Security Aspects of Cloud Based Mobile Health Care Application

Richard Cimler, Jan Matyska, Ladislav Balik,
Josef Horalek, and Vladimir Sobeslav(✉)

Faculty of Informatics and Management, Department of Information Technologies,
University of Hradec Kralove, Rokitanskeho 62, 50003 Hradec Kralove,
Czech Republic
{richard.cimler,jan.matyska,ladislav.balik,
josef.horalek,vladimir.sobeslav}@uhk.cz

Abstract. As mobile computing has become very common, a new vulnerabilities and security threads appeared. Cloud computing is a new distribution model of services for various technologies and solutions including the mobile applications. Mobile cloud computing benefits from the interconnection of these two areas. This approach brings many assets, but on the other hand, also the security risks and potential problems. This paper discuss **s**ecurity aspects of mobile cloud computing with a focus on the developed health care mobile application using cloud computation services. Personal data about health of the person are one of the most confidential thus need to be secured against different types of threats. Proposed solution is based on the smartphone as a client gathering data and the cloud servers as a computational platform for data storage and analysing.

Keywords: Cloud computing · Security · Mobile application · Health care

1 Introduction

Businesses, government agencies, organizations, and individual consumers are rapidly adopting mobile and cloud computing technologies [2]. This technologies are having a high potential for broadening their development, services, and marketing through information technologies [3] [4]. Securing the personal data is very important part of whole cloud computing concept. General overview of cloud computing security can be found at [5] [6]. Both papers are unique by its complexity and described analysis. Several areas of research and dynamic development of the mobile Cloud computing security are considered. Encryption and key management algorithms, called ad hoc Clouds in [5] are presented as well.

As mentioned in article [5] cloud computing bring various benefits to organizations and users. There are many challenges related to security and privacy in the Cloud environment. It opens up space for research new techniques for security and privacy in mobile Cloud and ad hoc Cloud. This includes a need for a dynamic security model and better crypto (and key management) algorithms that targets different levels of security and privacy for Cloud computing. With the increasing usage of the Cloud

P.C. Vinh et al. (Eds.): ICTCC 2014, LNICST 144, pp. 202–211, 2015.
DOI: 10.1007/978-3-319-15392-6_20

services it is possible to collect sufficient evidence from the cloud providers on the level of trust on each of their services. This can help the service providers, infrastructure providers, and the end-users to better choose the right services from the ever growing Cloud vendors.

In the paper [13] is described usage of virtualization as a tool for solving security issues of cloud computing using M2M (machine-to-machine) communications. In the M2M computing technologies personal computers, Internet, wireless sensors, and mobile devices are working together. There are many security threats for mobile devices which are the same as for the desktop and server ones. Virtualization technique in M2M communication is described as a way for increasing protection against mobile treats and increase of the performance efficiency.

There are a many benefits of Cloud computing but on the other hand a lot of security risks. Many technologies are connected in the Cloud Computing solutions. Together with its capabilities Cloud Computing inherits capabilities of these technologies but its vulnerabilities as well. It is necessary to understand these vulnerabilities to be able to use cloud computing safely. The article [7] presents the security issues of IaaS, PaaS, and IaaS Cloud models. Issues vary depending on the model and described storage. Similarly presents solutions for Cloud deployment model and comprehensive paper [8] and [9]. In papers [10] [11]we can found, that Cloud Service as a kind of Web Services is based on Internet service, it faces all kinds of security problems because Internet has many inherent safety defects and also exists in other attacks and threats. Therefore the development of Cloud Service depends on its security deeply, and it is a major significance to consensus on the Cloud Service security. Security issues of the cloud based application for mobile devices and usage of different frameworks is discussed in many papers, articles and analyses such as [12] [13].

