Journal of Engineering
journal homepage: www.joe.uobaghdad.edu.iq
Number 7 Volume 27 July 2021

Electrical, Electronics and communications, and Computer Engineering

Proposed Security Framework for Mobile Data Management System

Samar Taha Yousif *
Lecturer
Baghdad College of Economic Sciences University
Baghdad, Iraq
samaral_ani@baghdadcollege.edu.iq

Zaid Abass Fadahl
Assistance Lecturer
Baghdad College of Economic Sciences University
Baghdad, Iraq
zaid.alhaboobi@baghdadcollege.edu.iq

ABSTRACT

Portable devices such as smartphones, tablet PCs, and PDAs are a useful combination of hardware and software turned toward the mobile workers. While they present the ability to review documents, communicate via electronic mail, appointments management, meetings, etc. They usually lack a variety of essential security features. To address the security concerns of sensitive data, many individuals and organizations, knowing the associated threats mitigate them through improving authentication of users, encryption of content, protection from malware, firewalls, intrusion prevention, etc. However, no standards have been developed yet to determine whether such mobile data management systems adequately provide the fundamental security functions demanded by organizations and whether these functions have been securely developed. Therefore, this paper proposes a security framework for mobile data that combines core security mechanisms to avoid these problems and protects sensitive information without spending time and money deploying several new applications.

Keywords: Mobile data Management System, Security Requirement, Security Framework, Smartphones, tablet PCs.

اقتراح إطار أمني لنظام إدارة بيانات الأجهزة المحمولة

زيد عباس فضل
مدرس مساعد
كلية بغداد للعلوم الاقتصادية الجامعة
بغداد ، العراق

سمر طه يوسف*
مدرس
كلية بغداد للعلوم الاقتصادية الجامعة
بغداد ، العراق

الخلاصة

تعد الأجهزة المحمولة مثل الهواتف الذكية وأجهزة الكمبيوتر اللوحية وأجهزة المساعد الرقمي الشخصي مزيجا مفيدا لأصحاب الاعمال المتنقلين لمساعدتهم على مراجعة المستندات ، التواصل عبر البريد الإلكتروني ، إدارة المواعيد والاجتماعات الخ. و مع تلك الامكانيات فأنها تفتقر الى ميزات الأمان الأساسية. و من اجل معالجة المخاوف الأمنية للبيانات الحساسة والمحافظة عليها يتم استخدام اثبات الشخصية، تشفير المحتوى والبيانات المهمة ، الحماية من البرامج الضارة ، الجدران النارية ، منع

*Corresponding author
Peer review under the responsibility of University of Baghdad.

https://doi.org/10.31026/j.eng.2021.07.02

Article received:18/10/2020
Article accepted: 16/3/2021
Article published:1/7/2021

التطفل والاختراق ، الخ. و لكن لحد الان لم يتم تطوير او اقتراح اي معايير لتحديد ما اذا كانت أنظمة إدارة الأجهزة المحمولة توفر وظائف الأمان الأساسية التي تطلبها المؤسسات بشكل كافٍ. لذلك ، تقترح هذه الورقة إطار عمل لإدارة بيانات الاجهزة المحمولة للجمع بين آليات الأمن الأساسية لتجنب المشاكل و لحماية المعلومات الحساسة دون إضاعة الوقت والمال في نشر العديد من التطبيقات الجديدة.

الكلمات الرئيسية: نظام ادارة معلومات الاجهزة المحمولة، متطلبات الأمان، أطر الأمان، أجهزة الهاتف الذكية.

