Security and Privacy Issue Management in Mobile Cloud Environment

[1]N.Usha
Lecturer, Dept. of ISE, SJBIT,
Bangalore,
n.ushanagaraj@gmail.com

[2]Bhavana. V,
Lecturer, Dept. of ECE, Amrita Vishwa Vidhyapeetam University,
Bangalore,
bhavanapyarilal@gmail.com

Abstract - Mobile cloud computing is becoming more and more popular among mobile users and developers who can see a direct benefit to overcome the resource limitations in mobile devices – be it battery life, memory space or processing power. The widespread adoption of programmable smart mobile devices and connecting to public domain of internet as well as cloud service providers provide newer privacy as well as security challenges across enterprises. Data loss from stolen or decommissioned mobile devices, unsecured information exchange through rouge access points and access of vulnerable network fetch privacy as well as security threats of mobile cloud computing. Data breaches, account hijacking, insecure API exposure, denial of services, malicious insider attacks, loss of encryption key, virtual machine isolation bring forth some of the additional security and privacy threats. An attempt to enumerate several privacy plus security threats and put forth best practices and recommendations as preventive as well counter measures on incidence. We have evaluated the provisioning of services such as Security as a Service (SecaaS) in different scenarios and practices based on the requirement of individual applications.

Keywords Mobile Cloud Computing; Cloud Computing; AAA Vulnarebilities;, STRIDE; SecaaS.

I. INTRODUCTION

With ever growing communication and computing infrastructure, mobile and other handheld devices have become more and more sophisticated realizing the vision of ubiquitous and pervasive application. In last couple of years, there has been a rapid mounting proliferation of mobile devices (such as smartphone, tablet) into the enterprises. To facilitate, mobile computing has gained remarkable momentum. Through Morgan Stanley Research Data and Estimates as of 9/12, Meeker [1][2] has shown that globally shipments of Smartphone and tablets exceeded PCs (including notebooks and laptops) in Quarter four of 2010 and the trend continues to overshoot till 2015. However, mobile and handheld devices are constrained due to resource limitations primarily caused by limited battery life requiring recharging, constrained size of memory or limited power of the processor especially during roaming and challenge of being seamlessly connected throughout mobility or even limited size of physical persistent storage. Typical mobile handsets will continue to have limitations in power, memory, storage capacity, on-demand and wireless bandwidth. Execution of high computational tasks in a mobile device may also drain the battery power very quickly. To address these limitations of mobile devices, cloud computing can be an obvious choice when most of the resources (CPU, Memory and I/O) intensive tasks can be performed at cloud and thereby saving energy of the mobile handsets. Cloud computing with its *pay-per-use* model alleviates the in-house computing cost and thereby stands as an obvious choice for global enterprises targeting cost optimization yet having flexible, secured and efficient use of IT resources. Mobile cloud computing [3] has emerged as rapidly growing with enormous popularity within mobile users and developers community who can see a direct benefit to overcome the resource limitations in mobile devices. There is also a need for lightweight security framework for mobile computing with limited processing on the device level and with less communication overhead. Use of inescapable BYOD (Bring Your Own Device) to access enterprise data through cloud services has increased the security and privacy risks multifold. IT infrastructure department can no longer exercise such tight control over personal devices. And with the use of personal devices, the ever growing corporate perimeter has grown larger and more diffuse, defying attempts at management and control. There has been a paradigm shift of security controls in traditional enterprise workstations connected over LAN and WAN. For example, malware detection software that runs behind the traditional resource-rich computers will not work for mobile device. From privacy point of view, today's mobile computers are getting location based service (LBS) such as "where is the nearest gas station or police station?" Location based service has a privacy threat too. An adversary can get hold of the location data and can predict the habit of the person's movement. Adopting cloud services such as IaaS (Infrastructure as a Service), enterprises are facing greater risks in protecting their sensitive and confidential information and maintaining compliance to standards. One such prominent standard is Payment Card Industry Data Security Standard (PCI DSS) [4][5] for merchants, acquirers, Issuers, processors who store, process or transmit credit card and Personal Accountholder Information (PAI). Another such standard is The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules for protection of healthcare information.

