Rasid G.Alakbarov, Ogtay R. Alakbarov
Institute of Information Technology of ANAS, Baku, Azerbaijan
rashid@iit.ab.az, oqtayalakbarov@yahoo.com

DOI: 10.25045/jpit.v09.i1.09

SECURITY AND PRIVACY ISSUES IN MOBILE CLOUD COMPUTING

This article investigates security and privacy issues on cloud platforms used in mobile cloud computing. Threats arisen from users' data protection and network security in mobile cloud computing are analyzed. At the same time, the article analyzes information security in mobile cloud computing, confidentiality, location and displacement of data, completeness of data, cyber attacks. Scientific-theoretical problems of security and privacy issues of mobile cloud computing are investigated and the status of researches in this direction is analyzed.

Keywords: *mobile computing cloud, mobile equipment, information security, confidentiality, cyber attacks, computing and memory resources, computing clouds, virtual machine, cloud services.*

Introduction

At present, intensive research is being carried out to effectively utilize the computing and memory resources of data processing centers with the use of *Cloud Computing* technology throughout the world. The systems with large computing and memory resources are built based on computer networks with high-speed connection channel. The emergence of new cloud services and the development of mobile applications for mobile devices has recently led to the creation of mobile computing systems based on these technologies. At present, mobile users are widely benefitting from Cloud Computing technologies. The rapid growth of mobile devices (laptops, tablets, smartphones, etc.) in the world and their integration to cloud computing over the Internet through appropriate telecommunication technologies (GPS, 3G, 4G, Wi-Fi, etc.) has led to the development of a new technology - *mobile cloud computing*. Obviously, the capabilities of any mobile device (computing and memory resources) are limited. Nevertheless, mobile users use these devices to solve issues requiring great computing and memory resources. In this regard, cloud computing technologies are widely used. Thus, the problem of restricted computing and memory resources available on mobile devices can be eliminated with the use of cloud technologies. In recent years, the fall in prices of cloud services has enabled mobile users to benefit from these services.

Storage and use of large-scale data of users and organizations in cloud attracts hackers and create privacy problems for mobile users [1, 2]. In this regard, the threats to the security of mobile devices and the risks of mobile cloud computing have been studied and recommendations have been given. The main goal of a mobile computing environment is to provide mobile users with software applications and services through cloud service providers over the Internet. Thus, to ensure the access of users of mobile cloud computing to the applications on cloud servers, it is important to analyze problems occurring in different parts of the network, that is in mobile devices, network, mobile applications and their security.

This article thoroughly explores the problem of data security and confidentiality of personal data emerged from the use of mobile cloud computing.

Security issues on mobile cloud computing platforms and mobile devices

In cloud technology, software applications and data are located and stored on cloud servers of the Internet rather than the individual mobile devices, and presented to the users on demand. Since mobile cloud computing implements the data and software that require great computing and memory resources, mobile devices do not need to have powerful technical capabilities.

Mobile cloud computing is a new network concept that utilizes computing services of mobile devices.

Traditional security issues of the clouds computing still remain. However, traditional security mechanisms cannot provide confidentiality of application data in the cloud due to the expansions of the capabilities and boundaries of the use of cloud services of the enterprises. Public cloud and features of numerous services have a great impact on the information security of mobile cloud computing [3, 4]:

- Application used on cloud platforms and the data stored on them do not have stable infrastructure and security boundaries. This complicates the isolation of the physical resources subjected to attacks;
- Cloud platforms offering cloud services to users and organizations may be owned or operated by multiple providers. Taking into account the diversity of interests, it complicates the application of unique security measures to the solution of the conflicted issue in cloud;
- Public cloud and the use of virtual cloud resources by multiple users enable unauthorized users to access the user data;
- Cloud computing platforms provide the storage of a variety of data and fast access to these data, and therefore, cloud security measures should also provide the processing needs of data.

Security problems caused by the presentation models of SPI (SaaS, PaaS, IaaS) services, deployment models and key cloud features affect all aspects of the infrastructure, including network level, host level, and application level. Security problems occurred on cloud platforms are reviewed below.