1. INTRODUCTION

With the popularization of mobile devices and the continuous expansion of the mobile Internet industry, more and more user groups can use a variety of mobile applications through smartphones, tablets, etc., to assist work, study, food, clothing, housing, transportation, etc., making the work and life of individuals more convenient **(Reinfelder and Benenson, 2017).** In order to ensure the user's controllability and preventing leakage problems of some applications and data, a mobile management system is used to realize the remote management function for the mobile terminal **(Taal et al., 2017).** With the rise of (Bring Your Own Device) BYOD in recent years, many security challenges have been brought to the internal security management **(Jamal et al., 2018)**, a lot of companies have started to deploy mobile management systems, trying to build a secure and reliable environment when users access and process companies information via mobile terminals **(Eslahi et al., 2015)**. The major security problem is not concerning the devices or the data inside the company, but it’s concerning managing the access of the user and the device to the company data and increasing of the enterprise network in exposure to malware because mobile devices lack visibility and control **(Jamal et al., 2020)**. Various mobile device management system frameworks continue to evolve, and products are constantly being modified. The remote wipe, device lock, location information reporting, and other functions provided have enhanced controllability and security to a certain extent **(Vorakulpipat et al., 2017)**. If the mobile management system has security risks, it can trigger more severe security issues. For example, the mobile terminal is illegally locked, information is illegally removed, private information is gathered illegally, and communication content is leaked.

This paper comprehensively analyzes the security threats that mobile management may face and offers security solutions for mobile management systems in terms of identity, communication software, and data.

This paper is structured as follows: Section 2 explains the basic operating concept of mobile management; Section 3 summarizes and analyzes various security issues and challenges in current mobile management; Section 4 presents the countermeasures to security threats, the common mobile management approach, and the overall security framework of mobile management; Finally, Section 5 summarizes the content of this paper.

2. WORKING PRINCIPLE OF MOBILE MANAGEMENT

Mobile management system typically consists of two parts: a mobile terminal (smartphones, tablet computers, etc.) and a management platform (management servers, certificate servers, database servers, etc.) which communicates through a mobile data communication network or wireless networks such as Wi-Fi **(Adinugroho, Reina and Gautama, 2015)**. In order to improve security, the management platform usually adds an additional area for the agent to provide external services. The composition of the mobile management system is shown in **Fig. 1**.

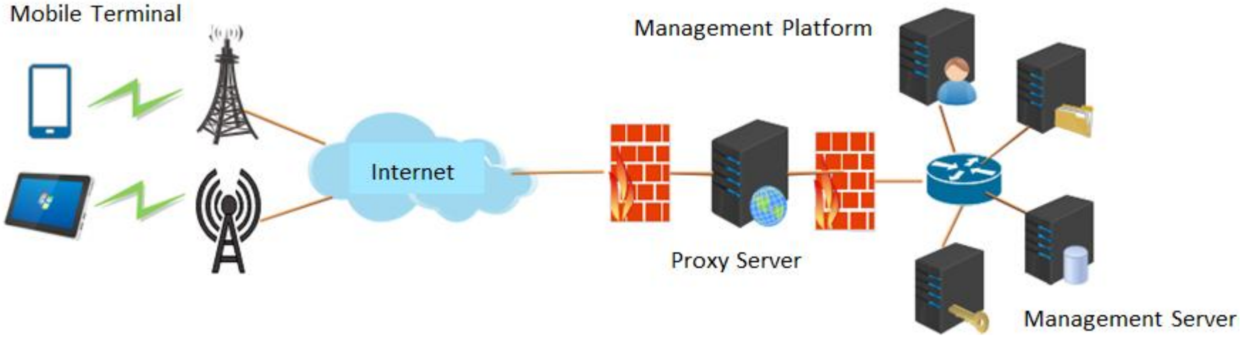

Figure 1. Semantic diagram of the mobile management system.

Terminal devices need to undergo operations such as registration, identity verification, and approval before the management platform can realize the daily management of terminal devices, like issuance of instructions and strategies, execution, and results reporting **(Delac, Silic, and Krolo, 2011)**. The mobile management system's account opening and registration process primarily combine the following steps: managers import user and terminal information; user operations trigger registration, and the terminal sends a request for registration to the management platform; the management platform reviews the request; if manual intervention is necessary, registration will be submitted for approval to the management; once the user and device identity has been verified to be valid, the management platform will return a successful registration response to the mobile terminal, turn on the remote management function, and incorporate the terminal into a regular mobile management system.

Mobile management system key function can be divided into account opening (including configuration, deployment, and registration) and day-to-day management. **Fig. 2** shows the registration process.

