents. In this work, an application called Fuzzy BYOD (FBYOD) is proposed. FBYOD introduces the use of fuzzy logic to assess in real time the security impact of the smartphone by automatically evaluating and recalculating any changes to the customizable security settings and the amount of user data files. As an additional feature, FBYOD enables the device to access new corporate information whose relevance is compatible with the level of risk presented by the device. This application is implemented and validated in a non-simulated corporate environment and in a scenario where mobile devices use the Android operating system. The results obtained demonstrate the effectiveness of FBYOD in promoting access to corporate information whose importance is compatible with the security impact generated by the mobile device.*

Keywords *— BYOD, custom configuration, data theft, fuzzy*

I. INTRODUCTION

Until the early 1990s, corporate offices were mainly made up of desktop computers and their peripherals. Years later, with the popularization of the Internet and mobile technologies, users have the opportunity to perform their work activities outside the business environment and in different devices, whether belonging to the company or not. Recently some organizations have adopted a policy called Bring Your Own Device (BYOD). This approach allows users to connect their own equipment such as tablets, smartphones and notebooks computers to the corporate network and thus it becomes possible to carry out the work activities [1], [2].

BYOD offers advantages such as user mobility, however adopting this policy increases security-related risks. Unlike devices owned by the company, the equipment used for BYOD may not have all the security configurations and applications required for work activities to be performed safely, in addition to store information of different levels of importance [3], [4].

The customizable security settings of the mobile device operating system can directly impact the security of the device and as a result, data theft and financial loss can occur. Thus, the individual assessment of the security impact that each custom configuration represents together with the quantification of the data stored in the mobile device may provide a degree of security impact, which that equipment presents. In this way, the device is classified to access corporate information whose importance is compatible with its degree of security impact.

In this work, we propose an application called Fuzzy BYOD (FBYOD). FBYOD introduces the use of fuzzy logic to evaluate the security impact of the smartphone in real time by assessing the device's customizable security settings data and the amount of user data files stored in the device. In this way, FBYOD enables the device to access new corporate files whose importance is compatible with the degree of security risk presented by the device. The software is implemented and validated in a real-world corporate scenario where the BYOD policy is adopted.

This paper is divided as follows. The next section provides the background, section three presents the related works, section four describes the data collected, section five presents the general structure of FBYOD, section six describes about the implementation of FBYOD, section seven presents the experiments and results obtained, in the sequence,FBYOD screens are illustrated by section eight, limitations and future work are shown in section nine and finally the conclusion is made in section ten.

II. BACKGROUND

BYOD is adopted by 59% of US companies in order to offer mobility, increased productivity and to reduce costs related to equipment purchase [5]. Mobile devices such as smartphones and tablets have common features compared to ordinary desktop computers, such as Internet access and document editing. However, when it comes to safety there are significant differences [6]:

- *Mobility:* mobile devices are not located into a specific physical space. In this way, they can be stolen or lost more easily;
- *Increased customization:* mobile devices used for BYOD are typically not shared with other users, so more customization of the device settings and installed applications occurs;
- *Connectivity:* Mobile devices commonly provide interfaces for 3G, LTE, wireless and bluetooth network access. Therefore, the area for exploitation of vulnerabilities is enlarged.

According to a security report issued by [7], in the year 2016 the number of new vulnerabilities found in operating systems for mobile devices Google Android and Apple iOS increased about 10% compared to 2015. A vulnerability is defined as a shortcoming that can be exploited by malware or even by malicious users and thus compromise the security of a particular system [4], [8], [9]. Table I shows the history of vulnerabilities encountered in these operating systems in the years 2014-2016 [7].

Table I: History of New Vulnerabilities FoundinAndroidandi OS Operating Systemsin 2014, 2015 and 2016.

Year	Android	iOS	Total
2014	12	178	190
2015	89	463	552
2016	316	290	606

The exploitation of vulnerabilities can result in inoperable or unstable corporate systems and data theft. In addition to these inconveniences, financial loss can also occur, as 34% of the equipment used for BYOD store important information[10].

A. Risks Related to Custom Security Settings

An important point related to mobile device security is tied to its customizable security settings. A customizable security setting is defined as a parameter adjustment that users can perform on their equipment. In this way, that parameter setting can affect the system's security with different levels of severity [4]. For example, disable the device unlock password. Even though it is a valid customization of the configuration, the security risks are increased in order of an easier access to the device's data. On the other hand, changing the background picture is also a configuration customization but without any security risk.

An average user's security knowledge is low, as he or she is usually not able to understand the real objective and mainly the consequences in customizing security configurations. In this way, even if it is unintentional, serious security vulnerabilities can be generated and thus successful malware attacks or people intent on doing so may occur [11], [12].

B. Data Importance

Devices used for BYOD can store a large variety of personal and corporate data including documents, photos, video, emails, passwords and so on [13]. These files may contain information of different levels of importance, such as family photos, recorded audio from a meeting, a new corporate project, among others. In order to reduce the impact of eventual data theft, data must be classified according to their importance through the principles of confidentiality, availability and integrity. These principles are explained in sequence [14], [15]:

- *Confidentiality*: confidentiality refers directly to who needs to know a certain information. In this way, when a document is stolen through the action of a malware or intended person to execute the data theft, for example, the principle of confidentiality is broken;
- *Availability*: when certain information can be accessed in accordance with the access policies assigned to it, then it is called that this information is available;
- *Integrity*: information is considered incorrupt when it has not suffered any unauthorized changes. In this way, the information remains free of any data that does not correspond to it.

Violation of any of these principles may cause different levels of impact to the user or the corporation. These levels are called [15]:

- *Low*: a violation is considered low when it does not impact on the continuity of the organization's activities or causes insignificant financial loss;
- *Medium*: when the violation is considered medium, there is a temporary reduction or halt in the user's or corporation's work activities, or significant financial loss;
- *High*: a violation of any of those principles is considered high when the damages cause great financial loss or inability to continue the organization's activities.