Problems occurred on IaaS platform. Cloud technologies use cloud-based virtual machines (VMs) to provide users with computing resources. Therefore, VM's security is one of the key issues. The goal is to protect the VM operating systems and software applications from malware and viruses that affect the physical servers using common security solutions. Cloud consumers are responsible for VM's security. Each cloud consumer (user) must be capable to identify and eliminate the predicted risk by using his/her security control mechanisms [5, 6]:

- *Image repository*. Unlike physical servers, VMs are at risk even when they are in offline mode. Image repository can be damaged by infringing the files located on VM through malicious code. Moreover, the data stored there can also be stolen. Cloud providers reliably protect the image repository. Another problem related to the VM templates is that the initial data of the users can be stored in the templates, and a new user may violate privacy issues when using these copies;
- *Virtual network security*: Shared deployment of different servers located on the same network infrastructure by the renters increases the probability of intrusion into physical servers and DNS servers;
- *VM Boundary Security*: Compared to physical servers, VM has virtual boundaries. VMs built on a physical server use the same processor, memory, input-output, and network adapter (there is no physical isolation between VM resources). Cloud providers are responsible for ensuring the VM boundaries.

Security issues on the PaaS platform: PaaS service offers the interface, security function, application interface (AI), which controls the applications. The proposed AI should be equipped with security mechanisms that provide identification (authenticity) and authorization [6].

Security issues on the SaaS platform: Security of SaaS model is provided through the joint efforts of cloud service providers and software providers. This model combines data and network security management with the security issues discussed in the previous two models [7].

Web-application sustainability Browsing (Scanning): Security of web-applications to be placed on the cloud infrastructure should be verified by web-application scanners [8]. Firewalls designed for web-applications should be detect existing gaps.

These threats aim at getting (stealing) the personal information (e.g., credit card numbers, passwords, contacts, locations) of the users or the resources of their mobile devices.

Guaranteed protection of data of the mobile cloud users from others and network security are the key issues.

Security of mobile users. Mobile devices face various security threats (malicious software codes, virus programs, etc.). For example, when using software applications for GPS (*Global Positioning System*), problems with data privacy protection arise. Therefore, it is recommended to install security software that identifies the threats for mobile devices. Malware that threatens the security of various mobile devices used in the network affects the privacy of the mobile users. Two major security issues of mobile users exist: mobile application security and privacy (confidentiality). The most common way to check security issues is to install and deploy security software and antivirus on mobile devices. Since mobile devices have limited resources, their protection against threats is more difficult than of personal computers. Several methods are used to identify the threats and transmit security mechanisms to the cloud. Mobile users should undergo a series of risk assessment procedures before using software applications. All commands implemented through the software applications on mobile devices should be checked for malicious software. In addition, mobile devices also control the implementation of antivirus programs on cloud security servers [9]. In this regard, security and privacy issues in mobile cloud computing should be reviewed. Since most mobile devices are unprotected or poorly protected, the risk of data loss and theft is great. Unauthorized user can easily access mobile devices and get the data.

The threats affecting the security of mobile devices are as follows [4-10]:

- Data loss on lost or stolen mobile devices;
- Data theft through malicious mobile software;
- Data leakage through the vulnerabilities of the software application;
- Vulnerabilities within the devices and operating systems;
- Secure network access and unauthorized access points;
- The presence of malicious cloud-based software applications;
- The lack of reliable management capabilities of software application interfaces.

During wireless communication, malefactors (hackers) can attack data. Accessing data from multiple access points may cause the overload of the connection channel. This can block data usage for certain services. To prevent the data loss on mobile devices, malware should be monitored and antivirus software should be used to eliminate them. This software controls the malware. Malicious code (applications) is not just virus programs. Malicious applications include phishing programs and spamming occurring in malicious social networks, and the applications used for personal data theft. A secure communication channel is built using wireless protocol encryption to prevent malefactors' access to the network. Security and privacy have always been a major issue in data sharing between mobile devices and cloud.