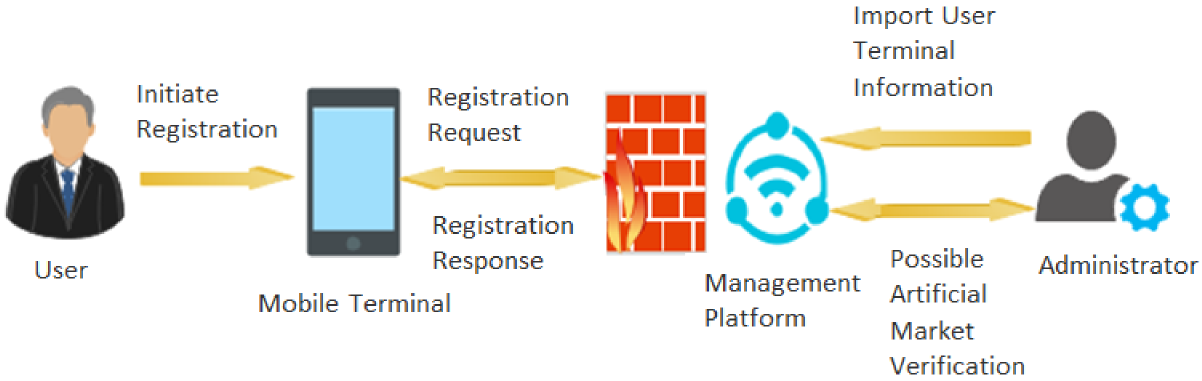

Figure 2. Semantic diagram of the mobile management registration process.

The general way of managing mobile terminals regularly primarily comprises the following steps: managers log in to the management platform and issue instructions; the mobile terminal receives the instructions and executes them after checking its validation; the terminal reports the output results to the management platform; managers may display the instruction execution results via the management platform. The specific management process is shown in **Fig. 3**.

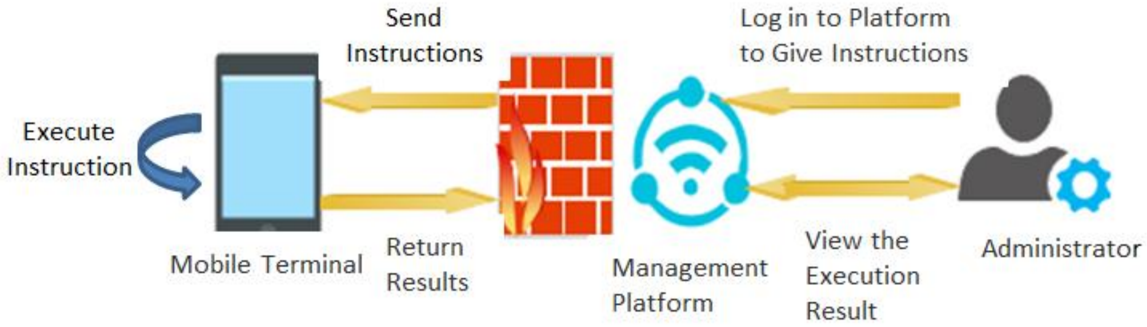

Figure 3. Semantic diagram of the mobile management process.

3. MOBILE MANAGEMENT SECURITY THREAT ANALYSIS

The security threats facing mobile management systems mainly include system, communication environment, functions, and data. It can be divided into three types: security threats to the core operating environments such as the platform's security and mobile terminal security and other specific operating environments, for channels communication security threats such as identification, signaling and business data threats, security threats for the implementation of functions such as platform management and terminal strategy execution; security threats for data usage and storage, etc. **(Sheila, Faizal and Shahrin, 2015)**. **Fig. 4** shows mobile data security architecture design. This paper will elaborate on the various security threats mentioned above.