However, each principle may have a different degree of impact. Thus, the information can be classified according to the following notation:

SC = {(Confidentiality, Impact), (Availability, Impact), (Integrity, Impact)}

The notation above illustrates that the *security category* (SC) which the information is classified is composed by the values (low, medium or high) for each of the principles. However, only the highest impact value among the three principles is considered [15]. For example, if a given information has a security category of SC = (Confidentiality, Low), (Availability, Medium), (Integrity, High), that SC is classified as *high* in order of its highest value applied.

C. Fuzzy Logic

In traditional logic, there are only two possibilities, the true and the false values. Consequently, in the classical theory of sets, an element belongs or not to a particular set. In fuzzy logic, the concept of true and false is approached by varying the degree of truth. In this sense, an element can belong both to one set and to another according to a value of pertinence, defining its degree of inclusion in sets [16], [17].

Based on this premise, fuzzy logic is recommended for scenarios where the distinction between elements is difficult to gauge. Lofti A. Zadeh proposed the fuzzy logic in 1965, allowing the development of systems, such as process control systems and decision support systems [18]–[20]. The basic fuzzy logic components are explained below:

- *Fuzzification process*: in fuzzy logic, sets define linguistic terms (such as little, good, low, hot) and membership functions define in a range of [0,1] the degree of inclusion of a given element in those sets. The fuzzification process consists in correlating an input value, usually a numerical value called crisp, with the available sets by measuring the degree of compatibility of each element. The result of the fuzzification are fuzzy sets, denoted by linguistic terms [18], [19], [21].
- *Rule base*: the rule base is essential for the operation of a fuzzy system, from which the output value is generated. Its content is based on the human form of decision. A fuzzy rule is a simple "IF-THEN" decision structure, where fuzzy variables are compared to linguistic terms, both in the antecedent and in the consequent of the rule. The antecedent and the consequent of the rule may contain more than one condition, joined by logical operators "AND and OR". In general, a fuzzy rule has only one output. Experts from the field of application commonly create the rule base, however it can be extracted through machine learning algorithms [22]. For instance, fuzzy rule could be defined as "IF temperature is "hot" THEN fan speed is "high"".
- *Fuzzy inference*: In the inference step, it is possible to obtain logical conclusions, even in an uncertain scenario, through the relation of the input value with what is defined in the rules. The inference process is similar to the human way of analyzing data and information in order to obtain a relevant conclusion for decision making. This feature supports the so-called approximate reasoning mechanism given to systems based on fuzzy logic [19], [22]. The inference process begins with the activation of the rules in the rule base that map the inputs provided in the antecedent. The result of activating a rule is a fuzzy value, derived from the aggregation of antecedents through, for example, a minimum function for the logical operator "AND" or a maximum function for the logical operator "OR", if these operators are present in the rule. If these values of activation result in the same consequent set, they need to be aggregated, in this case the one with the highest value prevails, since it adds the value of the other in itself. This process is known as rule aggregation. Finally, the activated output sets are delineated by the activation values resulting from the aggregation of the rules.
- *Defuzzification process*: the output region defined by the fuzzy inference mechanism configures, through its linguistic terms, the possible outputs of a fuzzy system. However, some application scenarios should result in accurate numerical measurement. In these cases, defuzzification consists of calculating a numeric value in the output region. These calculations can be, for example, through the mean of the maxima (MOM) and the centerof gravity (COG) methods [18].Fig. 1 illustrates a typical fuzzy inference system workflow:

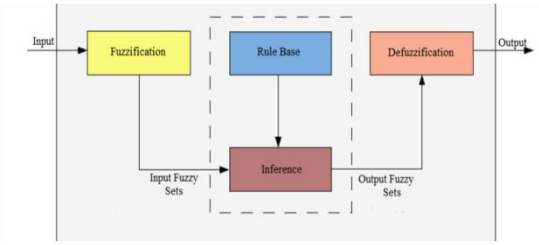

Fig. 1 - Components and workflow of execution of a fuzzy inference system.

The fuzzy inference system receives crisp values as input variables. Then, the fuzzification

process occurs in order to assign degrees of pertinence to those variables for each of the input fuzzy sets. After these processes, the inference of the rules is called and, finally, the defuzzification process is invoked.

III. RELATED WORK

This section presents the works related to this paper and their contribution to the state of the art.

The work proposed by [23] argues about the benefits and drawbacks BYOD usage. In the opinion of the authors, data theft can occur in order of the amount of information stored in the device and the use of inadequate security mechanisms. As a way to mitigate data theft, a framework is proposed. The framework provides security recommendation for the entire equipment lifecycle, such as device registration, required settings, applications and device disposal. As a limitation, this framework does not present any automated deployment tools.

The paper published by [24] discusses that data theft is primarily caused by malware or applications that store corporate data without permission. As a proposal, the authors develop access policies based on the security framework of the North Atlantic Treaty Organization (NATO). These policies are build on the security impact of violating the principles of confidentiality, availability and integrity. Therefore, access profiles are created and assigned to users. To automate policy deployment, a prototype has been developed and it has a administration portal where the administrator configures policies. Then, a client application installed on the mobile device receives them. As limitations, only the Android operating system is supported and tests on non-simulated environments are required.

The work presented by [4] addresses the popularization of BYOD, the increasing amount of information stored on mobile devices and two of the main threats: data theft and privacy breach. As a way of measuring those threats, the authors apply an approach to assess the security impact of the customizable settings of the Android operating system. In this way, a software prototype has been developed and it is installed on the mobile device, which the evaluation is desired. Once installed, the application collects the values of the customizable security settings of the Android operating system and compares them with values recommended by the literature. Then it possible to evaluate how safe the equipment is and also to assess the most misunderstood points by the users.

As a way to contribute to computing security, the nonprofit organization called Center for Internet Security (CIS) [25] aims to assist businesses and users. The purpose of this organization is achieved by providing documents entitled CIS Benchmarks. These documents contain security recommendations for open-source and proprietary systems custom configurations, including Google Android and Apple iOS operating systems. In this way, BYOD administrators and users can obtain basement in order to proceed with the customization of security settings. The documents provide focus on the practical aspects of system configuration. Therefore, it is possible to adjust the recommended value that each configuration option may have in order to improve the level of security, which that configuration implies in the system. In practice, each document contains, among other information, relevant security settings, including a brief description and discussion of the importance of each configuration, the audit steps required to collect the values already configured in the system, and the value proposed by CIS Benchmark document. One of the advantages of the approach proposed by CIS organization is that the recommended parameters are based on acquired specialists' experience. However, the documents only provide guidance on how to perform the verification and adjustment of the settings without offering any automated tools for performing this task.

