Analysis of Security Threats of Cloud Computing

Tomas Svoboda, Simeon Karamazov
University of Pardubice, Faculty of Electrical Engineering and Informatics,
Pardubice, Czech Republic.
tomas.svoboda5@student.upce.cz

***Abstract*—The aim of this paper is to introduce the result of a long-term research done in the Czech Republic and focused on the security of cloud services. The results of the research reflect more than eighty representatives of national and supranational organizations in the environment of the Czech Republic, and also state organizations within self-government territorial units. The paper examined cloud deployment issues connected with the current legislative and law on cybernetic security. The results of the research are summarized in a SWOT analysis.**

***Index Terms*—Cloud Computing; Research Cloud; Corporate Environment; Cloud Security.**

I. INTRODUCTION

First proposal of cloud computing was originating in 1960. Pronounced development of this technology was seen between the years 2007 and 2008. In these years the term cloud was first put into use [1]. There are many advantages which cloud brings to organizations and cloud owner. Organizations can pay only for services that they really need. Owner of cloud have a possibility to maximally utilize computer resources to minimize costs for maintenance [2].An important chapter is the security of the services provided by a provider. Confidentiality, integrity, and availability are three key featured the provider should be able to offer their customers [3].

One of the big security threat is the unavailability of data to legitimate users. But also breach of privacy is a big problem [4]. Data in a cloud can be divided into public data, for which minimal security is required, and private data, which contains highly confidential information that require an appropriate level of security. Provider is fully responsible for cloud security. If the users stored their data into cloud, they trust to provider. They usually don't have any information about implemented security measures. Users also don't have any information about abide by the agreed SLAs. [5]. In the same way, customers have no way of knowing where the servers are physically located, on which server their data are stored, or what law regulations apply to them [6]. According to that, customers must believe that providers are trustworthy and their data are protected against outside attacks, not from the inside attacks. [10]. To eliminate the possibility of an inside attack, the basic security measure is data encryption, during which the encryption key is with the customer and the provider is not able to decrypt the data without the key [7].

Nowadays, there are an increasing number of mobile devices that use cloud. On the other hand, these devices have limited resources, such as capacity of storage. This problem is solved by mobile cloud computing (MCC). MCC is applicable in various areas, such as entertainment, health, transportation etc. [10-16] Main problem is the security of a mobile device and user data in a mobile cloud. Mobile devices possess data and file security in the form of password protection, but these passwords can be viewed by other users as well. When the device is stolen, the thief can gain access to the target data rather easily [17]. A good choice is securing data through encrypting algorithms, thanks to which the data are transmitted and saved into the cloud in an encrypted form [18].

II. CLOUD COMPUTING AND SECURITY

A. Cloud Models

Cloud security is primarily dependent on what version of a cloud the organization uses. In our research we proceeded from the approach of Mell and Grance, who defined four basic models [1]. Public cloud is defined as a cloud, where the services are provided to a huge number of customers. The provider is responsible for availability of the provided services. The advantage of it is a low price for services. The disadvantage is a limited option of customizing the service according to customer needs, which comes from the idea of providing services to as many customers as possible, as with a public cloud. The issue of security is closely linked with a public cloud, as it is important to ensure that every customer has access inly to their own data and at the same to restrict access to data of other users.

A public cloud most often uses the mechanism of authentication, authorization, and accounting to authenticate the user. Private cloud differs from a public one mostly by being used only for needs of an organization within an inside network (intranet). That being said, it is necessary for an organization to have a whole infrastructure at their disposal. The provider is then most commonly the IT department of the organization, or it is provided via outsourcing. The advantage is knowledge of the infrastructure and data security is fully in the hands of organization, in which the data are located. While using a private cloud, it is not necessary to solve the problem of various customers accessing (organizations) the infrastructure, just like with the private cloud.

Community cloud is a specific example of a public cloud. The infrastructure is shared among several organizations that use it a thus create a community. It can be own directly by the organizations in the community or by a third party. These organizations can be linked by, for example, field of operation or similar requirements for cloud services. Community cloud can be used mostly in the area of state administration. Hybrid cloud is a combination of a private and a public cloud and a part of the infrastructures, for security reasons, is operated within the organization and other part of it is rented from a third party. The organization can have a part of their data under control and part outside.