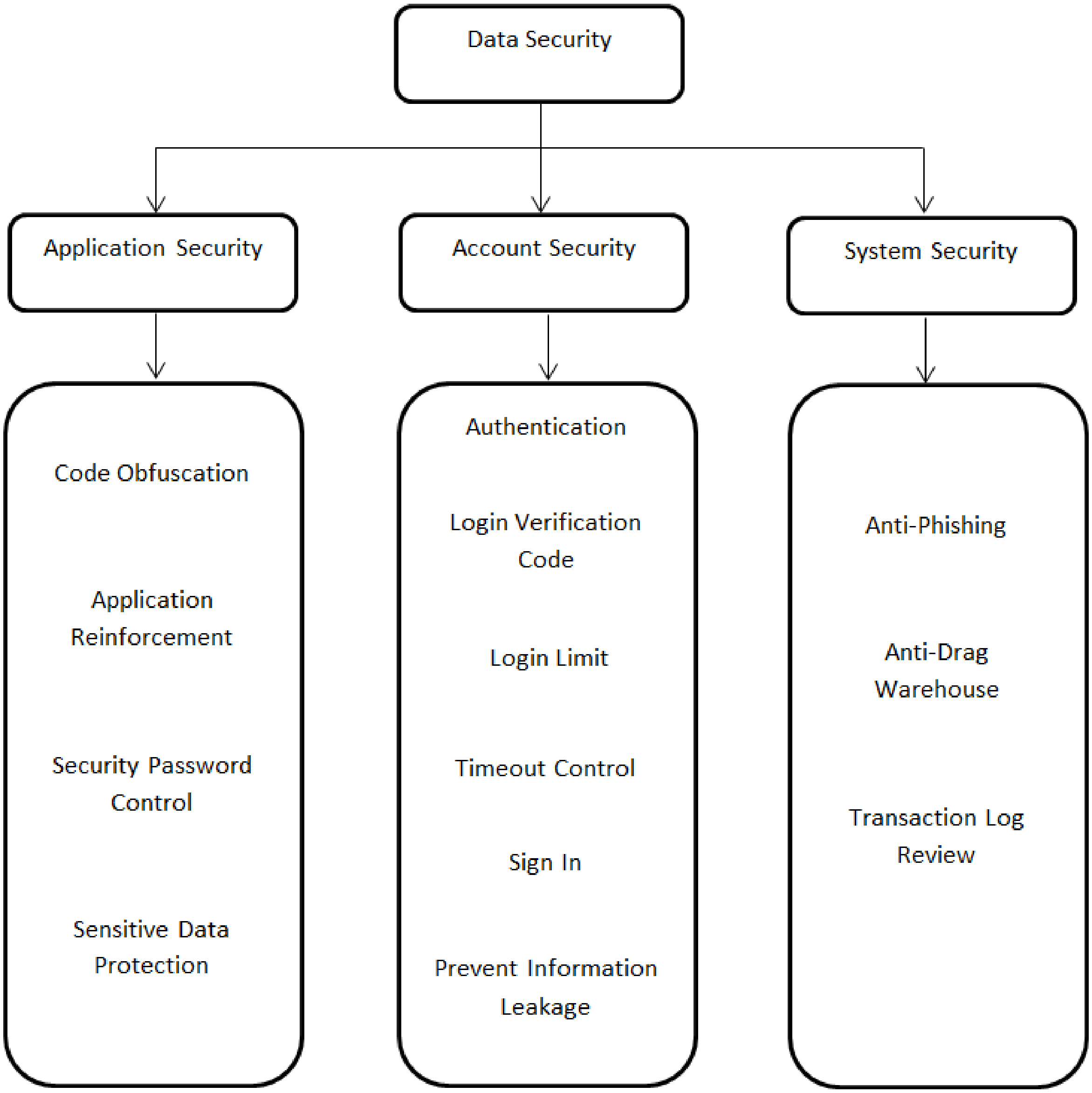

Figure 4. Mobile data security architecture design.

3.1 Basic Operating Environment Security Threats

The basic operating environment can be divided into two parts: mobile terminal and management platform. When the basic operating environment suffers from major security threats, mobile security cannot be guaranteed. The fundamental security threats of mobile terminals include the following aspects primarily: security threats to terminal hardware layers, security threats to system software layers, and security threats to device software layers. Security threats to the hardware and system software layers will affect mobile management directly, including chip security, electromagnetic monitoring, operating system vulnerabilities, and backdoors **(Zlatanov, 2016)**. In addition, framework issues and system rooting are usually high due to mobile management software. Therefore, the effect of security threats at the application software layer is often ignored **(Cesaratto and Forman, 2017).** However, since the security threats at the application software layer are complex, variable, and large in number, they may even target mobile management software attacks.