II. BACKGROUND AND RELATED WORK

Several researchers have contributed towards interesting work related to security and privacy issues alongwith suitable authentication services for mobile cloud users. Hung et al [6] have proposed a mobile cloud execution framework to utilize the cloud virtualization access from a mobile station with

encryption and isolation to protect against eavesdropping from cloud providers. They have also considered issues of migrating applications and data synchronization between several execution environments along with communication issues. Khan et al [7] have emphasized that enterprise adaptability of the mobile cloud computing paradigm is facing impediment because of inherent security threats and a number of loopholes and challenges that still exist in the security policies of mobile cloud computing. Suo et al [8] have outlined the challenges of security and privacy in the mobile cloud computing while enumerating the benefits of mobile cloud computing as ondemand self-service and extendibility, with infrastructure, platform, and software services provided in a cloud to mobile users through the existing public domain mobile network. Jana and Bandyopadhyay [9] analyzed several security threats and its measures, and suggested additional recommendations on top of best practices adopted for Identity and Access Management (IAM) for mobile cloud users. Slawomir Grzonkowski et al [10] have presented a mutual and two-factor authentication and claimed to be more secure against various phishing attempts than existing trusted third party protocols. They have also outlined several authentication services such as Kerberos, a third party authentication protocol, Open ID, designed to provide Single Sign-On features and decentralized user authentication supporting same login credentials at multiple websites and OAuth [11] protocol. Chen and Wang [12] talked about a security framework of group location-based mobile applications in cloud computing. Ristenpart et al [13] discussed how an IaaS allows users to create VM according to the capacity they require on a just in time basis. The authors' showed that it is possible to map the likelihood of target VM's location. With this information, intruders can instantiate VM as a co-resident VM with the target VM to make cross-VM side channel attack. Data isolation failure in a multi-tenancy environment and hypervisor layer attack are new class of attacks which were not present in traditional enterprise networks. Many of the concerns and fear of the cloud has been addressed by Chow et al [14]. Instead of protecting data from outside using systems and applications, authors propose a self protecting data by injecting intelligence into the data to protect itself. Data needs to be self defending, self-describing and encrypted and packaged as per the policy without any dependence on the environment where it is stored or processed. Barazzutti et al [15] stressed on privacy preserving filtering that can be supported by several mechanisms for encrypted matching in order to help to avoid information leakage especially in a content-based publish/subscribe model. Dash et al [16] suggested solutions for secure mobile cloud architecture by using one of data mining tasks, a privacy preserving K-Medoids. The goal was to cope up with the challenge how multiple parties in a mobile could framework collaboratively conduct information exchange without breaching data privacy. Bin Liu et al [17] focused on privacy-preserving collaborative learning for the mobile setting to address supporting complex classification methods like support vector machines, respecting mobile computing and communication constraints, and enabling user determined privacy levels. Zhou and Huang [18] presented a privacy preserving cipher policy attribute-based encryption to protect sensing data while lightweight wireless communication devices extend cloud services into the sensing domain within mobile cloud computing infrastructure. Also an attribute based data storage system can act as a cryptographic group-based access control mechanism during information exchange in mobile cloud. Pirker et al [19] presented privacy preserving cloud resource-payment to enable mobile clients to anonymously consume resources of a cloud service provider such that the provider is not able to track users' activity patterns. Satyanarayanan [20] discussed a wide range of issues in areas such as privacy, software licensing, and business models with the emergence of cloudlet-based hardware/software ecosystem to support for example, cognitive assistance for attention-challenged mobile users, scalable crowd-sourcing of first-person video, and ubiquitous mobile access to one's legacy world.