In the work proposed by [26], the authors address the importance of information that users store on smartphones in accordance with the principles of confidentiality, availability and integrity. As a way of measuring what types of information are stored on the devices and their importance, a research with smartphone owners was carried out. As a result, it turned out that application passwords, work-related documents, photos, videos, among other files are stored on the smartphone and they are also considered important, especially when it comes to confidentiality. Additional results from the survey show that most users do not take protective measures to prevent data theft or preservation of the principle of availability, such as performing backups. Thus, the authors conclude that these devices store sensitive personal and corporate files but do not receive the necessary security mechanisms to remain them protected.

The paper proposed by [27] also comments on information stored on mobile devices. In that work, the authors argue on the need for new authentication methods to protect different types of data allocated in the equipment. According to his research, the use of Personal Identification Number (PIN) authentication does not provide an adequate level of security because it can be easily deduced in order of its short size, usually four numeric characters. In a survey conducted, it was revealed that passwords, e-mails, files stored on device have a high degree of confidentiality for users, whether this information relates to personal or corporate context. In conclusion, the authors

comment that different types of data need security levels compatible with their importance.

In the work developed by [28], the authors propose the fuzzy logic usage to evaluate the legitimacy of smartphone users. According to the authors, breach of the confidentiality of the data contained in the devices is common, mainly caused by device loss of theft. In this way, the authors have developed a software prototype that collects certain data contained in the device, such as number of incoming and outgoing SMS messages, incoming and outgoing voice calls, web browser usage history and wireless connection history. Then, those data are processed by the fuzzy inference system. Thus, the user profile is created and as new data is collected from the device and processed by the fuzzy inference system, the results are compared and the degree of legitimacy of equipment's user is assessed. In conclusion, the authors state that the accuracy index provided by the prototype is greater than 90 %.

The works presented above give a glimpse into the importance of the data contained in the mobile device and the methods applied for its safety. However, no papers connect the principles of confidentiality, integrity and availability of the information accessed with the security risk that the mobile device represents.

IV. SECURITY SETTINGS AND STORED DATA

This section presents the data used as background for this work.

A. Security Settings

The customizable security settings that this work considers are based on [4], [25] publications. These settings are organized into categories as shown in table II, at the end of this document due to its size, and can be used for different operating systems such as Android and iOS. In the specific case of this work, this table was used as a basis in the development of FBYOD for the Android operating system.

As shown by table II, in addition to the common configurations, each operating system has peculiar characteristics. To evaluate how secure a mobile device is in relation to its customized security settings, simply collect the adjusted values on the device and compare them with the recommended values. However, items marked with an asterisk cannot be evaluated by automated tool [4]. In addition to security settings, security recommendations are also associated. These recommendations, whose value is represented by a dash, have the purpose of guiding the user or an administrator to avoid vulnerabilities and are not checked by an automated tool. For example, using VPN on public wireless networks prevents data from being intercepted during transmission.

B. Security Impact Assessment of Customizable Security Configurations

The evaluation of the security impact caused by the wrong adjustment of the customizable security settings is based on [4]. Table III describes the security impact levels used in this work.

Table III: Description of Security Impact Levels Caused by Non-Recommended Adjustment of Customizable Settings.

ImpactLevel	Description	Impact Description
1	The configuration is not relevant and it is very unlikely to exploit this configuration on case of misconfiguration.	In case of attack, the impact is minimum.
2	The configuration is relevant and it is unlikely to exploit this configuration in case of misconfiguration.	In case of attack, the impact is limited.
3	The configuration should be correctly adjusted and may be exploited in case of misconfiguration.	In case of attack, the impact may bring danger to the user.
4	The configuration is important and will likely be exploited in case of misconfiguration.	In case of attack, important information disclosure may occur and limited financial loss.
5	The configuration is critical and will be very likely be exploited in case of misconfiguration.	In case of attack severe financial and data loss may occur.

As shown in table III, the security impact caused by misconfiguration of the customizable security settings are spread over five levels and have different consequences. Following, table IV shows the customizable settings evaluated by FBYOD and their respective impact levels.

Table IV: Security Impact Level of Android's Customizable Security Settings and Security Recommendations.

Customizable Configuration	Impact Level
Category - Password	
Enabled password	5
Enable alphanumeric password	5
Disable visible password	5
Enable user data wipe after excessive invalid password input	5
Setup password age	4
Enable password history	3
Setup minimum password size	4
Setup minimum complex characters	4

Disable visibility for pattern password	3
Category - Network	
Remove known wireless network entries	2
Disable network notification	2
Disable wireless adapter when not needed	3
Disable bluetooth adapter when not needed	3
Disable personal hotspot when not needed	3
Disable bluetooth discovery	3
Category – Permission	
Disable write permission on /system directory	4
Disable write permission on /data directory	4
Do not "Jailbreak" (root)	5
Category - System	
Setup screen lock time	5
Power button immediately locks screen when pressed	5
Enable storage encryption	5
Disable developers option	4
Disable install third-party application option	5
Disable localization services when not needed	3
Disable mock location	3
Enable automatic date and time zone setup	2
Install anti-malware tool	3
Category - Content	
Limit the number of stored SMS messages	1
Limit the number of stores multimedia messages	2

As shown by table IV, each customizable security configuration or security recommendation set in disagreement from table II has a specific security impact. This work is limited to the Android operating system and the items in table II whose evaluation can be performed by an automated tool.

The items described in table IV may generate vulnerabilities or increase the surface of security attacks. The items that make up the password category provide an initial barrier to unauthorized access to the equipment. Enabling settings that ask for alphanumeric passwords, numeric characters, complex characters favor the use of non-trivial passwords, which makes it more difficult to break [29], [30]. Similarly, disabling the visibility of passwords prevents a closer person from viewing eventual typed characters.