Basic security threats on the mobile platform include mostly malicious code, password blasting attacks, DDOS attacks, deep-hole system database slip holes, middleware vulnerabilities, and basic library slip holes, etc. **(Kim, 2016)**, **(Mittal and Mishra, n.d.)**. Furthermore, the protection of the basic network services involved, including DNS and other security threats, also needs to be considered **(Kassem et al., 2019)**. While traditional network security threats have been examined more comprehensively, new attacks and slip-hole use continue to occur and grow rapidly. Therefore, mobile platform security threats still require a continuous update.

3.2 COMMUNICATION SECURITY THREATS

Securing communication between mobile terminals and management platforms are essential requirements for remote management due to the mobile management system complement the comprehensive management of mobile terminals. Therefore, the information privacy and control commands have higher requirements for the reachability, privacy, integrity, and non-repudiation of the information **(Moshir, 2015)**. If credibility and security cannot be ensured, mobile management will also lose its proper meaning **(Chen et al., 2016).**

In a broader context, communication security threats can be divided into the following:

● Channel security threat: the communication link between the mobile terminal and the management platform may be subject to various attacks, such as illegal closure of mobile data links or Wi-Fi interference, communication data discarding, and so on, leading to a communication unable to establish, maintain or transfer data, resulting in mobile terminals being removed from the control of management platform (Smartphones and Pomak, n.d.).

● Identity security threats: If security vulnerabilities occur in the identity authentication between the management platform and the mobile terminal, security issues that arise, such as terminal access to a fake management platform, a large number of invalid mobile terminals are recorded on the management platform, and the terminal's online status is falsified. This results in serious consequences such as the failure of the entire mobile management system, and even mobile terminals are illegally managed **(Cesaratto and Forman, 2017)**.

● Data communication security threats: mainly including monitoring, modification, and forgery of communication content. Once the communication content is monitored, the attacker can obtain privacy through monitoring, such as terminal location information. Changing or copying management instructions can result in invalid or illegal management of the terminals.

3.3 SOFTWARE IMPLEMENTATION SECURITY THREATS

When designing and implementing the various functions of the mobile management system software, there can be many security hazards, including design flaws, implementation process conflict with design expectations, code bugs and configuration management errors, etc. All these are security problems that must be addressed during the design and deployment of the software **(Nagappan and Shihab, 2016)**.

3.4 DATA USAGE AND STORAGE SECURITY THREATS

Mobile management generates a huge amount of privacy and sensitive data, where the use and storage of such data pose many security threats **(Cesaratto and Forman, 2017).** If proper security measures and technologies are not used for protection, it may lead to major safety issues such as data leakage. The security threats in data usage and storage primarily include the use or storing of user passwords, keys and private information in plain text, data protection keys are not secured, the strength of the encryption algorithm is too weak and data access is not effectively controlled; data is exported or shared without encryption, desensitization or incomplete processing, etc. **(P. et al., 2016)**.

4. A MOBILE MANAGEMENT SECURITY FRAMEWORK

In order to resolve security risks and security threats that may occur in the mobile management system, it is essential to use various security technologies comprehensively and to incorporate a complete security management system in designing, developing, upgrade maintenance and management, etc. then conduct safety maintenance work during the life cycle to ensure mobile management system security and reliability. The next subsection explains the cryptographic techniques, security tools, and security measures that may be involved in mobile management security. Based on that and on the characteristics of the mobile management system, a new mobile security framework is proposed that can respond comprehensively to different security threats.
The proposed framework gives a more extensive vision by considering state-of-art information, modernistic mobile terminals, and most recent improvement innovations in the framework design.

4.1 SECURITY TECHNOLOGY

● Cryptographic technology: It forms the basis of several security protections. The cryptographic technologies that could be sandy in mobile management include encryption and decryption digests and verification of signatures, etc. primarily. The latest popular algorithms include AES, RSA, ECC, SHA series, MD5, ElGamal, and so on **(Mathur, Agarwal and Sharma, 2015)**. Furthermore, HMAC, which is a combination of digest function and secret, and CBC digest created by the encryption algorithm, are also used in large numbers **(Naik, Jenkins and Newell, 2017; Whiteman and Data, 2017).**

● Security tools: In order to deal with different security threats, there is a large number of security equipment and security software. Using these security tools can effectively improve the system's security protection capabilities and withstand various attacks. The core security tools are VPN, Firewall, IDS/IPS, WAF, gatekeeper, virus protection system, data leakage prevention DLP, Vulnerability scanning tools, code security review testing tools, system status monitoring tools, etc. **(Ammari *et al.*, 2017; Ajibo *et al.*, 2018; Tian *et al.*, 2018; Yu *et al.*, 2018)**.