III. AAA AND PRIVACY VULNERABILITIES

Eventual goal and indeed one of the major challenges of secured mobile could computing with privacy preserving ability is to provide reliable AAA (authentication, authorization and accounting) with different levels of access control (rule based or role based) and efficient governance within IAM [21] to meet enterprise business requirements using mobile cloud framework. A cloud based location trusted server (LTS) proposed by Chow wt al [22] can be used to collect the location request information and using k-anonymity and GPS service. The location information can be put in a 'cloaked region' or blurred zone and sent to LBS server for further processing. LBS server will be processing 'cloaked region' information where k (using k-anonymity) number of people are present including the requester. The adversary will not be able to detect the individual person's location from of 'cloaked region' information [23] and hence the privacy is protected. This is an example of protection of data privacy for mobile users using cloud computing. Otherwise, the LBS faces a privacy issue when mobile users provide private information such as their current location. Yong [24] applied tunable anonymity, through both asymmetric and symmetric encryption primitives into the authentication process providing k-anonymity to preserve privacy in mobile computing scenario. Zhu et al [25] proposed a location-based fine-grained access control mechanism for LBSs, enabling effective location-based authentication, access control as well as privacy protection. Their approach is based on the construction of a spatio-temporal predicate-based encryption by means of efficient secure integer comparison. We have taken an in-depth view of the AAA (Authorization, Authentication and Accounting) vulnerabilities in mobile cloud environment [6] [7] that have a serious business impact such as service delivery, company reputation customer's trust, IP rights, HR data and financial implications. The list of typical threats of mobile cloud computing due to AAA vulnerabilities and their corresponding security controls such as Impacts, STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Services, and Elevation of Privilege) and CIANA (Confidentiality, Integrity, Availability, Non-Repudiation and Authenticity) are shown in Table I.

Threats	Security Controls		
	Impacts	*STRIDE*	*CIANA*
Malicious insiders and data breaches	Abuse of high privileged administrative roles	Data tampering, information disclosure, identity spoofing	Confidentiality, Integrity, Availability, Authenticity
Intercepting data during information exchange or failure to isolate virtual machine environment	Sniffing, spoofing, man-in-the middle-attack, side channel and replay attack	Data tampering, repudiation, information disclosure, identity spoofing	Availability, Non-Repudiation, Confidentiality, Integrity
Denial-of-services during control of resources in cloud	Identity theft, unlimited resource usage.	Denial of Services	Availability
Data loss, loss of encryption key	Identity theft	Repudiation, Denial of Services	Availability, Non-Repudiation
Accounts and Service traffic hijacking	Phishing, service hijacking, fraud, reuse of credential and password	Data tampering, repudiation, information disclosure, elevation of privilege, identity spoofing	Authenticity, Confidentiality, Integrity, Availability, Non-Repudiation
Insecure interfaces and APIs	Reliance of weak-set of interfaces causing problems in confidentiality, integrity, availability and accountability	Data tampering, repudiation, information disclosure, elevation of privilege	Authenticity, Confidentiality, Integrity
Loss of operation and security logs	Hacking, unauthorized access to gain	Data tampering, repudiation,	Availability, Confidentiality, Integrity

TABLE I. TYPE OF THREATS DUE TO AAA VULNERABILITIES

The general controls against each type of threats related to AAA vulnerabilities are given in Table II. Against each type of STRIDE, we have shown the controls that has been suggested by CSA [26] to address the threats using IdEA (Identity, Entitlement and Access Management) having five main components – Authentication, Authorization, Administration, Audit & Compliance and Policy. This security guidance is applicable to mobile cloud computing too. The guidance has covered a wide range of topics including Identity Architecture, Identity Federation (interconnection of disparate Directories Services) and use of SAML (Security Assertion Markup Language) to ensure portability to disparate and independent security domains.

Type of threat	Control
Spoofing	Dual or strong authentication
Tampering with Data	Digital Signature (as used in SAML), Hashing
Repudiation	Digital Signature (as used in SAML), Audit logging
Information Disclosure	SSL, encryption
Denial of Services	Security Gateways