Connected clouds then remain unique entities, which are interconnected using standardized application interfaces or proprietary technologies that enable data and application transferability.

B. Cloud Security

Many expert books and articles deal with cloud computing security. The most relevant document about cloud computing security is the one by Cloud Security Alliance (CSA) [9]. Founded in 2008, CSA's main aim is to support proven security techniques within cloud computing and to provide information about cloud computing as such. CSA defines nine security risks for clouds. Data breaches are the biggest threat to an organization's competitiveness. The risk of data abuse by the organization's competitors for their advantage was an issue even before cloud computing technology came along. But with its development, new possible ways to attack service providers came and the risk of data theft and their abuse rose.

Data can get lost as a result of data cracker attacks, natural disasters, but also technical difficulties of the provider. Such risk is called data loss. Both the provider and the customer are responsible for data loss in all cases. If the costumer uses an encryption key which gets lost, there is no possibility to recover the lost data. Account or service traffic hijacking is a type of an attack, which has been known for a long time, thus it is not considered a new threat. Its aim is to steal access data for a user account, thanks to which the attacker can manipulate user´s data and use his account for his own benefit. Availability and security of services is dependent on the security of basic API which ensure authentication, authorization, monitoring, etc. In case a security error in API occurs, it is impossible to ensure safe run of the service as a unit.

Denial of service attack is denying access to a service or at least slow it down as much as possible. This attack is most commonly done via consuming all available system tools (CPU performance, hard drive capacity, RAM capacity, etc.). Concerning cloud computing, the aim of the attacker is to prevent users from getting to their data and applications. The scenario, in which the application is unavailable, but it consumes more sources, leads to the customer ending up paying for the service, although they have not been using it. Malicious insiders represent an abuse of a user account.

Provider's administrator poses a huge security threat as they can have access to target information. To prevent such malicious activities, it is advisable to use an encryption key. Such key must be stored by the customer outside the cloud of the provider.

Another security risk is abuse of cloud services. Big computing performance of a cloud can be misused for hacking passwords or encryption keys. Insufficient due diligence is a threat concerning the ignorance of a cloud. When cloud was introduced, many organizations tried to implement this technology as fast as possible. The main reasons were the vision of lower infrastructure costs, scalability, instant access, etc. But many organizations did not understand the mechanisms of cloud technology, including the reactions of the provider to errors in case of a malfunctions, use of encryption, or user activity monitoring. Shared technology vulnerabilities concern components of the infrastructure (such as the CPU, etc.) that have not been designed to ensure 100% user isolation when being accessed. Thank to this vulnerability, the entire cloud platform can be in jeopardy.

Another important view of the issue is presented by Gartner Inc., an organization that defined seven security risks for clouds. [8]. With privileged user access, data are stored on cloud service provider's servers. The customer should learn as much as they can about the server, the persons with access to it and data stored on it, and how access to the server will be monitored.

For cloud service providers, regulatory compliance means conducting external audits that investigate how providers secure the data entrusted to them. If the provider is not willing to participate in said audits or they don't present data from audits upon request, they lose credibility in their customers' eyes. Physical data location may be hidden to the customer. In this context, Gartner advises that the customer makes sure whether the provider upholds personal data protection appropriate for the particular country, in which their data center is located. Customers' data are located in the cloud together. The cloud provider then should use appropriate encryption mechanism to separate the data of individual customers. Such procedure is called data segregation. At the same time, the provider should also be able to provide information about how and by whom the encryption mechanisms were designed. If encryption fails, the worst consequence can be data unusability and therefore only professionals in the field should design and test encryption solutions. The customer should also ask for information about if and when data recovery is possible in case of a malfunction. The provider should regularly back up customers' data to ensure that the possibility of recovery is always present.

Investigative support in cloud computing can mean the impossibility of investigating illegal activities. According the Gartner's advice, the customers should request investigative support along with a proof that the provider has experience with such support. Long-term viability means that if the provider faces financial difficulties, or the organization is acquired by another organization, it should not affect availability of customers' data in any way. The customer should ask the provider how to acquire their data back in a format that would enable their import into replacement application, should such scenario occur.