Data security on mobile cloud computing servers is another issue. On cloud servers, users do not control the data and are unaware on which servers the data are located on the cloud. In such cases, the data loss can be caused when the physical data carriers are damaged or deleted by certain individuals.

Security and privacy issues in mobile cloud computing

In this section of the article, data security issues in mobile cloud are reviewed. Whilst placing customer data in cloud, data access should be limited only to the authorized users. Unauthorized access to the personal data of the customer by the staff of cloud service providers is one of the potential threats to cloud data. Additionally, providers should train customers to provide security of cloud data. They should be provided with confidentiality policies and procedures. Security of all user data stored in cloud must be ensured.

Security issues in mobile cloud computing include:

• *Data security*. Security is of great importance since mobile clouds are primarily associated with data storage and processing. At present, various cloud platforms offer built-in security measures. SSL (*Secure Sockets Layer*) is a cryptographic protocol that provides secure connection channel between the mobile user and cloud server [11]. As far as information security is concerned, the companies should introduce security policies and procedures for data and operations. Providers may also provide company training, education and guidance on OPSEC (*Open Platform for Secure Enterprise Connectivity*) to ensure full implementation of the policies and procedures. The policies related to access control, authentication procedures, user management, encryption, content delivery, and overall communication security should be developed and the measures should be taken for their acceptability [12]. Providers should ensure the users about the provision of security and privacy of user data and applications. This enables a user confidence in the mobile platform of the manufacturer offering cloud services. Cleaning the lost or stolen devices remotely can prevent the abuse of data on mobile devices. Most mobile manufacturers and mobile users generally provide this feature [13]. Mobile devices (cellular phones, PDAs, smartphones, etc.) are vulnerable to a variety of threats such as malicious codes (e.g., viruses, worms, and Trojans). Running the *Global Positioning System (GPS)* can also cause security problems for mobile devices. The simplest way to reveal security problems for any mobile device is the installation and use of security software (Kaspersky, McAfee and AVG antivirus software). However, mobile devices have limited processing power and insufficient battery, therefore, their protection against the threat is much more difficult than other computer devices (e.g., personal computers). In this regard, threats detection capabilities can be transferred to cloud. This paradigm includes the installation and use of the existing Cloud AV platform, which provides detection service installed in cloud. It also enables the parallel use of several antivirus systems by storing them in virtualized containers. This approach facilitates the effective detection of the threats and reduces energy consumption by up to 30%. Although the storage of large volumes of information and applications has a number of advantages, the integrity of information and applications, authentication and user protection should also be considered [14].

• *Confidentiality and privacy*. Detection of the geographical location of a mobile user creates problems with their confidentiality and privacy (date of birth, credit card information, personal information, history of disease, etc.) of the user data. If mobile devices use GPS technology, this makes it much easier to define their physical location. Security of enterprise data can only be enhanced through the analysis and examination of certain cloud services. It should be guaranteed that the data access is limited to the authorized users after being placed on the cloud server. Unauthorized access to the user data by cloud personnel is a risk that can potentially endanger the cloud data. Customers should be guaranteed and appropriate policies should be applied. Moreover, confidentiality policies and procedures should ensure the safety of the users' data on cloud servers. The risk of confidentiality violation, including data theft and phishing can be reduced by taking a number of measures for data sharing among interconnected systems, implementing monitoring, adopting protocols and notifying the users about social media safety. Companies can address their legal and security challenges by developing a policy on social media and implementing a number of procedures to protect the infrastructure. Otherwise, their data infrastructure and reputation can be damaged [16]. The most effective way to maintain the data integrity and confidentiality is the encryption. Encryption protects data processing from external interventions, providing the storage and transmission of data [17]. GPS devices allow the mobile users to benefit from the Local Based Services (LBS). However, the SLA can cause a privacy problem when the mobile user shares his or her personal information using this system. To address this problem, the Trusted Location Servers (LTS) are used [18]. Digital Rights Management (DRM) provides solutions for other privacy problems. Non-structured digital content (e.g., video, photo, audio, e-book, etc.) is often shared with piracy and illegally. Phosphor, which is a cloud-based digital right management scheme for mobile phones with SIM card, is offered to prevent their piracy and illegal distribution [19]. It increases flexibility and eliminates security gaps at very low cost. However, since this approach is based primarily on the SIM card of mobile phones, it can not be used on the devices such as laptops that access those content via Wi-Fi [20].