Similarly, the utilization of wireless and bluetooth adapters provides facilities in the use of internet and communication with other equipment. However, as reported by Common Vulnerabilities and Exposures (CVE) [31], Android operating system has accumulated 23 vulnerabilities related to the use of Wi-Fi and 55 vulnerabilities related to bluetooth technology. Thus, the indiscriminate use of these technologies may favor malicious actives of malware or intended persons to do so. Similarly, device location-related settings can be exploited to provide user location data to third-party applications and people.

Using jailbreaking allows common applications to run with administrative privileges and so make any changes to the system. The device that has undergone the jailbreak process has increased data theft surface. This is caused in order of any data can be accessed by any applications.

Even if the device is not jailbroken, /system and /data directories must retain their original access permissions. The /system directory stores the Android operating system itself while the /data directory holds data related to installed users and applications. Therefore, enabling non-standard writing permissions in these two directories may violate the principles of confidentiality, integrity, and availability [32], [33].

Settings such as "setup screen lock time" and "power button immediately locks screen when pressed" provide important protection to the user. If, for example, the user has unlocked the device through his or her password and there is none or a long time screen lock set, the device behaves in a similar way as if it had no protection of any type of passwords at all, since it would be available for consultation after the first password unlock. Similarly, the power button will turn off the screen, however it can be adjusted to not require a password immediately after it is pressed, which favors data theft by intruders.

Installing applications from unofficial sources can generate threats. Third-party applications, as well the software under development that can be run through a development device, do not pass the official store sieve, so they may contain malware.

Therefore, the use of anti-malware tool is recommended, even though only official applications are installed.

To protect equipment data, including SMS and MMS messages, storage encryption configuration provides an additional layer of data protection. Thus, the data can only be accessed through a password or a decryption token.

SMS and MMS messages may contain relevant information. In this way, it is good practice to remove the messages that will no longer be used.

Due to the security impact, if the mobile device has unsafe values for any of the "enable password", "setup screen lock time", "do not "Jailbreak" (root)" and "disable install application from third party option " configurations, the security impact represented by the device is considered high. These set of four configurations is called "fundamental configurations".

C. Device's Stored Data

Mobile devices store an average of 500 user data files. These files include documents, photos, video, and audios. Among these files, low, medium and high importance information can be found [4]. Table V illustrates the most commonly used file extensions for these type of files.

Table V: File Extensions Commonly used for Certain File Types.

File Type	Extension
Document	doc, docx, xls, xlsx, odt, ods, ppt, pptx, pdf
Audio	mp3, ogg
Video	avi, mpg, mpeg, mp4, 3gp, mov, flvv
Photo	jpg, png, bmp, tif, gif

V. FBYOD PROTOTYPE GENERAL STRUCTURE

This section presents the FBYOD structure. The prototype is based on a client-server model, which means the client runs in user's smartphone, and the database is stored in a cloud environment. Fig. 2 illustrates FBYOD general structure.

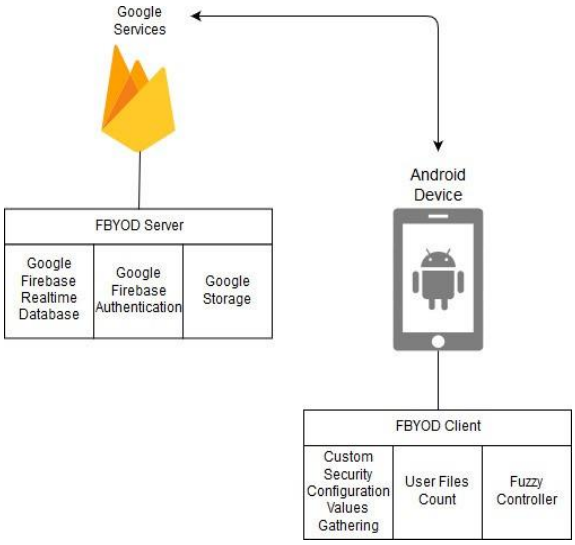

Fig. 2- FBYOD general structure

FBYOD client application is published on Google Play [34] and is compatible with the Android operating system version 4.0.3 and above. This application has the following features:

- *Customizable Configuration Value Gatherer Module:* this module verifies in the mobile device under evaluation the values assigned to each of the items described in table IV. However, no fix is applied or suggested. If the value for the item conforms to the II, the security impact is evaluated as zero. However, if the item is misconfigured, the security impact is evaluated according to table IV. As output, this module returns the sum of the security impacts of all misconfigured items;
- *File Counter Module*: the file counter module searches the mobile device's storage for files whose extension is compatible with table V. At the end of the process, the total of found files is returned;
- *Fuzzy Controller Module*: the fuzzy controller module is used to calculate the security impact index that a mobile device represents. Through this index, the device is classified to access corporate information of low, medium or high importance. As input parameters, the fuzzy controller module receives the outputs of the customizable configuration value gatherer and the file counter modules. As output of the fuzzy controller module, the device security impact index is calculated. This index is a numerical value in a range of 0 to 100. Thus, 0 represents no security impact whereas 100 is the maximal security impact that a mobile device may have.

The FBYOD server components are described below:

- *FBYOD Database*: the database stores the information collected by the FBYOD client application modules;
- *FBYOD Authentication Module*: this module stores the login data such as username and password of FBYOD system users;
- *FBYOD Storage Module: this module stores the* corporate files made available by the administrator and which can be accessed through FBYOD client interface. These files must be classified into distinct directories according to their importance.

Fig. 3 illustrates the workflow of FBYOD. After the FBYOD client has been installed on the mobile device, the user logs in using his or her username and password. After a successful login, the Customizable Configuration Value Gatherer and File Counter modules are automatically invoked. Then, the Fuzzy Control module is called and at the end of its processing, the device's security impact index is calculated and so the equipment is classified to access low, medium or high importance files stored in FBYOD Storage module. A device classified to access a file of high importance, can also access medium and low importance files. Conversely, a device classified to access low importance files will not have access to more relevant information. When the security impact index of the device has already been calculated, the data obtained by the FBYOD client modules is transmitted to the FBYOD database. If any changes to the device's customizable security settings or the amount of data files stored on the mobile device occur, the process restarts.