Modern solution for solving security issues is usage of the frameworks. It also enables to ensure the integrity, secure the data and improves user's identification. Proxy-based multicloud computing framework is introduced at [14]. Several features such as dynamic, on-the-fly collaborations, addressing trust, resource sharing among cloud-based services, privacy issues without pre-established collaboration agreements or standardized interfaces are described in this paper. Another Secured Mobile-Cloud framework is proposed in [15]. Framework is focused on the security of data transmitted between the components of a mobile cloud application. Two aspects are taken into the account: energy consumptions and users options regarding the security level required for private data. Several distributed components deployed in the cloud or on the mobile device are included in the framework. There is proposed a proof of concept of Android prototype as well.

2 Safety of Cloud Computing Application and Services

We can classify user data concerning the state of user's health among one of the most personal data that the user has. For that reason, we have to take into consideration the safety of saved data and pay attention to the risks of individual solutions.

Those problems are in most of the cases not connected to a technical solution. A range of safety risks connected with public Clouds run is not solely technical. Prob-

lems connected with cooperation with another subject play a big part here. For example, it is possible to use the situation when the client uses services of supplying company for SaaS. Even if the client verifies the company to find out if it meets the technical requirements, it is reliable, etc., unexpected complications can occur. The company can go bankrupt, it can be merged with another company or bought by another company. Thereafter, our data go to someone else and we cannot influence that. These non-technically orientated issues are the subject of risk management and even though we have to include their risks, they have no direct connection with the operation solution from the technical perspective.

The main technical risk related to public Cloud is a loss of isolation. The isolation is for the run of public Cloud solution absolutely crucial. If the clients run their own service in public Cloud, their operator is obliged to separate their data and processors from other clients even though they share the same hardware. That way the physical disks, processors, RAM memories and network connections are shared and their separation happens in logical layers, in software. The virtualization safety of data storages is very closely connected to that. The user, however, does not have an influence on this operator's environment. The effective protection of application run in Cloud environment resides for the user or operator in a careful selection of the provider and in case that the provider cannot be trusted, it is good to opt for running an own private Cloud.

We have to consider that the run of a private Cloud or a home server does not automatically guarantee a higher safety. This presumption would be possible only in case where we would consider that the operator of the private cloud or home server has unlimited tools or skills for their protection. We would recommend the client to use the services of public Cloud and private Cloud in case that it is convenient to invest resources to building an administration of such solution. When a customer chooses a cloud provider, there are seven general security issues concerning Cloud computing described by Gartner [20]. They include issues like privileged user access which addresses risk of confidentiality disruption. This issue is connected either with data transfers and Cloud service provider. Both are addressed by an application security model and a careful selection of a provider. These risks address most common issues related with cloud-computing oriented solutions. It can be used as a reference for Watchdog implementation same as for general use with any cloud-computing oriented project.

3 Cloud Based Mobile Health Care Application

Modern smartphones are powerful devices with computing performance comparable to personal computers and laptops. Various sensors are embedded into these devices. These sensors are capable of monitoring a lot of different physical quantities which makes smartphones, together with smartphone computation performance, useful devices capable of monitoring and processing information about status of person. It is possible to monitor position of person, not only wide area position using GPS but position of the body towards the earth surface as well. That enables to monitor the

occurrence of critical situations such as a fall of the person to the ground. By using an accelerometer and a gyroscope it is also possible to monitor the person's breathing [21]. Further devices can be located in the surrounding area and transmit information from sensors about the condition of the environment. Actuators controlled by the application should adjust the environment in the location according the health status of the monitored person. Based on data from sensors, the application can create also a notification of the alert action – to call an emergency, to create a warning message to relatives or personal doctor.