● Security measures: Comprehensive use of various security measures to achieve different security functions is an important part of maintaining the security of mobile management, which include: identity authentication, authorization control, log activity audit, data protection, software protection, monitoring of environmental status, monitoring of service status, equipment monitoring, and timely system upgrades, etc. **(Cai and Wu, 2018)**.

4.2 MOBILE MANAGEMENT SECURITY FRAMEWORK

Several security threats affect the mobile management system. Based on the composition of mobile management, business, environment, and the security threats faced by mobile management, a complete mobile management security framework is designed to address various security concerns. Mobile management security can be divided into four sections according to the category and level of work: security management, basic security, operational and maintenance security, and business security. Security management involves all forms of security-related organizational management work, which is a required management assurance for secure mobile management, while the security function for the basic operating environment of the mobile management system is fundamental security. Furthermore, the security of operation and maintenance is used to ensure the availability of a mobile management system. Finally, protection for companies is represented by the protection of the mobile management system itself.

Fig. 5 demonstrates the proposed mobile management security framework. Security management, operation, maintenance security, and basic security are the security issues facing all mobile service systems. Although business security requires targeted design based on the characteristics of mobile management services, and due to the sensitivity of the mobile management operation, it is necessary to perform two-way identity authentication for all parties, encryption core communication content, etc.; In addition, to ensure channel availability, multiple communication channels such as SMS, near-field communication, etc., are supported to enhance management command accessibility.

Mobile application software may also face threats such as analysis of recompilation and malicious calculations. Therefore, it is important to incorporate code obfuscation, remote anti-calculation change, and other security protection measures in design and development. Furthermore, in order to ensure the privacy of the terminal identity, it is necessary to perform operations such as confusion, randomization, temporalization, and encryption on identity information must be carried out to avoid terminal identity leakage and trigger security problems such as tracking.