TABLE II. CONTROLS AGAINST THREATS RELATED TO AAA VULNERABILITIES

IV. SECURTY AS A SERVICE (SECAAS)

Security as a Service (SecaaS) [9] offered by Cloud Service Providers (CSP) include security solutions for several different media, web, email and allied for prevention for data loss as well as robust identity and access management (IAM). Cloud Security Alliance (CSA) had come out with a set of implementation guidelines for each area of SecaaS [27] in order to have a defined implementation guideline as a standard to adopt by individual cloud vendors. The major components of IAM SecaaS [27][28][29] as defined by CSA guideline are Authentication (Strong and Risk Based Authentication), Identity Federation Services (Federated Identity Management, Federated Single Sign-on) Identity Management Service (Provisioning and De-provisioning, Centralized Directory Services, Privileged User Management) Authorization, Access management, Audit and Reporting. To avoid data leakage emanated from muti-tenancy cloud environment, Security Service Providers (SSP) are trying to make sure high level of data compartmentalization. Shared data within cloud environment are anonymized to protect data privacy by inhibiting the exposure of identity and source of data [26]. SecaaS is becoming an indispensable component for enterprises. SecaaS providers are now diversifying their offerings to include IAM, prevention for data loss, web security, and business continuity planning (BCP) as well as disaster recovery (DR), encryption, email security, security assessment, intrusion prevention and detection systems (IDS/IPS), security information and event management (SIEM) etc to provide enterprises with secure business resilience, business continuity and competitive advantage. However there are concerns when implementing SecaaS. The primary goal of IAM SecaaS implementation guide by CSA [27] was to address the concerns and requirements of security controls for cloud users. Some of these are potential lack of control over data, SecaaS provider operations, visibility for compliance purposes, multijurisdictional regulatory requirements, portability and interoperability (to avoid vendor lock-In) etc. Interoperable representation of authorization or entitlement information (lack of support of OASIS XACML or OAuth authorization standards), access control granularity and resource based access control are some of the concerns too. Security service providers have addressed those issues of cloud users and coming up with more matured offerings. Kim et al [30] presented Fiat-Shamir protocol that uses *zero-knowledge authentication* that aims to create a system where an entity can prove that it knows a secret without actually revealing it, thereby protecting from intrusion.

V. RECOMMENDATIONS AND BEST PRACTICES FOR SECURITY AND PRIVACY MANAGEMENT IN MOBILE CLOUD

The top threats to mobile computing [28][29] have been released by CSA (Cloud Security Alliance). We have made some additional recommendations on top of the best practices based on our analysis and research work. Based on our analysis of incidences of security as well as privacy threats from data captured over a period of years in electronic payment industries, we have identified the several top root causes and captured through an Ishikawa or fishbone diagram [9]. (Fig 1).

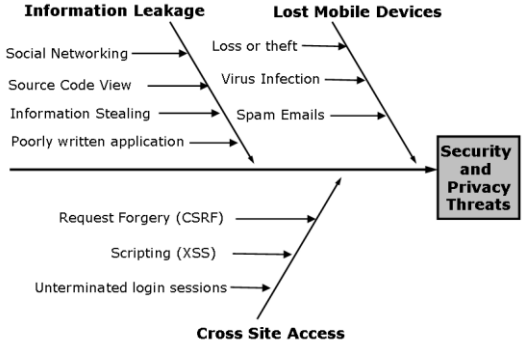

Fig. 1. Nature of Security and Privacy Threats

According to captured fishbone analysis, the nature of security and privacy threats as well as recommended counter measures are presented next.

- *Lost Mobile devices due to loss or theft, virus infection, spam emails* – On top of awareness of the owner of the device, on incidence of the event of being stolen, lost or decommissioned, the device needs to be deactivated.

Additionally, as a preventive measure, the physical storage should be encrypted and stored data must remain secured against unauthorized access even when it is lost or stolen. The device must be connected to a central security server on a periodic basis to scan and remove the PAI (Personal Accountholder Information). Antivirus software (AV) must run at each device including BYOD and get periodically updated as per antivirus (AV) policy of the enterprise. However, special malware protection software is required for mobile devices. Cisco Identity Services Engine (ISE) engine [31] supports enterprise networks with number of mobile users and mobile devices.

- *Information Leakage due to social networking, source code view, information stealing or poorly written application* – Guard against Social Engineering can be done through periodic awareness sessions on proper usage of social engineering.

All outside access from device must go through a localized or server centric proxy tool capable of data loss prevention (DLP). Internet Web Security Service agents can help to monitor improper usage of Internet. Implementation of Messaging Security System like InterScan Messaging Security Suite (IMSS) can be done to block spam emails coming in. Flaw in application security (coding error) needs to be prevented through secure coding best practices for ensuring Payment Card Industry Data Security Standard (PCI DSS) compliance. All remote access sessions over the Internet must be encrypted using virtual private network (VPN). All payment transaction information transmitted over, an end to end trusted network must adhere to PIN and CVV (Card Verification Values). Two factor authentications using mobile such as smart card with PIN, hardware token can be used for privileged users who have access to business sensitive data. It is unlikely that both smart card and mobile devices will be lost or stolen together. Dawn Song et al [31] suggested data protection as a service (DPaaS) as a suite of security primitives which can be offered by a cloud platform to enforce data security and privacy.