VI. FBYOD IMPLEMENTATION

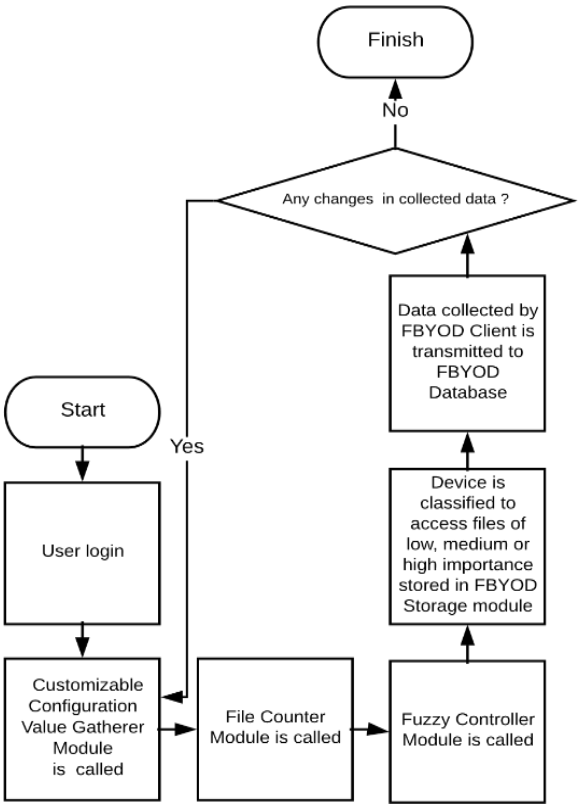

Fig. 3 -. FBYOD workflow chart.

For the implementation of the FBYOD client application, Android Studio [35] development tool was used in orderof its versatility and compatibility with the Android operating system. In the sequence, the implementation process of FBYOD client modules is described.

A. Implementation of the Customizable Configuration Value Gatherer Module

For the implementation of this module, calls to the Android operating system APIs were performed. These APIs, such as WifiManager (for collecting data for wireless networks), BluetoothAdapter (for collecting data from bluetooth interface), and Settings.System (general system settings), among others, provide specific methods for querying the customizable security settings attributes and then get the assigned values. However, the following items have no API interface and were implemented as follows:

- *Do not "Jailbreak" (root)*: To verify if the device is runs with administrator permission, FBYOD checks if the "su" application is found on the system. "Su" allows other applications to run with administrative privileges in addition to allowing access to all directories of the operating system [33];
- *Install Anti-malware tool*: To check if an anti-malware tool is installed, in November 2018 a survey was conducted in Google Play app store [36]. In this research, it was verified which anti-malware applications were available. In this way, a list of the package names of those applications has been generated and FBYOD uses that list to check if any of those packages are installed.

For information on which APIs and their methods should be handled, a research has been done in the official Android operating system's documentation and on the well-known programming site "Stack Overflow" [37], [38].

B. Implementation of the File Counter Module

The implementation of the File Counter module uses table V as backgroud. Thus, a research for files that are compatible with those extensions in the user's default storage directory is performed. In order to get the address of this directory the method *Environment.getExternalStorageDirectory().getPath()* is invoked.

C. Implementation of the Fuzzy Controller Module

The Fuzzy Controller module is implemented based on the jfuzzy library [39]. This library is developed through the Java programming language and is compatible with the Android Studio development tool. The workflow that this module follows is as identical as described by fig. 1.

- *Input variables*: The Fuzzy Controller module uses as input variables the output result of the Customizable Configuration Value Gatherer and File Counter modules. These two variables are fuzzified in the respective universes through trapezoidal pertinence function [18]. The universe where the output of Customizable Configuration Value Gatherer is fuzzified ranges from 0 to 105 and has three fuzzy sets named as follows: low, medium and high. The ending value of the range is defined as 105 because it is the value if all collected customizable security settings were set incorrectly. The second input variable universe, where the output of File Counter is fuzzified, ranges from 0 to 500 and has the same three fuzzy sets. The ending range value is adopted in order of being the average number of user data files stored in a mobile device.
- *Rule set*: the subsystem uses the Mamdani method and a specialist developed the rules. For aggregation of the antecedents of the

rules, the operator "AND" is applied. Table VI shows the developed rules.

Table VI: Fuzzy Rules Used by FBYOD.

Fuzzy Rule
IF "Risk Configuration" is low AND "User Files" is low THEN "Security Impact Index" is low
IF "Risk Configuration" is low AND "User Files" is medium THEN "Security Impact Index" is low
IF "Risk Configuration" is low AND "User Files" is high THEN "Security Impact Index" is medium
IF "Risk Configuration" is medium AND "User Files" is low THEN "Security Impact Index" is low.
IF "Risk Configuration" is medium AND "User Files" is medium THEN "Security Impact Index" is medium.
IF "Risk Configuration" is medium AND "User Files" is high THEN "Security Impact Index" is high.
IF "Risk Configuration" is high AND "User Files" is low THEN "Security Impact Index" is medium
IF "Risk Configuration" is high AND "User Files" is medium THEN "Security Impact Index" is high.
IF "Risk Configuration" is high AND "User Files" is high THEN "Security Impact Index" is high.

- *Output*: the output of the Fuzzy Controller module is obtained through the centroid defuzzification method. The output universe ranges from 0 to 100 and has three output fuzzy sets named as follows: low, medium and high. Through the output of the fuzzy controller, the device is classified to access the information stored in the FBYOD Storage module. To access high-relevance files a device must have a security impact index lower than 30. Similarly, if the security impact index is between 30 and 60, the device is classified to access medium-relevance files and an index greater that 60 only enables the device to access low-relevance files.

In order to validate the operation of the fuzzy controller module, the MATLAB tool was used [40]. Thus, the module configurations generated by the jfuzzy library were reproduced in MATLAB and tested through the same sequence of input variables. As a conclusion, it was observed compatibility of the obtained output values and thus the FBYOD fuzzy controller module becomes valid.