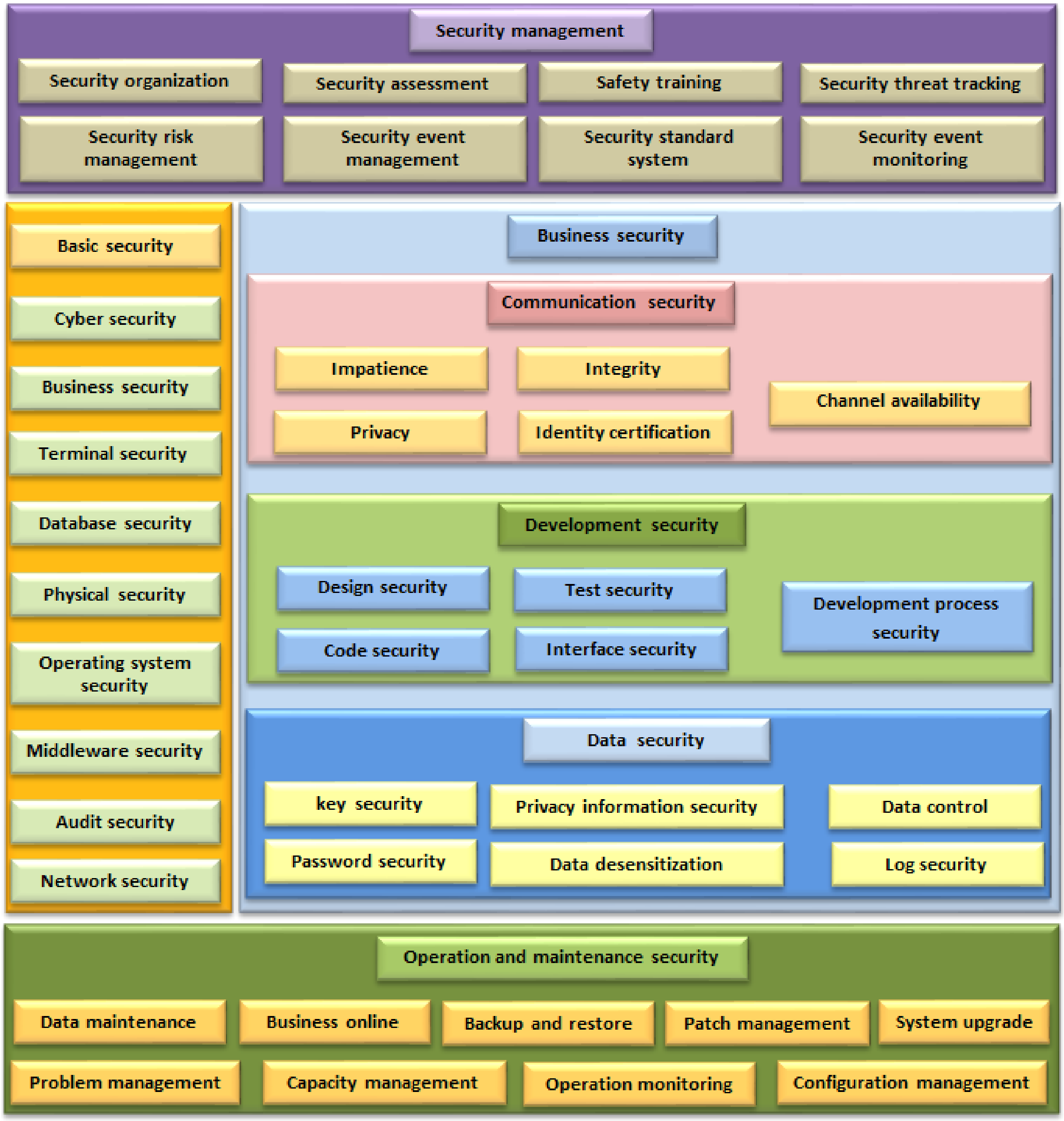

Figure 5. Schematic diagram of the proposed mobile management security framework.

The mobile management security framework described above does not affect the actual mobile management implementation. Any current mobile management system can refer to this security framework to enhance security protection capabilities at all levels. Thus, the framework has the benefits of wide applicability and can satisfy the mobile management system's actual user requirements.

5. CONCLUSIONS

A secure comprehensive framework that covers different security issues related to the mobile data management system environment was proposed. The most essential characteristics of the proposed framework are:

1) Summarizes standard security classifications and proposes some targeted security problems and ways of resolving them to reduce the risk of leakage and theft of corporate information transmitted via mobile devices

2) Resolve the emerging security challenges of the mobile data management system

3) Enhancing mobile management security without modifying the basic implementation process of current mobile management. As future work, the proposed framework needs to be implemented and tested to validate its effectiveness and efficiency.

REFERENCES

- Adinugroho, T.Y., Reina and Gautama, J.B., 2015. Review of Multi-platform Mobile Application Development Using WebView: Learning Management System on Mobile Platform. Procedia Computer Science, [online] 59(Iccsci), pp.291–297. Available at: <http://dx.doi.org/10.1016/j.procs.2015.07.568>.
- Ajibo, A.C., Udechukwu, F.C., Ogbuka, M.C., Nwafor, C.U., Nwachi-Ikpo, J., and Ani, C.I., 2018. Review of network integration techniques for mobile broadband services in next generation network. Nigerian Journal of Technology, 37(2), p.470.
- Ammari, N., El Mrabti, A.A., El Kalam, A.A., and Ouahman, A.A., 2017. Securing the mobile environment: Firewall anti-leak of sensitive data on smartphone. ACM International Conference Proceeding Series.
- Cai, Y., and Wu, F., 2018. Data Security Framework for Electric Company Mobile Apps to Prevent Information Leakage. Procedia Computer Science, [online] 139, pp.280–286. Available at: <https://doi.org/10.1016/j.procs.2018.10.269>.
- Cesaratto, B.B.G. and Forman, A.S., 2017. Cyber Threats to Employee Data and Other Confidential Information Are Front and Center in 2017. (May), pp.1–8.
- Chen, M., Qian, Y., Mao, S., Tang, W., and Yang, X., 2016. Software-Defined Mobile Networks Security. Mobile Networks and Applications, [online] 21(5), pp.729–743. Available at: <http://dx.doi.org/10.1007/s11036-015-0665-5>.
- Delac, G., Silic, M., and Krolo, J., 2011. Emerging Security Threats for Mobile Platforms.
- Eslahi, M., Naseri, M.V., Hashim, H., Tahir, N.M., and Saad, E.H.M., 2015. BYOD: Current state and security challenges. ISCAIE 2014 - 2014 IEEE Symposium on Computer Applications and Industrial Electronics, pp.189–192.
- Jamal, F., Abdullah, M.T., Abdullah, A., and Hanapi, Z.M., 2018. Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology. International Journal of Engineering & Technology, 7, pp.74–79.
- Jamal, F., Abdullah, M.T., Abdullah, A., and Mohd, Z., 2020. A Systematic Review Of