• *Data integrity*. Providing data security, cloud service providers should implement certain mechanisms to maintain the data integrity by providing data security and describe where and in what conditions these data sets are. The cloud provider should notify the customers about the location of specific data in cloud, their origin and integrity mechanisms.

• *Placement and displacement of data*. Cloud offers high mobility of data. Consumers do not always know where their data is placed. Nevertheless, a user may require the location where his/her confidential information is stored on the storage device in the cloud. They may also indicate preferable locations (e.g., information stored in India). In this case, an agreement between a cloud provider and a consumer is required. According to this agreement, the data should be stored on a particular server and at a specific location. In addition, cloud providers are responsible for providing security of these systems (including their data) and protecting customer data. Another issue is the data displacement from one place to another. Data is initially stored in an appropriate place predefined by cloud providers. However, this information can be moved from one place to another in terms of security. Cloud providers can sign agreements and share each other's resources.

• *Cyber attacks*. All networks are exposed to one or more malicious attacks (hackers). The threats to data can be reduced by controlling the security of all Web 2.0 servers. In addition, the risk of unauthorized data access via social media and websites can be eliminated by separating Web 2.0 servers from other internal servers in the future [21]. Potential attacks may include:

✓ *DoS attacks (Denial of Service)*. Cloud servers are often exposed to DoS attacks, since multiple clients can simultaneously access clouds, which can make DoS attacks even more effective;

✓ *External attacks to channel*. Hackers develop malicious VM and each time place it close to the purchased cloud server. After a certain period of time the security of a cloud server becomes at risk, and then, the data transmission channel is attacked from the outside;

✓ *Authentication attacks.* The authentication problem of virtual services is considered one of the weakest vulnerabilities. A user may use a number of mechanisms and methods to protect the most targeted identification processes by attackers;

✓ *Man-in-the-middle Encryption attacks*. Typically, the attacker (hacker) enters between two users. In such attacks, the attacker is located on the path of communication, and then everything depends on him. Thus, it can interfere the communication or change its direction [22].

Network Monitoring. In addition to delays and bandwidth issues, network monitoring is also crucial. It is important to have a dynamic cloud monitoring system that provides traffic redirection, shared access, and service delivery. On the other hand, there is a need for monitoring to effectively detect malfunctions and network delays and to resolve security issues in the mobile cloud computing. Without certain network monitoring, any company cannot determine at what extent the users are following the policy related to the dissemination of valuable information. Additionally, programming languages used in Web 2.0 applications (such as Java, AJAX, and JSON data exchange formats) also enable malicious software to access and damage (e.g. accessing or deleting information or applications) the network infrastructure of the company. Therefore, each company using social media should perform high-level security to protect any information located within a network infrastructure [23].

• *Compliance and performance*. At present, there is no formal standard set of policy for mobile cloud computing. However, there are a number of rules for the storage and use of data in the *PCIDDS (Payment Card Industry Data Security Standard)* and *HIPAA (Health Insurance Portability and Accountability Act)* standards [24]. Regular reporting and auditing are also required for these standards. These rules are important to be fully and appropriately used in order to move corporate data to cloud. Use of open clouds can be complicated or even impossible if the data have certain legal restrictions or do not meet any of the rules. In this regard, providers must build cloud infrastructure and approve their compliance with safety standards to meet the needs of the managed markets.