D. Implementation of the FBYOD Database

FBYOD uses the Google Firebase Realtime Database database [41]. Firebase Realtime Database is a NoSQL-type database and is hosted in a cloud environment on Google's own servers. The choice of this database is based on the compatibility of its APIs for the development of mobile applications, secure transmission of data between the mobile device and the database itself, and also automated implementation of data retransmission in case of internet link unavailability between the application and the database.

The FBYOD database stores the data collected by the client application modules and is organized as shown in fig. 4:

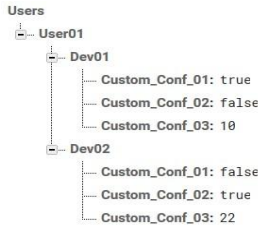

Fig. 4- FBYOD database structure. In this example, only three sample collected items and their values are displayed in each device due to lack of space.

The data structure illustrated by fig. 4 shows that the collected datais linked to a device code, so the user can use more than one mobile device and this code is connected to the username.

E. Implementation of the FBYOD Authentication Module

Authentication of FBYOD users is done through the username and password pair. The authentication base adopted is the Google Firebase Authentication and the choice is based on its compatibility with the adopted database. User registration is done directly in the Google Firebase administration console [42].

F. Implementation of the FBYOD Storage Module

The platform chosen to store and make available files for FBYOD is Google Firebase Storage [43]. Just like the other solutions used to compose the FBYOD server modules, Google Firebase Storage is in Google's own cloud environment and thus does not require the use of a local storage server.

The FBYOD Storage module uses three directories as described below:

- *Low*: this directory stores low-relevance files;
- *Medium*: similarly to the previous item, this directory stores medium-relevance files;
- *High*: within this directory are stored the most relevant files.

In the current FBYOD development state, the system administrator must first sort and distribute the files within those directories through Google Firebase administration console.

VII. EXPERIMENTS AND RESULTS

The FBYOD was validated within the corporate environment of the city hall of São Bento do Sul, state of Santa Catarina - Brazil. To reach this goal, 28 devices compatible with the BYOD policy were used. Fig. 5 shows the statistics of the data obtained.

As shown in fig. 5, users neglect security settings, primarily related to the password category. Among the data set obtained, no device used configurations to require alphanumeric password, minimum password size, minimum complex characters, wipe data after excessive failed login attempts, password age and password history. More severely, 7 handsets do not use any type of passwords at all. It is also observed that the use of anti-malware tool is poorly adopted, thus facilitating the infection and dissemination of malware.

In this data sample, the average number of files stored in the memory of the mobile device is eight times greater than reported in the literature, an average of 4056 files stored per device. The SMS amount is also greater than recommended, an average of 206 messages stored per device. All these vulnerabilities represent a possibility for the occurrence of data theft and consequent financial loss.

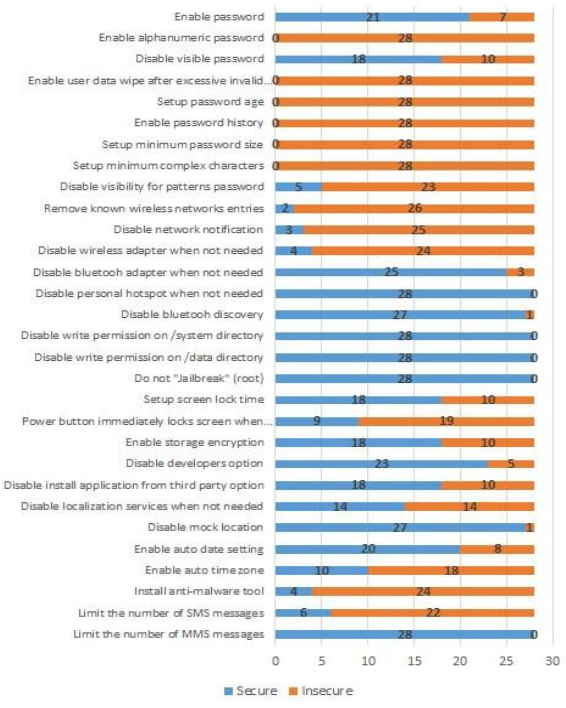

Fig. 5 - Statistics collected from 28 devices.

On the other hand, important aspects of security have been preserved. No evaluated device has been ”jailbroken” or has write permissions to the /data and /system directories. It is also observed that a considerable part of the users adopt measures for the correct lock of the device’s screen, storage encryption and installation of third-party applications. In this way, the surface to be explored in a possible data theft is reduced.

To access the information made available in the FBYOD Storage module, three devices were classified to access high relevance files and none for medium-relevance ones. On the other hand, 25 equipment were classified to access only low relevance files. Regarding the equipment classified to access low-relevance files, 24 of them obtained this classification in order of one or more “fundamental configurations” were in disagreement with recommended values. Table VII illustrates the security impact index generated by FBYOD for all assessed devices.

Table VII: Security Impact Index Generated by FBYOD.

Device	Security Impact Index	Access Level
Device 1	20,93	High-relevance files and below.
Device 2	25,81	High-relevance files and below.
Device 3	21,90	High-relevance files and below.
Device 4	90,16	Low-relevance files.
Device 5	100	Low-relevance files.
Device 6	100	Low-relevance files.
Device 7	100	Low-relevance files.
Device 8	100	Low-relevance files.
Device 9	100	Low-relevance files.
Device 10	100	Low-relevance files.
Device 11	100	Low-relevance files.
Device 12	100	Low-relevance files.
Device 13	100	Low-relevance files.
Device 14	100	Low-relevance files.
Device 15	100	Low-relevance files.
Device 16	100	Low-relevance files.
Device 17	100	Low-relevance files.
Device 18	100	Low-relevance files.
Device 19	100	Low-relevance files.
Device 20	100	Low-relevance files.
Device 21	100	Low-relevance files.
Device 22	100	Low-relevance files.
Device 23	100	Low-relevance files.