- *Cross Site Access due to request forgery (CSRF), scripting (XSS) or non-terminated login sessions* – Cross-site scripting (XSS) may try to inject vulnerable client-side script into web pages viewed by other users. Conformance to the PCI-DSS standards as well as Open Web Application Security Project (OWASP) guidelines to validate user supplied input using white lists (positive filter) to comply with the expected format is recommended. The client side code must not allow an attacker to get access to sensitive information.

For this, ensuring positive input validation; HTML and XML encoding are recommended. Insufficient CSRF (Cross Site Request Forgery) can be protected by following PCI-DSS standards and OWASP guidelines to include unique token in a secreted field so that the value can be sent in the body of the HTTP request, while avoiding its inclusion in the URL, which is subject to direct exposure. All non-terminated sessions must be automatically signed out in timely manner. We have also captured the top security threats in terms of pareto analysis diagram (Fig 2). The horizontal axis represents the type of threat. The left and right vertical axes represent the frequency of occurrence and cumulative percentage of the total number of occurrences respectively. Out of the different security threats captured like virus infection, spam emails, social engineering, loss of smart cards, exposure to source code, improper resource release, information stealing, loss of mobile devices, cross site scripting (XSS), cryptographic issues, cross site request forgery etc. we find that virus infection, spam emails, social engineering contribute to more than eighty percent of privacy and security threats.

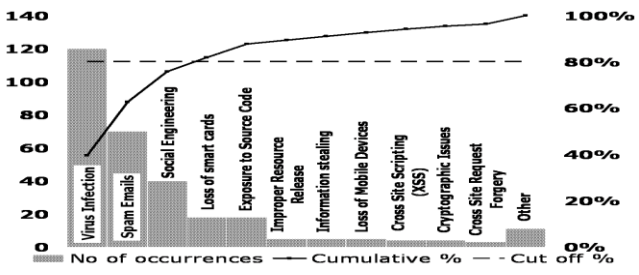

Fig. 2. Pareto analysis of top privacy and security threats

Some additional recommendations for efficient and effective privacy and security controls are given below.

- *Prudent selection the appropriate computational task* - It is recommended to judiciously select the computational part that needs to be in the cloud environment and rest of the part resident in the mobile device while keeping in mind the power and storage constraints of mobile devices.
- Karthik

Kumar et al [33] have suggested energy saving of the mobile devices and optimal network bandwidth usage by reducing computation at the mobile system while off loading high computational intensive tasks with less communication overhead at the cloud.

- *Partition of computations for running on cloud* - The thumb rule is that for very high processor bound computation offload it to cloud and for high to and fro communication, use the mobile device itself. However, depending on network bandwidth and volume of data exchange, on-the-fly decisions are required to be taken whether to offload to cloud or execute the application locally in the mobile device. The possible solution is partitioning computation between the mobile devices and the cloud environment to reduce energy consumption while partially processing the real time data on the mobile devices [9].
- *Keeping Control Over Data* - Data Owners need higher control over their own data as compared to the Cloud Service Providers (CSP) acting as hosts. Bogdanov and Kalu [34] suggested Secure Multiparty Computation (SMC) and Homomorphic Encryption (HE) where processing can be done on encrypted data and the use of multiple secret-shared databases so that no single host can have the capability to recover data.
- *Secure Communication between mobile client and cloud* server - A component based Secure Mobile-Cloud (SMC) framework suggested by Popa et al [35] can help to ensure integrity of an application during setup and secure the communication between the application components running in mobile and cloud. On the same framework, encryption module is preferred at mobile device and HSM (Hardware Security Module) at the cloud end. HSM should be housed in a secured environment with higher level of security controls [36]. This will ensure a secure point to point encryption (P2PE) which is a requirement of PCI-DSS for mobile payment transactions.