III. Research And Its Results

The research was conducted in Czech Republic from February till November 2014. The research was divided into two parts. In the first part we realized a personal meeting with persons, who were responsible for IT in the organizations. The reason for this was to determine their objective response for the next part of research. In the second part, the questionnaire survey was realized in organizations. Standardized questionnaire was used as a research method. The questionnaire survey is one of the quantitative research methods. Advantages of the questionnaire research are the low time and financial demands. Research may be conducted with a small number of researchers, but still allows acquisition of data and the large number of people. For respondents it is important in a relatively high degree of anonymity and time consuming.

The results are highly representative for the rest of the population (or specific group). Results can be also statistically processed. In addition, the questionnaire can be

used repeatedly for comparative investigation. The responses from the questionnaires can be quantified and analyzed. Standardized questionnaire has a fixed structure. There were total of 30 closed questions in the questionnaire. In this question the respondent could have selected an already given answer or select the option 'other answer' and provide their opinion. The questionnaire was grouped into logical groups that contained questions concerning similar issues. There were three groups of questions. The first one contains questions about information of the organization. The second one contained questions about utilizing or not utilizing cloud services and also about deploying cloud services. The third one was focused at the threats of security of cloud services. Individual questions were then made available to the respondent in blocks based on their first response. So, if the respondent was already using cloud services, there logically were no questions why they would not use them. The results of the questionnaire research are then compared with a created SWOT analysis. In the next part of the article, results of selected parts of the research are introduced.

IV. Evaluation And Results of Gained Data

The first interesting result, gained during a research, was the discovery that 53% of organizations approached about co-operation on our research actually participated. In our research, we gained information from 87 organizations in a questionnaire research, results of which are presented below. Out of the 87 organizations, 73% of them utilize cloud services. The rest of organizations do not utilize cloud services. This value is relatively high, which can be cause by the fact that they have not implemented cloud solutions. After adding the number of organizations that refused to take part in our research and for which we assume that they do not utilize cloud services, the total percentage of organizations in the research, who use cloud services, is 35%. Although, the structure of individual organizations is far more interesting to the research itself.

A. Structure of Participating Organizations

Following results, depicted on Figure 1 represents the percentage of organizations utilizing cloud services. Interesting fact is that 40% of organizations which operating in the field of IT use cloud services in their operation. 33% of power engineering - production and management organizations using cloud services. It is actually a rather surprising result. It can be awarded to development new technologies including smart networks and smart metering, which is supported in the Czech Republic not only by organization managements, but also by state grant policy. Last result is a small portion of 14% of industrial organizations, operating in the field of machine industry, construction and glass production, that utilize cloud services, can be awarded to relatively high price for innovation of current infrastructures.

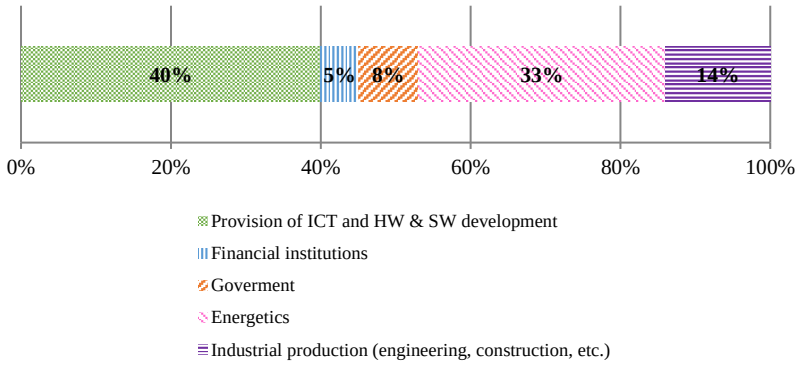

Figure 1: The structure of the organizations using cloud computing (Source: authors)

B. Type of Deployed Cloud Solution Depending on the Type of the Organization

Based on the obtained data from the research, there are not present all of possible deployed cloud solutions. Figure 2 depicts those results. The first interesting result is that organizations utilizing three types of cloud - the hosted private cloud, hybrid cloud and custom private cloud. In the sphere of government only the custom private cloud is being used, because another solution is more or less impossible for legislative reasons, especially because of the emphasis on security requirements of sensitive data.

Based on the next result, the organizations are aware of their data. For that reason they using only hosted private, hybrid or custom private cloud solutions. None of organizations use public cloud solution. Security requirements of organization data, that is stored into cloud is the key factors that affected the deployment of cloud services. These three utilized types of cloud provides an option to provide data security in compliance with requirements set by the law on cyber security and last but not least, in compliance with internal documents of the organization, the usage of which is defined by internal documents of organizations in compliance with ISO 27000.