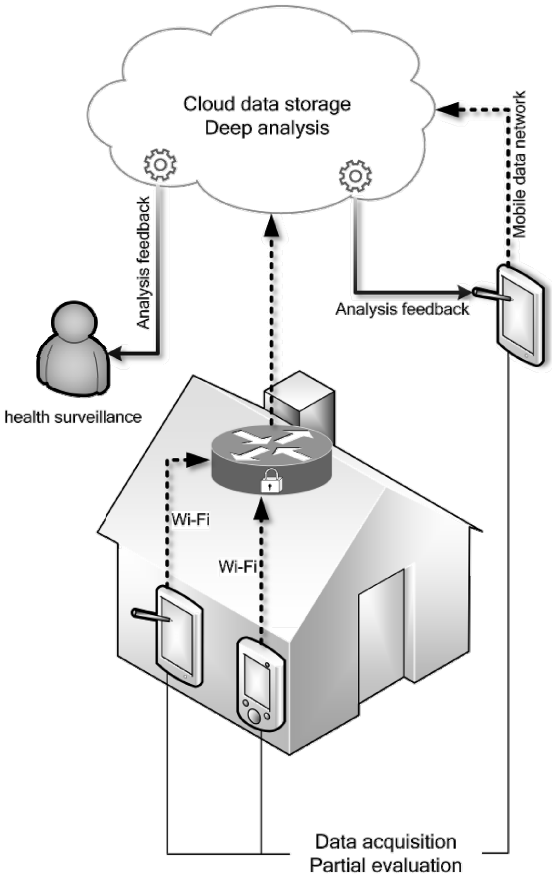

Fig. 1. System scheme

Application named Watch Dog is an application which is being currently created primary to monitor position and activities of the elder people and notify about life threatening situations. Measured data are partly evaluated in the devices in order to find out dangerous situations such as fall of the person. After basic evaluation in the device data are sent to the cloud server where deeper analysis will be running on the long term data. Wi-Fi connection can be used for indoor usage of the system. Data

size of transmitted data is optimized also for using device outdoors with technology 3G, GPRS or LTE. Due to deep analysis computation demands it is run in the cloud server and only most critical functions run on the smart phone. System scheme can be seen on Fig.1.

3.1 Client and Server Communication

There is a communication model required for the receiving and processing the data. Client and server communicate based on this model. The basic parameters of the model are data format, frequency of sending data, and amount of data transferred per one transmission and a confirmation upon receival and cataloging.

Data Transmission Frequency

Based on the used application, a frequency of 1 minute seems adequate as the transmission frequency. During this time interval, the client collects data and every minute prepares a data package that is sent to the server. This time interval can be further adjusted, but there is a problem of high communication utilization. One minute interval allows an evaluation even for some life-threatening situations. Of course the one minute interval is too long for a timely identification of critical situations like a respiratory failure. For a timely identification of such events, data processing must be done on the device itself.

The system logs the data locally and allows to keep up to 48 hours of measurements. These data can be send in one transmission containing the data from the last confirmed synchronization in case there was a communication failure or the service was unavailable for some time. The reason can be for example, the lack of mobile or Wi-Fi data connection.

Data Structure and Extent

The data measured on each sensor are send in a raw form to the server. For this type of data, which is basically a set of numeric variables, easily processable structure of ASCI comma-separated values is to be used. It is a simple, convenient and data format. It is expected to use chunks of data with 300 lines, which are generated by a local data collection in the interval of 200ms. The volume final volume of the data for one minute measurement is to be up to 0.5kB.

Confirmation upon Receival and Cataloguing

The system uses round-robin model for the local (the client's database) storage of data. Therefore only a limited amount (fixed amount after the first 48 hours) of data is stored on the client device and the old data is always replaced with the new one. This way, the client's device database never exceeds the size of 72MB and allows to use the application even on less equipped devices. This mechanism makes the application rather usable not only with the always available Wi-Fi connection but also with a connection provided by a mobile network operator, such as GPRS, CDMA, 3G, LTE, etc.

Every line of ASCI coma-separated data is identified with a time stamp which also serves as a unique key in the server's database. The long-term data are stored in a pre-processed and summarized form.

Upon receival, checksum of the data package is always recalculated, so that it is possible to detect any data corruption during transfer. During the server-client communication, the server confirms the reception of the data packages. The server can also request additional retransmission of some data from the last 48 hours. The data are in this case identified by a timestamp.

3.2 Communication Security Model

There is a two-way communication between client and server, which always uses a communication media that are vulnerable to eavesdropping in some way, whether it is using the Wi-Fi or the Internet. It is necessary not only to encrypt the data, but provide additional security features. For that reason, the application uses [16] AAA security model, Authentication, Authorization and Accounting.