VI. CONCLUSION AND FUTURE WORK

On paradigm shift from traditional desktops and laptops, Smartphone and tablet based mobile computing connected to cloud backbone is the proclivity of the modern day technology as well as business across enterprises. As network boundaries are getting redefined, traditional security controls also need to be revisited to cope up newer privacy and security challenges of mobiles when connected to cloud. Trend predicts that with more and more BYOD getting accepted as enterprise policy, .and keeping inherent resource constraints of mobile devices in mind, mobile cloud computing has emerged with a greater promise.

Most of the computational and storage requirement will be controlled by the servers residing at cloud service provider's end. Traditional rules for privacy and security will be redefined at different levels starting from all layers of application architecture. Security and privacy compliance requirements are getting redefined be it PCI-DSS (Cloud Computing Guidelines) or any other standards. Future work lies in embracing mobile cloud computing as the de-facto standard for computational analysis and IT requirements. Daniela POPA et al [38] have suggested a component based Secure Mobile-Cloud (SMC) framework to ensure integrity of an application during setup and secure the communication between the application components running in mobile and cloud. Having encryption module at mobile device end and HSM (Hardware Security Module) [36] at the cloud end will provide higher control on information security and data privacy.

Future work lies to come up with standards for compliance of tighter privacy and security controls in mobile cloud computing scenario to cope up the need of ubiquitous pervasive computing.

REFERENCES

[1] Meeker M., Internet Trends @ StanFord – Bases, *Presentation by Kleiner Perkins Caufield Buyers*, Dec. 3, 2012, URL: www.kpcb.com/file/kpcb-2012-internet-trends-update, last accessed: June 2013.

[2] Katy Huberty, Ehud Gelblum, *Morgan Stanley Research. Data and Estimates* as of 9/12

[3] M. Reza Rahimi, Nalini Venkatasubramanian, Sharad Mehrotra, and Athanasios V. Vasilakos. 2012. MAPCloud: Mobile Applications on an Elastic and Scalable 2-Tier Cloud Architecture. In *Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing (UCC '12)*. IEEE Computer Society, Washington, DC, USA, 83-90.

[4] Information Supplement: PCI DSS Cloud Computing Guidelines. *PCI Data Security Standard (PCI DSS)*, Ver. 2.0, Date: Feb, 2013 by Cloud Special Interest Group, PCI Security Standards Council URL: https://www.pcisecuritystandards.org/pdfs/pr_130205_Cloud_SIG.pdf, last accessed: June 2013

[5] Information Supplement: PCI DSS Wireless Guidelines Standard: *PCI Data Security Standard (PCI DSS)* Version: 2.0 Date: August, 2011 by Wireless Special Interest Group (SIG) PCI Security Standards Council URL: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guideline_with_WiFi_and_Bluetooth_082211.pdf, last accessed: June 2013.

[6] Shih-Hao Hung, Chi-Sheng Shih, Jeng-Peng Shieh, Chen-Pang Lee, and Yi-Hsiang Huang. 2012. Executing mobile applications on the cloud: Framework and issues. *Comput. Math. Appl*. 63, 2 (January 2012), 573-587.

[7] Abdul Nasir Khan, M. L. Mat Kiah, Samee U. Khan, and Sajjad A. Madani. 2013. Towards secure mobile cloud computing: A survey. *Future Gener. Comput. Syst*. 29, 5 (July 2013), 1278-1299.

[8] Hui Suo; Zhuohua Liu; Jiafu Wan; Keliang Zhou, "Security and privacy in mobile cloud computing," *Wireless Communications and Mobile Computing Conference* (IWCMC), 2013 9th International , vol., no., pp.655,659, 1-5 July 2013

[9] Debasish Jana and Debasis Bandyopadhyay, "Management of Identity and Credentials in Mobile Cloud Environment", *Proceedings of the 2013International Conference on Advanced Computer Science and Information Systems* (ICACSIS 2013), September 28-29, 2013, Bali, Indonesia

[10] Grzonkowski, S.; Corcoran, P.M.; Coughlin, T., "Security analysis of authentication protocols for next-generation mobile and CE cloud services," *Consumer Electronics - Berlin (ICCE-Berlin), 2011 IEEE International Conference on*, vol., no., pp.83,87, 6-8 Sept. 2011.