Device 24	100	Low-relevance files.
Device 25	100	Low-relevance files
Device 26	100	Low-relevance files
Device 27	100	Low-relevance files
Device 28	100	Low-relevance files

VIII. FBYOD INTERFACES

FBYOD consists of two user interfaces. Fig. 6 shows the login interface and fig. 7 presents the interface with the list of available files for that device. Below the list of files, it is shown the security impact index of that mobile device and the relevance of the information it is classified to access. In the example illustrated by fig. 7 the device has a security impact index of 20,94 and is rated to access information of low, medium and high relevance.

Fig. 6 - FBYOD login screen.

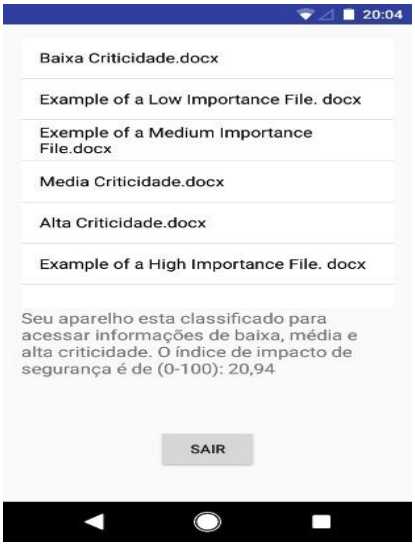

Fig. 7 - FBYOD available files screen and security impact index description.

IX. LIMITATIONS AND FUTURE WORK

As limitations, FBYOD does not propose any type of correction in the customizable security settings if they are set with unsafe values. Likewise, the file counter module treats all file types equally, without weighing any confidentiality, availability and integrity criteria. Still as a limitation, this version of FBYOD does not allow uploading files through the client interface.

As future work, it is desired to implement patches for the unsecured settings.Additonaty, it is opportune to develop a method to assess confidentiality, availability and integrity criteria of all counted files, so the limitation of treating equally the users' files considered by FBYOD is mitigated.

X. CONCLUSIONS

After analyzing the results obtained by FBYOD, it becomes evident that a considerable part of the users does not adopt recommendable measures of security, mainly related to password category. Thus, severe data thefts can occur due to these vulnerabilities and allied the amount of files stored in the equipment eight times greater than that found in the literature.

FBYOD has proven effective in providing an access level to corporate files whose importance is consistent with the security impact index that the device represents and thus mitigate the security impact of data theft and other digital threats.

REFERENCES

[1] E. Sitnikova and M. Asgarkhani, "A strategic framework for managing internet security," in Fuzzy Systems and Knowledge Discovery (FSKD), 2014 11th International Conference on. IEEE, 2014, pp. 947–955.

[2] T. Oktavia, Y. Tjong, H. Prabowoet al., "Security and privacy challenge in bring your own device environment: A systematic literature review," in Information Management and Technology (ICIMTech), International Conference on. IEEE, 2016, pp. 194–199.

[3] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, "Review of the information security and privacy challenges in bring your own device (byod) environments," Journal of Information privacy and security, vol. 11, no. 1, pp. 38–54, 2015.

[4] D. A. Vecchiato, "Benchmarking user-defined security configurations of android devices," Ph.D. dissertation, Unicamp - UniversidadeEstadual de Campinas, Campinas - Brazil, 2016.

[5] M. Lazar, "Byod statistics provide snapshot of future," https://bit.ly/2Ccjw5l/, 2017, accessed 12/13/2018.

[6] R. Ko, A. Tan, and T. Gao, "A mantrap-inspired, user-centric data leakage prevention (dlp) approach," in Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, Dec 2014.

[7] Symantec, "Internet security threat report - istr," Symantec Corporation, techreport 22, Apr. 2017. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[8] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 3–14.

[9] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 95–109.

[10] L. Page, "The trade offs for bring your own devices," IS Practices for SME Success Series, vol. 1, no. 1, 2013.

[11] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," Computers & Security, vol. 29, no. 8, pp. 840–847, 2010.

[12] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices," in Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011, pp. 96–111.

[13] W. Jeon, J. Kim, Y. Lee, and D. Won, "A practical analysis of smartphone security," in Symposium on Human Interface. Springer, 2011, pp. 311–320.

[14] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A model for information assurance: An integrated approach," in Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, vol. 310. United States Military Academy, West Point. IEEE, 2001.

[15] R. S. Ross and M. M. Swanson, "Standards for security categorization of federal information and information systems," NIST, techreport NIST FIPS 199, Feb 2004. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[16] G.-l. Shao, X.-s. Chen, X.-y. Yin, and X.-m. Ye, "A fuzzy detection approach toward different speed port scan attacks based on dempstershafer evidence theory," Security and Communication Networks, vol. 9 , no. 15, pp. 2627–2640, 2016, sCN-14-0841.R1. [Online]. Available: http://dx.doi.org/10.1002/sec.1508

[17] H. Fatima, G. N. Dash, and S. K. Pradhan, "Soft computing applications in cyber crimes," in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), March 2017, pp. 66–69.

[18] L. A. Zadeh, "Fuzzy sets," in Fuzzy Sets, Fuzzy Logic, And Fuzzy Systems: Selected Papers by Lotfi A Zadeh. World Scientific, 1996 , pp. 394–432.

[19] W. Yunwu, "Using fuzzy expert system based on genetic algorithms for intrusion detection system," in 2009 International Forum on Information Technology and Applications, vol. 2, May 2009, pp. 221–224.

[20] A. Almutairi, D. Parish, and J. Flint, "Predicting multi-stage attacks based on ip information," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), Dec 2015, pp. 384–390.

[21] G. P. Rout and S. N. Mohanty, "A hybrid approach for network intrusion detection," in 2015 Fifth International Conference on Communication Systems and Network Technologies, April 2015, pp. 614–617.

[22] N. Naik, "Fuzzy inference based intrusion detection system: Fi-snort," in Computer and Information Technology; Ubiquitous Computing andCommunications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. IEEE, 2015, pp. 2062–2067.

[23] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "Byod security engineering: A framework and its analysis," Computers & Security, vol. 55, pp. 81–99, 2015.