C. Reasons Affecting the Deployment of Cloud Solutions

Figure 3 depicts the reasons affecting organizations that not using cloud services yet, but deem it necessary to implement them. The first reason, that affecting the deployment of cloud solutions is an independent inspection of cloud providers by an external audit. According to results of the research, this is not very important factor for organizations. This point of view, that logically only applies to public and hybrid cloud services, is a determining factor only for 25% of subjects.

Second aspect that can be considered rather restricting for not utilizing cloud services is the unavailability of high-speed connectivity for organizations. Its rise is a key element for 50% of participating organizations. This issue is significant mostly for organizations that provide cloud services and also a connectivity to the cloud, as there is a

huge number of such organizations in the Czech Republic and they should take that fact into account when offering their services to end users. For 50% of organization it is important to know about handling their data, data security and physical location of the data. Based on this, organizations incline to implementing a hybrid cloud or private cloud solutions exactly for the security and data control reasons.

The most significant aspect, from the viewpoint of organizations, is not complex or overcomplicated legislative scope that defines cooperation between the customer and the provider. There were no significant changes to the development of risks affecting potential customers switching to cloud services, which can be seen on the comparison of a conducted investigation of risks defined by Gartner. The investigation points mainly to the large risk lying in data security, which was actually mentioned by 50% of respondents. In compliance with the previous discovery of overcomplicated legislative scope regarding the legal responsibility of the provider and the customer, it is also possible to find a correspondence with the Gartner agency, which deems legal obstacles a significant risk as well.