Certification process can be complicated due to a number of non-technical factors, including general concepts about the cloud. There are numerous security threats and therefore it is impossible to take preventive measures for each of them. When a user runs any application, it does not have an idea about the characteristics and consequences of the potential security threats associated with the usage. Thus, the user must be notified about the network and data security. As for social media, trainings should be developed to address additional risks that it cause. These social media trainings can also be applied to the annual security frameworks of the organizations. Social media and websites can also be resolved through these certification and accreditation procedures, thereby ensuring the security standards of organization. Furthermore, a monitoring framework can be organized by the organization benefiting from the knowledge of workers with high social media and IT skills [24].

• *Responding to incidents*. Incidents may occur even after the measures taken to ensure data security, and instructing users about the safety methods. Each cloud provider company must set out a plan to respond to prevent data loss and abuse and to protect against malicious attack. Most providers do not improve their security services claiming that they can not be attacked. However, it should be noted that cloud-based services often attract the attention of hackers. Therefore, it is more appropriate to take measures before being attacked. In other words, the prevention of any attack is easier than its subsequent restoration [25].

In many cases, a cloud user is unaware of where the cloud services are physically located. Nevertheless, these places also face some disasters such as include fire, hurricane, and natural disaster. Therefore, in this regard, they should take some measures, otherwise, the cloud provider can not respond to these threats and provide uninterrupted service [26].

Related works on security and privacy issues

Security and privacy issues of mobile cloud computing have been explored by many researchers so far. Multi-cloud systems have been recently used to address security and privacy issues in mobile cloud computing more reliably. This system allows the users to use the services of non-dependent providers, which eliminates the dependence of users on one cloud provider. At the same time, this system eliminates the problem of data transmission to other clouds if there is a problem in cloud. The users of cloud services are anxious that one cloud system alone can not provide security and privacy. Therefore, they use multi-cloud systems for data storage and processing. Many articles on high-level security issues of multi-cloud systems have also been published [27].

The access to data by unauthorized users and hackers can be avoided through storing vital data of the organization's employees (credit card and health information, etc.) in multi-cloud systems [28].

When switching from single-cloud systems to multiple-cloud systems, privacy and security issues are distributed across multiple providers, increasing the users’ trust in the integrity of the system. If users have any problems with the use of data stored in cloud, there is no need to relocate them to other clouds. Cloud system easily avoids these types of problems, since it has previously placed those data in other clouds [29].

The storage of encrypted data of users on different cloud servers by dividing them into certain portions can increase security and privacy [30].

Popovich et al. [31] in their work indicate security and privacy issues facing providers, which offer cloud services. Cloud servers are at a distance, and users access resources via VM. Many VMs are created in one physical machine. Although each user works on a personal virtual environment, utilized VMs cause security threats to one another. The authors propose a method to eliminate these threats.

A new architecture of mobile cloud computing, which provides the integration of mobile applications with various cloud services for data security, is offered [32]. The proposed model improves data storage and processing on mobile devices. The model maintains the integrity and security of data.

G.Portokalidis et al. offer a scheme to detect threats against mobile devices (smartphones), based on CloudAU research conducted by Oberheide et al. in their work [33]. Clouds contain many smartphone backups that simultaneously detect different types of attacks. The proposed scheme minimizes the transmission load and reduces energy consumption by up to 30%. In this method, the cloud is considered to be completely reliable.

User authentication is a problem in mobile cloud computing. When using cryptography methods to encrypt and authenticate the data, when the key is exposed or lost, the access to resources becomes complicated. Therefore, an effective management of mobile computing systems is required. In [34], an identification model using profiling is offered. It ensures the combination of user and service information. However, the application of complex security algorithms must be implemented taking into account the limited resources of smartphones [34].

Phosphor model is also offered, where the interaction between the SIM card and the *Digital Rights Management Agent* is supported by the *Licensing Status* protocol.

In [35], a new proxy re-encryption scheme for secure data service and a new model with an identifier-based encryption scheme. This scheme ensures the confidentiality of a user. Thus, the cryptographic translation of the data is performed by a user. However, this increases the energy and processing requirements of the mobile device.

In [36], security issues caused by malicious software in the mobile environment are explored. This malware affect one VM and quickly infects others. The attacked VM causes data leakage and loss, which is a serious problem for cloud users.