AAA – Authentication, Authorization and Accounting

The AAA is a security model, which provides all the basic security features the system needs. AAA model is a widespread standard, therefore it allows interconnection of the application with other already existing services, such as various domain and authentication services. Authentication, in this case, provides user authentication using a username and a password. With these, the user can access both, the web frontend and mobile applications (where the password is saved for user convenience).

Authorization grants an access to user's own data and also the data of other users, if the he owns the permissions. Authorization also includes a verification of used mobile device for data collection, as discussed further. The purpose of Accounting is a collection of usage information, later used for billing purposes and for access logging to identify safety incidents.

Mobile Device Verification

As a part of authorization, the system uses verification of a mobile device that is connected to the user account and is able to upload logged data to the cloud server. To ensure a stronger security, it is not possible to use just any mobile device with the installed application using a username and a password. In order to communicate with the application, the server authenticates also a unique identifier of the device that is generated upon the first run and registered to the user's account. This method can be combined with an IMEI number verification. This security model is similar to the one that some banks use for their smartphone banking.

Transmission of Recorded and Processed Data

HTTPS protocol is used for the transmission of recorded data [16]. It features a complete model of the security based on the use of certificates and it also includes mechanisms for a safe key exchange, symmetric data encryption and hashing methods. The

server, as well as the application, is to support an SSL 3.0, or alternatively TLS encryption.

Data Encryption
Based on focus of the application, it is necessary to provide a high degree of security. The data are encrypted during the transmission on the level of the application itself and moreover it is presumed, that only secure communication links will be used. On the application level, symmetric encryption of AES protocol is to be used. With the length of a key 256-bit, the sufficient level of security is provided. More secure variant of AES (with a longer key length) can be used, but there is only small amount of additional security in comparison to higher processing requirements. The encryption using AES 256-bit protocol is directly implemented in the Java and other major programming languages and therefore its use is simple for the mobile devices.

4 Mobile Application and Type of Cloud Computing Service Models

Modern mobile applications that require efficient platform for recorded data processing very often use remote data processing by means of servers situated in a local network or in the Internet. These servers then either offer user interface with higher functionality or they only process the data and send them back.

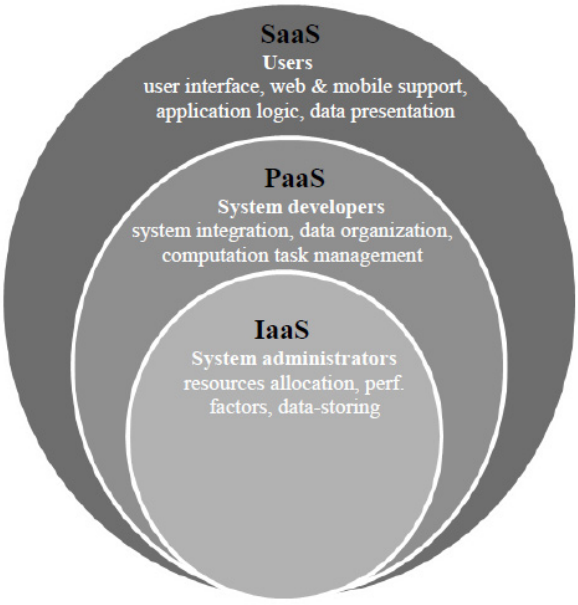

Fig. 2. Cloud computing distribution models

If the concern is an application that needs a remote data processing in order to work and it can make use of the web access as a platform for visualization of those

processed data, it can be thought about a backend platform in form of Cloud solution. With Cloud solution there is a choice of its form. From the point of view of offered services, there can be distinguished three basic distribution models. See Fig.2.

4.1 Watchdog Cloud Computing Solutions

Watchdog application is able to run in three majorly different solutions. Two of them are purely cloud based, and the third is a small environment oriented.

Public Cloud Run as Service
With Watchdog application, Cloud solution for processing and presenting data (in case of public Cloud) has a form of a software run as a service. User has to log into that application and the application will offer three basic services. First, there is a performance for data processing and processing itself. Second, there is a presentation of processed data. Finally, there is a storage where the processed data are saved.