[24] A. Armando, G. Costa, A. Merlo, L. Verderame, and K. Wrona, "Developing a natobyod security policy," in Military Communications and Information Systems (ICMCIS), 2016 International Conference on. IEEE, 2016, pp. 1 – 6.

[25] CIS, "Security benchmarks," https://www.cisecurity.org, 2018, accessed 04/30/2018.

[26] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 228–235.

[27] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Moller, "On the need for different security methods on mobile phones," in Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. ACM, 2011, pp. 465–473.

[28] F. Yao, S. Y. Yerima, B. Kang, and S. Sezer, "Fuzzy logic-based implicit authentication for mobile access control," in SAI Computing Conference (SAI), 2016. IEEE, 2016, pp. 968–975.

[29] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in Proceedings of the 11th international conference on mobile and ubiquitous multimedia. ACM, 2012, p. 13.

[30] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: keystroke-based authentication system for smartphones," Security and Communication Networks, vol. 9, no. 6, pp. 542–554, 2016.

[31] MITRE, "Cve - common vulnerabilities and exposures," https://cve.mitre.org, 2018, accessed 05/01/2018.

[32] H. Zhang, D. She, and Z. Qian, "Android root and its providers: A double-edged sword," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 1093–1104.

[33] Y. Shao, X. Luo, and C. Qian, "Rootguard: Protecting rooted android phones," Computer, vol. 47, no. 6, pp. 32–40, 2014.

[34] P. R. Uhlig, "Fuzzy byod - fbyod," play.google.com/store/apps/details?id=mestrado.dissertacao.com.fbyod, 2018.

[35] Google, "Developers – Android Studio" https://developer.android.com/studio, 2018, accessed: 09/23/2018

[36] ——, "Google play store," https://play.google.com/store, 2018, accessed 14/11/2018.

[37] ——, "Android developer," https://developer.android.com/, 2018, accessed 08/01/2018.

[38] "Stackoverflow,"https://stackoverflow.com/,2018, accessed: 08/07/2018.

[39] Rada-Vilela, "fuzzylite: a fuzzy logic control library," 2017. [Online]. Available: http://fuzzylite.com

[40] "Matlab2019," https://www.mathworks.com/products/matlab.html, 2019

[41] Google, "Google firebase realtime database," 2018. [Online]. Available: https://firebase.google.com

[42] ——, "Google firebase administration console," 2018. [Online]. Available: https://console.firebase.google.com

[43] ——, "Google firebase storage," 2018. [Online]. Available: https://firebase.google.com

Table II Customizable Configurations and Security Recommendations.

Customizable Configuration	iOS	Android	Recommended Value
Category - Password			
Enabled password	X	X	Enabled
Permit simple password	X		Disabled
Enable alphanumeric password	X	X	Enabled
Disable visible password		X	Disabled
Enable user data wipe after excessive invalid password input	X	X	Enabled, 10 attempts
Invalid password maximum input attempts	X		6
Setup password age		X	Up to 90 days
Enable password history		X	At least 24 passwords
Setup minimum password size	X	X	6 iOS, 5 Android
Setup minimum complex characters	X	X	2
Disable visibility for pattern password		X	Disabled
Category - Network			
Remove known wireless network entries	X	X	Enabled
Disable network notification	X	X	Disabled
Disable wireless adapter when not needed	X	X	Disabled
Disable bluetooth adapter when not needed	X	X	Disabled
Disable personal hotspot when not needed	X	X	Disabled
Enable SIM card protection		X*	Enabled
Disable bluetooth discovery	X	X	Disabled
Disable wireless network auto reconnect	X	X*	Disabled
Disable VPN when not needed	X	X*	Disabled
Only connect at trusted wireless networks	X	X	-
Disable wireless wizard		X*	Disabled
Use VPN when connected to public wireless network	X	X	-
Category – Permission			
Disable write permission on /system directory		X	Disabled
Disable write permission on /data directory		X	Disabled
Do not “Jailbreak” (root)		X	Disabled
Category - System			
Setup screen lock time (in seconds)	X	X	iOS 120, Android 90
Power button immediately locks screen when pressed	X	X	Enabled
Enable storage encryption		X	Enabled
Disable developers option		X	Disabled
Disable install third-party application option		X	Disabled
Disable localization services when not needed	X	X	Disabled
Disable mock location	X	X	Disabled
Enable automatic date and time zone setup	X	X	Enabled
Install antimalware tool		X	Installed
Disable AirDrop discovery	X		Disabled
Disable voice dialing when device is locked	X		Disabled
Disable “Siri” usage when device is locked	X		Disabled
Disable application previews when device is locked	X		Disabled
Enable option that denies user profile removal	X		Enabled
Disable managed application to save data into iCloud	X		Disabled
Enable encrypted iCloud backups	X		Enabled
Force backup encryption	X		Enabled
Disable untrusted certificates	X		Disabled
Disable unmanaged source documents to managed destinations	X		Disabled
Setup AirDrop as an unmanaged destination	X		Disabled
Disable Handoff usage	X		Disabled
Disable Control Central notification when screen is locked	X		Disabled
Enable fraud warning	X		Enabled
Enable Safari domain management	X		Enabled
Enable notification only from managed applications	X		Enabled
Disable SMS preview when screen is locked	X	X*	Disabled
Remove all data before device disposal	X	X	-
Enable “Find my Device” function	X	X*	Enabled
Check if firmware is up to date	X	X*	Enabled
Disable “Smart Lock” function		X*	Disabled
Enable device remote location finding		X*	Enabled
Remove guest profiles		X*	-
Frequently check applications’ permissions		X	-
Category – Content			
Limit the number of stored SMS messages		X	Up to 20
Limit the number of stores multimedia messages		X	Up to 20
Allow message moving from this user account	X		Disabled
Keep application up to date	X		-
Category – Browser			
Accept web cookies	X		From the visited web sites
Disable auto-fill content in browser	X	X*	Disabled
Disable browser’s plug-ins		X*	Disabled
Disable stored password into the browser	X	X*	Disabled
Enable SSL site checks	X	X*	Enabled