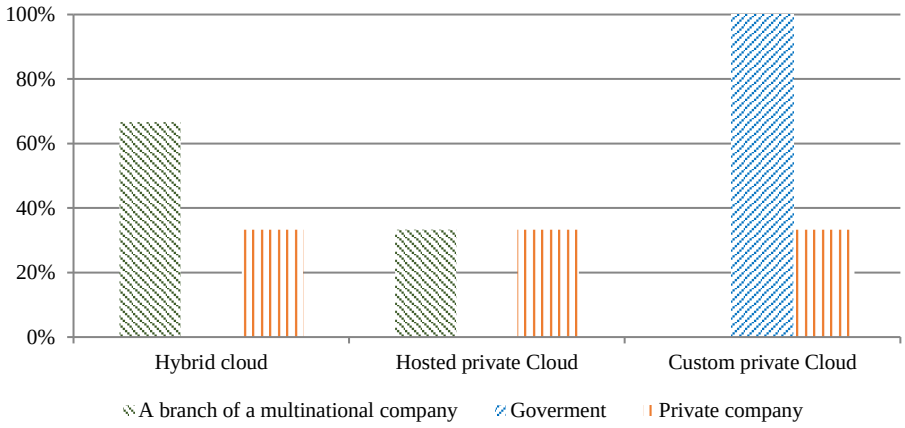

Figure 2: Analysis of the reasons affecting the use of cloud services

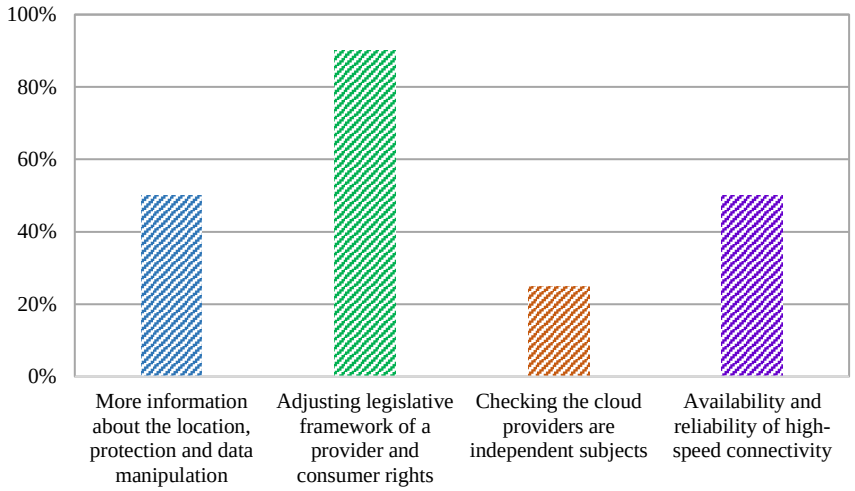

Figure 3: Analysis of the reasons affecting the use of cloud services

D. Type of Security Depending on the Type of the Organization

Result presented last regard used options of security while using cloud services. Figure 4 depicts said results. As expected, the demand for security is highest in the sphere of government organizations, 80% on average. Of course, private organizations and subsidiaries of supranational companies are not falling behind with the average of 62%. The most feared scenario is data interception during their transfer into a cloud and their subsequent misuse. Simple, yet efficient solution is to secure the data transfer by an encryption key. Based on the results of the conducted research, organizations are very well aware of the problem and on average 67% of them use encryption. Furthermore, all government organizations also monitor user activities. It is actually rather logical, as handling sensitive data requires the highest level of security and monitoring of user activities can then serve as binding materials for audits. When monitoring users, there logically is the need to distinguish which user is being monitored. Using user accounts and user roles are used in such a case, as each user role had different access rights. Each user can only perform operations assigned to his user role. 92% of private companies and 75% of government organizations and subsidiaries of supranational companies acknowledged user monitoring, which leads to the assumption that not only government, but also private companies do not underestimate their data privacy in terms of their transfer into a cloud and subsequent data handling.

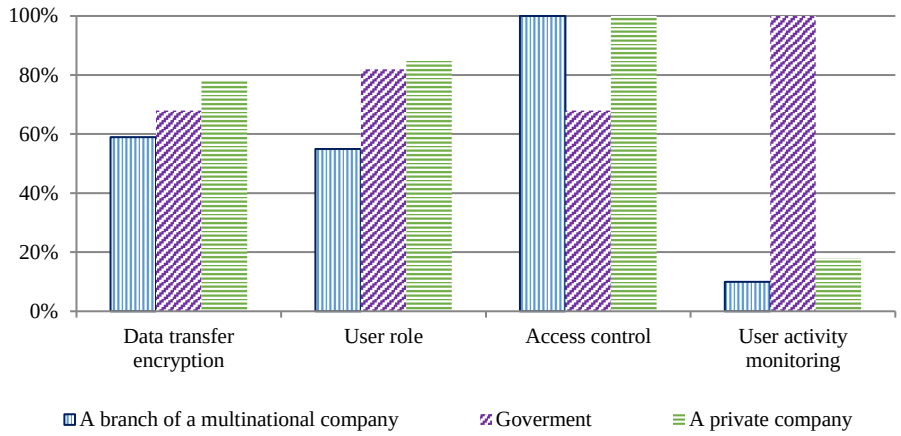

Figure 4: Used security options depending on the type organization structure of the organizations

V. CONCLUSION

The paper described results of the first conducted research of cloud security in the Czech Republic. Just like any other technology, cloud computing brought along many advantages and disadvantages. The results can be summarized by a SWOT analysis that corresponds with complex results of the realized research. Cloud computing brings many benefits e.g. infrastructure part of network is ensured by a provider. Customers also do not need to buy additional servers, computers and other equipment. Next benefit is the form of payment for services or the infrastructure in the form of subscription and the provider can estimate their future profits based on previous payments. Availability can be deemed a weak side, as providers' servers with customers' data are often located all over the world. If the customers want to have access to their data, the data should be provided in reasonable time. For providers, this can present a potential problem. Even Internet connection can be considered a huge disadvantage, as shown in the analysis of results of the research. The pressure to unify and adjust legislature, which would contribute to more frequent usage of cloud, can be seen as an opportunity confirmed by the research results. In the Czech Republic, law on cybernetic security, which solves the issue of ambiguous legislature and which dictates the way, how to store and secure data, took effect on January 1st, 2015.

It is necessary to also mention the treats, which includes data security, but more importantly the risk of their abuse by a third party. Potentially, customer data can be lost if the provider terminates the provision of provided services. The respondents also mentioned this issue in our research. This issue was considered by the participating organizations. Nowadays, cloud computing is used by many organizations and companies all around the world and also in the Czech Republic. There are many different types of organizations, that using cloud services. According to their opinion, cloud brings many advantages and on the other hand also many disadvantages. Organizations are conscious of both of these cloud features. Rising trend of using cloud services in Czech Republic is observed. Improving the availability of fast-connection for end users and better legislative scope can be deemed as the key factors of better utilizing cloud computing in the Czech Republic.