The authors offer Cloud AV platform and malware detection system. The mobile agent used in this model primarily analyzes malicious files. If its signature does not comply with the cached database, it is sent to the network service to detect malicious files through multiple machines running on the host machines in parallel with the use of virtualization method. These methods can detect malware better. The advantages of the device include the minimum complexity of software and low energy consumption. However, it has some limitations, such as operation interruptions and accidental confidentiality risks [37].

Conclusion

This article analyzed secure protection of the user data from others in the mobile cloud computing and security issues in mobile cloud computing network. The security and privacy issues that emerged during the use of mobile computing clouds were investigated, and solutions were indicated. The article provided a detailed analysis of data security in mobile cloud computing, confidentiality, data placement and displacement, data integrity, and cyber attacks. The problems of mobile cloud computing security and privacy were explored, and available studies in this field were analyzed.

This work was implemented with the financial support of the Science Development Fund under the President of the Republic of Azerbaijan - Grant # EIF-2014-9 (24) -KETPL-14/02/1

References

1. Gayathri M.R., Srinivas K. A Survey on Mobile Cloud Computing Architecture, Applications and Challenges // International Journal of Scientific Research Engineering & Technology, 2014, vol.3, no.6, pp.1013–1021.
2. Qi H., Gani A. Research on mobile Cloud Computing: review, trend and perspectives / Proceeding of IEEE second international Conference on Digital Information Technology & its application, 2012, pp.195–201.
3. Xiao Z., Xiao Y. Security and Privacy in Cloud Computing // IEEE Communications Surveys & Tutorials, 2013, vol.15, no.2, pp.843–859.
4. Gopichand M. An Overview of Security and Privacy Issue in Mobil Cloud Computing Environment // International Jornal of Advanced Researc in Computer Science and Software Engineering, 2016, vol.6, no.5, pp.779–784.

5. Hlavacs H., Treutner T., Gelas J.P., Lefevre L. Orgerie A.C. Energy consumption side-channel attack at virtual machines in a cloud / IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), 2011, pp.605–612.
6. Caytiles R., Lee S. Security considerations for Public Mobile Cloud Computing // International Journal of Advanced Science and Technology, 2012, vol.44, pp.81–88.
7. Chen Y., Paxson V., Katz R.H. What's New About Cloud Computing Security? Electrical Engineering and Computer Sciences University of California at Berkeley.Technical Report, no. UCB/EECS-2010-5, 2010, pp.1–8.
8. Chen Y.J., Wang L.C. A security framework of group location-based mobile applications in cloud computing / Proceeding International Conference on Parallel Processing Workshops, (ICPPW’11), 2011, pp.184–190.
9. Subashini S., Kavitha V. A survey on security issues in service deliverymodels of cloud computing // Journal of Network and Computer Applications, 2011, vol.34, pp.1–11.
10. Fernando N., Seng L.W., Rahayu L. Mobile Cloud Computing: A Survey // Journal of Future Generation Systems, 2013, vol.29, no.1, pp.84–106.
11. Donald A., Oli S., Arockiam L. Mobile cloud security issues and challenges: A perspective // International Journal of Engineering and Innovative Technology, 2013, vol.3, no.1, pp.401.
12. Sarrab M. Mobile Cloud Computing: Security Issues and Considerations // Journal of Advances in Information Technology, 2015, vol.6, no.4, pp.248–251.
13. Collings R. Mobile Cloud Adoption Challenges in the Enterprise. http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-theenterprise/
14. Dinh H.T., Lee C., Niyato D., Wang P. A survey of mobile cloud computing: Architecture, applications, and approaches // Wireless Communications and Mobile Computing, 2013, vol.13, no.18, pp.1587–1611.
15. Bahar A., Habib A., Islam M. Security architecture for mobile cloud computing // International Journal of Scientific Knowledge Computing and Information Technology, 2013, vol.3, no.3, pp.11–17.
16. Jashizume K. H., Rosado D., Fernandez-Medina E., Eduardo B. An analysis of security issues for cloud computing // Journal of Internet Services and Applications, 2013, vol.4, no.5, pp.1–13.
17. Schoo P., Fusenig V., Souza V., Melo M., Murray P., Debar H., Medhioub H., Zeghlach D. Challenges for Cloud Networking Security / 2nd International ICST Conference on Mobile Networks and Management, 2010, pp.2–16.
18. Zhangwei H., Mingjun X. A Distributed Spatial Cloaking Protocol for Location Privacy / Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010, vol.2, pp.468–471.
19. Zou P., Wang C., Liu Z., Bao D. Phosphor: Cloud Based DRM Scheme with Sim Card / Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), 2010, pp.459–463.
20. Zhu Y., Hu H., Ahn G.J., Huang D., Wang S. Towards temporal access control in cloud computing / INFOCOM, 2012, pp.2576–2580.
21. Lakshmi I. A Review on Cloud Computing in Mobile Applications. // International Journal of Computer Science and Mobile Computing, 2016, vol.5, no.6, pp.149–161.
22. Gregg M. 10 Security Concerns for Cloud Computing. Global Knowledge, 2010, pp.2–7.
23. Sarrab M., Janicke H. Runtime monitoring and controlling of information flow // International Journal of Computer Science and Information Security, 2010, vol.8, no.9, pp.37–45.
24. Chow R., Jakobsson M., Masuoka R., Molina J., Niu Y., Shi E., Song Z. Authentication in the clouds: a framework and its application to mobile users / Proceeding ACM Cloud Computing Security Workshop (CCSW’10), 2010, pp.1–6.