[11] The Essential OAuth Primer: Understanding OAuth for Securing Cloud APIs, White Paper, *Ping Identity Corporation*, 2011, URL: http://www.innovation-district.com/wp-content/uploads/2012/04/The-Essentials-of-OAuth.pdf, last accessed: June 2013

[12] Yu-Jia Chen and Li-Chun Wang. 2011. A Security Framework of Group Location-Based Mobile Applications in Cloud Computing. In *Proceedings of the 2011 40th International Conference on Parallel Processing Workshops* (ICPPW '11). IEEE Computer Society, Washington, DC, USA, 184-190

[13] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security* (CCS '09). ACM, New York, NY, USA, 199-212.

[14] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (CCSW '09). ACM, New York, NY, USA, 85-90.

[15] Raphaël Barazzutti, Pascal Felber, Hugues Mercier, Emanuel Onica, and Etienne Rivière. 2012. Thrifty privacy: efficient support for privacypreserving publish/subscribe. In *Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems* (DEBS '12). ACM, New York, NY, USA, 225-236.

[16] Sanjit Kumar Dash, Debi Pr. Mishra, Ranjita Mishra, and Sweta Dash. 2012. Privacy preserving K-Medoids clustering: an approach towards securing data in Mobile cloud architecture. In *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology* (CCSEIT '12). ACM, New York, NY, USA, 439-443.

[17] Bin Liu, Yurong Jiang, Fei Sha, and Ramesh Govindan. 2012. loudenabled
privacy-preserving collaborative learning for mobile sensing. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems* (SenSys '12). ACM, New York, NY, USA, 57-70.

[18] Zhibin Zhou and Dijiang Huang. 2012. Efficient and secure data storage operations for mobile cloud computing. In *Proceedings of the 8th International Conference on Network and Service Management* (CNSM '12), Jorge Lobo, Philippe Owezarski, and Hui Zhang (Eds.). International Federation for Information Processing, Laxenburg, Austria, Austria, 37-45.

[19] Martin Pirker, Daniel Slamanig, and Johannes Winter. 2012. Practical rivacy preserving cloud resource-payment for constrained clients. In *Proceedings of the 12th international conference on Privacy Enhancing Technologies* (PETS'12), Simone Fischer-Hübner and Matthew Wright (Eds.). Springer-Verlag, Berlin, Heidelberg, 201-220.

[20] Mahadev Satyanarayanan. 2013. Cloudlets: at the leading edge of cloudmobile convergence. In *Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures* (QoSA '13). ACM, New York, NY, USA, 1-2.

[21] AWS Identity and Access Management Using IAM API Version 2010-05-08, *Documentation on Amazon Web Services*, November 29, 2010 URL: http://aws.amazon.com/releasenotes/AWS-Identity-and-Access-Management/5539247863296373, last accessed: June 2013.

[22] Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu. 2011. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *Geoinformatica* 15, 2 (April 2011), 351-380.

[23] Dinh, H.T., Lee, C., Niyato, D. and Wang, P., A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*. October 2011.

[24] Yong Xi. 2012. Location Privacy in Emerging Network-Based Applications. *Ph.D. Dissertation*. Wayne State University, Detroit, MI, USA. Advisor(s) Loren Schwiebert and Weisong Shi.

[25] Yan Zhu, Di Ma, Dijiang Huang, and Changjun Hu. 2013. Enabling secure location-based services in mobile cloud computing. In *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing* (MCC '13). ACM, New York, NY, USA, 27-32.

[26] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Prepared by the *Cloud Security Alliance*, URL: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf, last accessed: June 2013

[27] Cloud Security Alliance SecaaS Guidance, Category 1: Identity and Access Management, 2012 by *Cloud Security Alliance*, URL: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf, last accessed: June 2013

[28] Top Threats to Mobile Computing, Prepared by the *Cloud Security Alliance*, March 2010, URL: https://downloads.cloudsecurityalliance.org/initiatives/mobile/top_threats_mobile_CSA.pdf, last accessed: June 2013

[29] The Notorious Nine Cloud Computing Top Threats in 2013, published by *Cloud Security Alliance*, February 2013, URL: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, last accessed: June 2013

[30] Sung-Kyoung Kim, Tae Hyun Kim, and Seokhie Hong. 2013. Fiatshamir identification scheme immune to the hardware fault attacks. *ACM Trans. Embed. Comput. Syst*. 12, 1s, Article 65 (March 2013), 11 pages