ACKNOWLEDGMENT

This work and contribution is supported by the project of the student grant competition of the University of Pardubice, Faculty of Electrical Engineering and Informatics, Intelligent Smart Grid networks protection system, using software-defined networks, no. SGS_2016_016.

REFERENCES

[1] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology (NIST)", September 2011, Available at: http://goo.gl/3nGfE0

[2] J. Winkler, "Securing the cloud: cloud computer security techniques and tactics",in *Syngress/Elsevier*, pp. 290, 2011, ISBN 978-159-7495-929

[3] L. M. Kaufman, "Data security in the world of cloud computing", in*IEEE Security and Privacy*, vol. 7, pp. 61-64. doi:10.1109/MSP.2009.87

[4] B. Halpert, "Auditing cloud computing: a security and privacy guide", in*John Wiley*, pp. 206, 2011, ISBN 978-047-0874-745

[5] M. Hussain, and H. M. Abdulsalam, "Software quality in the clouds: a cloud-based solution", in*Cluster Computing*, vol. 17, iss. 2, pp. 389-402, 2014. doi: 10.1007/s10586-012-0233-8

[6] Anthony T. Velte, Toby J. Velte and Robert C. Elsenpeter. "Cloud Computing: praktický průvodce", in*Computer Press*, pp. 344, 2011, ISBN 978-80-251-3333-0

[7] M.I. Salam, W.-C. YAU, J.-J. Chin, S.-H. Heng, H.-C. Ling, R.C.-W. Phan, G.S. Pog, S.-Y. Tan, W.-S Yap, "Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage", in*Human-centric Computing and Information Sciences*, vol. 5, no. 19, pp. 16.

[8] J. Brodkin, Gartner: "Seven cloud-computing security risks", Available at: www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[9] Cloud security alliance, "Cloud Computing Top Threats in 2013: The Notorious Nine", 2013, Available at : https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[10] H. Lin, L. Xu, Y. Mu, W. Wu, "A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing", in*Future Generation Computer Systems*, vol. 52, pp. 125-136, ISSN 0167-739X, Available at: http://dx.doi.org/10.1016/j.future.2014.10.032.

[11] R. Cimler, J. Matyska, L. Balik, J. Horalek, V. Sobeslav, "Security Issues of Mobile Application Using Cloud Computing", In: *Advances in Intelligent Systems and Computing*, pp. 347-357, 2014. doi: 10.1007/978-3-319-13572-4_29

[12] J. Horalek, V. Sobeslav, "Intelligent Car Localization with the Use of Andruino Platform and Cloud Storage", In: *Lecture Notes in Electrical Engineering*, pp. 795-805, 2015. doi: 10.1007/978-3-319-24584-3_67

[13] M. Penhaker, O. Krejcar, V. Kasik, V. Snasel, "Cloud Computing Environments for Biomedical Data Services", In:*Intelligent Data Engineering and Automated Learning*, LNCS vol. 7435. pp. 336-343, 2012, doi: 10.1007/978-3-642-32639-4_41

[14] V. Sobeslav, P. Maresova, O. Krejcar, TC. Franca, K. Kuca, "Use of Cloud computing in Biomedicine". In: *Journal of Biomolecular Structure and Dynamics*, pp. 1-10, 2016. ISSN 0739-1102

[15] J. Machaj, P. Brida, "Wireless Positioning as a Cloud Based Service", In: *ACIIDS*, pp. 430-439, 2015, Springer LNAI9012, doi: 10.1007/978-3-319-15705-4

[16] R. Cimler, J. Matyska, L. Balik, J. Horalek, V. Sobeslav, "Security Aspects of Cloud Based Mobile Health Care Application" In: *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 202,doi: 10.1007/978-3-319-15392-6_20

[17] M. Sujithra, G. Padmavathi, Sathya Narayanan, "Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud", In*Procedia Computer Science*, vol. 47, pp. 480-485, ISSN 1877-0509, Available at: http://dx.doi.org/10.1016/j.procs.2015.03.232.

[18] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", In:*Procedia Computer Science*, Volume 48, Pages 204-209, 2015, ISSN 1877-0509, Available at: http://dx.doi.org/10.1016/j.procs.2015.04.171.