25. Huang D., Zhou Z., Xu L., Xing T., Zhong Y. Secure data processing framework for mobilecloud computing / Proceeding IEEE INFOCOM Workshop on Cloud Computing, (INFOCOM’11), 2011, pp.620–624.
26. Yogita D.M., Kailas K.D. Protection concern in Mobile Cloud Computing - A Survey // IOSR Journal of Computer Engineering (IOSR-JCE), pp.39–44.
27. AlZain M., Pardede E., Soh B., Thom J. Cloud computing security: From single to multi-clouds/45th Hawaii International Conference on System Science (HICSS), 2012, pp.5490–5499.
28. Cachin C., Keidar I., Shraer A. Trusting the cloud // ACM SIGACT News, 2009, vol.40, no.2, pp.81–86.
29. Vukolic M. The byzantine empire in the intercloud // ACM SIGACT News, 2010, vol.41, no.3, pp.105–111.
30. Shankarwar M., Pawar A. Security and privacy in cloud computing: A survey / Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, ser. Advances in Intelligent Systems and Computing. Springer International Publishing, 2015, vol.328, pp.1–11.
31. Popovic K., Hocenski V. Cloud computing security issues and challenges / MIPRO, Proceedings of the 33rd International Convention, 2010, pp.344–349.
32. Kovachev D., Klamma R. Framework for Computation Offloading in Mobile Cloud Computing // International Journal of Artificial Intelligence and Interactive Multimedia, 2012, vol.1, no.7, pp.6–15.
33. Portokalidis G., Homburg P., Anagnostakis K., Bos H. Paranoid Android: versatile protection for smartphones / Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), 2010, pp.347–356.
34. Choi E., Jeong H. User authentication using profiling in mobil cloud computing / AASRİ Confrence on Power and Energy Systems, 2012, pp.262–267.
35. Jia W., Zhu H., Cao Z., Wei L., Lin X. SDSM: a secure data service mechanism in mobile cloud computing / The First International Workshop on Security in Computers, Networking and Communications, 2011, pp.1087–1082.
36. Kim.T et al. Monitoring and detecting abnormal behavior in mobile cloud infrastructure / 2012 IEEE Network Operations and Management Symposium, 2012, pp.1303–1310.
37. Oberheide J., Veeraraghavan K., Cooke E., Jahanian F. Virtualized in-cloud security services for mobile devices / Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), 2008, pp.31–35.