Bring Your Own Device (BYOD) Authentication Technique A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique.

- Kassem, J.A., Sayeed, S., Marco-gisbert, H., and Pervez, Z., 2019. applied sciences DNS-IdM : A Blockchain Identity Management System to Secure Personal Data Sharing in a Network.
- Kim, G., 2016. Secure Mobile Device Management Based on Domain Separation. pp.918–920.
- Mathur, R., Agarwal, S., and Sharma, V., 2015. Solving security issues in mobile computing using cryptography techniques - A Survey. International Conference on Computing, Communication and Automation, ICCCA 2015, pp.492–497.
- Mittal, P., and Mishra, M.K., n.d. Trust and Reputation-Based Model to Prevent Denial-of-Service Attacks in Mobile Agent System. [online] Springer Singapore. Available at: <http://dx.doi.org/10.1007/978-981-13-2348-5_22>.
- Moshir, S., 2015. (12) United States Patent. 2(12).
- Nagappan, M., and Shihab, E., 2016. Future Trends in Software Engineering Research for Mobile Apps. pp.21–32.
- Naik, N., Jenkins, P., and Newell, D., 2017. Choice of suitable Identity and Access Management standards for mobile computing and communication. Proceedings of the 24th International Conference on Telecommunications: Intelligence in Every Form, ICT 2017.
- P., P., Dhanokar, P., Chaithanya, M.K., and U. Patil, M., 2016. Secure Storage of Data on Android Based Devices. International Journal of Engineering and Technology, 8(3), pp.177–182.
- Reinfelder, L., and Benenson, Z., 2017. Exploring Security Processes in Organizations: the Case of Smartphones. Mensch und Computer 2017 - Workshopband, [online] (September). Available at: <http://dx.doi.org/https://doi.org/10.18420/muc2017-ws05-0403>.
- Sheila, M., Faizal, M. A., and Shahrin, S., 2015. Dimension of mobile security model : mobile user security threats and awareness. 9(1), pp.66–85.
- Smartphones, E. N. and Pomak, W., n.d. Enterprise WiFi Hotspot Authentication with Hybrid. pp.247–250.
- Taal, A., Le, J., Ponce de Leon, A., A. Sherer, J., and S. Jenson, K., 2017. Technological and Information Governance Approaches to Data Loss and Leakage Mitigation. Computer Science and Information Technology, 5(1), pp.1–7.
- Tian, Z., Tian, J., Qiao, H., Li, X., Zhu, H., and Qi, W., 2018. Design of automated security assessment framework for mobile applications. Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2017-Novem, pp.778–781.
- Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., and Savangsuk, V., 2017. A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. Security and Communication Networks, 2017.
- Whiteman, R.E. and Data, R.U.S.A., 2017. (12) United States Patent. 1(12).
- Yu, X., Tian, Z., Qiu, J., and Jiang, F., 2018. A Data Leakage Prevention Method Based on the Reduction of Confidential and Context Terms for Smart Mobile Devices. Wireless Communications and Mobile Computing, 2018.
- Zlatanov, N., 2016. Computer Security and Mobile Security Challenges. (March).