The advantage of this solution is the already mentioned simplicity of use. The user does not have to care about the infrastructure nor the application. The user only uses the services in accordance with the SaaS model. In contrast, there are all disadvantages of public Clouds. The most important is undoubtedly the safety. Others are limited data control, impossibility to intervene in the form of application, etc.

Private Cloud for Gathered Data Processing
In case of running a Cloud application, we can think about the usual architecture Software as a Service as mentioned above, or about the possibilities of a private Cloud.

Considering the magnitude of the whole solution, it can be spoken about private Cloud only in connection with the organization that operates this service for their clients. If it was a case of one user of this application who runs server application at home for own purposes, we could not be talking about a Cloud solution. In contrast to that, we can imagine a situation where a nursing home with 500 clients runs this service as a private Cloud. Here, a necessary separation of the hardware infrastructure from the very service is put to work. IT staff takes care of the Cloud and the service is consequently used by care assistants and clients.

In case of the private Cloud the risks of security stay but the operator has an absolute control over the data and the form of the application (Open-source solution is expected) with all its positive and negative results (care of the Cloud, data backup, the risk of data mishandling).

Server Run for Independent User
In the case of the situation described above, where one user wants to operate the service only for own use, we cannot talk about Cloud solution but this form of operation is naturally also possible. However, there is a range of limitations and complications that make this solution, in our opinion, the least recommendable. Mobile application itself can evaluate some basic occurrences but primarily it is designed for constant communication with the server. Therefore, it is necessary to arrange either a constant

access to the server through Wi-Fi or make the server accessible from the Internet. For domestic use, there are difficulties arising with public addresses, possible use of dynamic DNS records, and also the server security when we cannot assume that an ordinary user will be at the same time a specialist in the server security area.

5 Conclusions

The aim of the paper was to present the security aspects of the utilization of Cloud computing approach in mobile applications in health care environment. Personal data has to be secured thoroughly. The developed mobile application collects data by using the internal sensors of a smart phone. Data are partly evaluated in the device to evaluate critical situation and sent to the server for the deeper analysis. There are more layers utilized for better security of solution. The application is using AAA security model, the server authenticates IMEI of the device and encrypting using SSL 3.0 as well. Data are also encrypted on the application level by the symmetric encryption by means of the AES protocol with the key length of 256-bit.

Three possible cloud computing solution of the developed application has been analysed: Public Cloud run as service, Private Cloud for gathered data processing and Server run for independent user. On the basis of the presented analysis of Cloud computing security issues and mobile health care application, it can be conclude, that this approach brings many assets and challenges at the same time. These problems can be solved by the proposed solution.

Acknowledgment. This work was supported by the project of specific research no. 2101 and 2103. Faculty of Informatics and Management, University of Hradec Kralove.

References

1. Hřebíček, J. a kol.: Scientific computing in mathematical biology, MU (2012). http://www.iba.muni.cz/res/file/ucebnice/hrebicek-vedecke-vypocty.pdf
2. Bureš, V., Otčenášková, T., Čech, P., Antoš, K.: A Proposal for a Computer-Based Framework of Support for Public Health in the Management of Biological Incidents: the Czech Republic Experience. Perspectives in Public Health **132**(6), 292–298 (2012). doi:10.1177/1757913912444260. ISSN: 1757-9139
3. Allan, R.: Cloud and Web 2.0 resources for supporting research (2012). http://tyne.dl.ac.uk/NWGrid/Clouds/
4. Bureš, V., Brunet-Thornton, R.: Knowledge management: the czech situation, possible solutions and the necessity for further research. In: Proceedings of the 6th International Conference on Intellectual Capital and Knowledge Management, McGill University, Montréal, Canada, pp. 95–102 (2009). ISBN: 978-1-906638-45-0
5. Chirag, M., Dhiren, P., Bhavesh, B., Avi, P., Muttukrishnan, R.: A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing **63**(2), 561–592 (2013). doi:10.1007/s11227-012-0831-5. ISSN: 0920-8542
6. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications **34**(1), 1–11 (2011). http://dx.doi.org/10.1016/j.jnca.2010.07.006. ISSN: 1084-8045

7. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications **4**(5) (2013). doi: 10.1186/1869-0238-4-5. ISSN: 1867-4828
8. Fernandes Diogo, A.B., Soares Liliana, F.B., Gomes João, V., Freire Mário, M., Inácio Pedro, R.M.: Security issues in cloud environments: a survey. International Journal of Information Security (2013). doi: 10.1007/s10207-013-0208-7. ISSN: 1615-5262
9. Lee, H., Kim, J., Lee, Y., Won, D.: Security issues and threats according to the attribute of cloud computing. In: Kim, T., Stoica, A., Fang, W., Vasilakos, T., Villalba, J.G., Arnett, K.P., Khan, M.K., Kang, B.-H. (eds.) SecTech, CA, CES3 2012. CCIS, vol. 339, pp. 101–108. Springer, Heidelberg (2012). doi:10.1007/978-3-642-35264-5_14. ISSN: 978-3-642-35264-5
10. Weihua, J., Shibing, S.: Research on the security issues of cloud computing. In: Du, Z. (ed.) Intelligence Computation and Evolutionary Computation. AISC, vol. 180, pp. 845–848. Springer, Heidelberg (2013). doi:10.1007/978-3-642-31656-2_115. ISSN: 2194-5357
11. Mouratidis, H., Islam, S., Kalloniatis, Ch., Gritzalis, S.: A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software **86**(9), 2276–2293 (2013). http://dx.doi.org/10.1016/j.jss.2013.03.011. ISSN: 0164-1212
12. Sujithra, M., Padmavathi, G.: Mobile device security: A survey on mobile device threats, vulnerabilities and their defensive mechanism. International Journal of Computer Applications **56**(14) (2012). doi:http://dx.doi.org/10.5120/8960-3163. ISSN: 09758887
13. Cagalaban, G., Kim, S., Kim, M.: A mobile device-based virtualization technique for M2M communication in cloud computing security. In: Kim, T., et al. (eds.) SecTech, CA, CES3 2012. CCIS, vol. 339, pp. 160–167. Springer, Heidelberg (2012). doi:10.1007/978-3-642-35264-5_23. ISSN: 18650929
14. Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G.J., Bertino, E.: Collaboration in Multicloud Computing Environments: Framework and Security Issues. Computer **46**(2), 76–84 (2013). ISSN: 0018-9162, WOS:000314943300019
15. Popa, D., Boudaoud, K., Borda, M.: Secure mobile-cloud framework - implementation on the mobile device. Acta Technica Napocensis **54**(4), 7–12 (2013). ISSN: 12216542
16. Wood, J., Aboba, B.: RFC 3539 - Authentication, Authorization and Accounting (AAA) Transport Profile (2003). http://tools.ietf.org/html/rfc3539
17. Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G.J., Bertino, E.: Collaboration in Multicloud Computing Environments: Framework and Security Issues. Computer **46**(2), 76–84 (2013). ISSN: 0018-9162, WOS:000314943300019
18. Gejibo, S., Mancini, F., Mughal, K.A., Valvik, R., Klungsøyr, J.: Challenges in implementing an end-to-end secure protocol for Java ME-based mobile data collection in low-budget settings. In: Barthe, G., Livshits, B., Scandariato, R. (eds.) ESSoS 2012. LNCS, vol. 7159, pp. 38–45. Springer, Heidelberg (2012)
19. European Union Agency for Network and Information Security. Cloud Computing Risk Assessment — ENISA (2009). http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
20. Brodkin, J.: Gartner: Seven cloud-computing security risks. Infoworld, 1–3 (2008)
21. Suba, P., Tucnik, P.: Mobile monitoring system for elder people healthcare and AAL. In: Conference on Intelligent Environments, vol. 17, pp. 403–414 (2013). doi:10.3233/978-1-61499-286-8-403