Identity and Access Management for Cloud Services Used by the Payment Card Industry

Ruediger Schulze(✉)

IBM Germany Research and Development GmbH, Schoenaicher Street 220, 71034 Boeblingen, Germany
ruediger.schulze@de.ibm.com

Abstract. The Payment Card Industry Data Security Standard (PCI DSS) mandates that any entity of the cardholder data environment (CDE) involved in the credit card payment process has to be compliant to the requirements of the standard. Hence, cloud services which are used in the CDE have to adhere to the PCI DSS requirements too. Identity and access management (IAM) are essential functions for controlling the access to the resources of cloud services. The aim of this research is to investigate the aspects of IAM required by the PCI DSS and to describe current concepts of IAM for cloud services and how they relate to the requirements of the PCI DSS.

1 Introduction

Credit card frauds are committed using different methods. According to [1], 60% of the value of fraudulent transactions within the Single Euro Payments Area (SEPA) were caused by card-not-present (CNP) payments in 2012. CNP frauds are committed without the actual physical use of the credit card, e.g. in online, phone or mail-order transactions. Online merchants are at an increased risks due to attacks which target to exploit vulnerabilities and obtain credit card records for use in CNP frauds and identity theft. The PCI DSS has been established to ensure the safety of the merchant's payment systems and has to be implemented by all merchants that provide payment with credit cards. The PCI DSS describes a set of 12 technical and operational requirements in five categories to protect credit card data [2]. The importance of the requirements claimed by PCI DSS can be illustrated at the example of the TJX data breach [3]. The TJX Companies, Inc., a department store chain in the United States, kept the magnetic strip data from customers credit cards in unencrypted from and was attacked by thieves first time in July 2005. In total, data of 94,000,000 cards was stolen. The PCI DSS defines some very prescriptive requirements to avoid such scenarios, e.g. sensitive authentication data must not be stored on storage at all and the primary account number has to rendered in unreadable format when stored. The requirements of the PCI DSS apply to all entities involved into the payment process, including service providers. Cloud services involved with credit

M. Luo and L.-J. Zhang (Eds.): CLOUD 2018, LNCS 10967, pp. 206–218, 2018.
https://doi.org/10.1007/978-3-319-94295-7_14

card payment have to be PCI DSS compliant. Cloud Service Providers (CSP) which are engaged by merchants as third-part service providers (TPSP) have to provide evidence of their PCI DSS compliance status [4]. IAM are essential functions when interacting with cloud services. IAM has to ensure that access to cloud services and related data is only granted to authorized users and that compliance with internal policies and external regulations is maintained. The aim of this research is to examine the IAM related requirements of the PCI DSS and to investigate current methods of IAM in the context of cloud services and PCI DSS. In the following, the requirements of the PCI DSS and the essential functions of IAM for cloud services are described, the PCI DSS requirements are assessed for their relation to the IAM functions and different methods of IAM for cloud services are analysed.

2 Payment Card Industry Data Security Standard

The PCI DSS has been issued to ensure the security of credit card and account data [2]. The latest version 3.2 of the standard has been released in April 2016 [2]. The technical and operational requirements of the PCI DSS apply to all entities involved in the process of the credit card payment. The scope of the PCI DSS is extensive. Any component included in the CDE is to be considered, including people, processes and technologies. The entities to be compliant with PCI DSS include merchants, processors, acquirers, issuers and services providers but also any entities that store, process or transmit cardholder data and sensitive authentication data. PCI DSS defines 12 requirements and corresponding test procedures which are combined into a security assessment tool for use during PCI DSS compliance assessments. The following requirements are to be assessed using the test procedures in the validation process [2]:

2.1 Build and Maintain a Secure Network and Systems

1. *Install and maintain a firewall configuration to protect cardholder data*
   Firewalls control the traffic between an entity's internal network and the untrusted, external networks, and the traffic in and out of sensitive areas within the internal trusted network. Firewalls and router configurations have to be established and implemented following a formal process for approving and testing all network connections and using documentation of business justification and network diagrams.
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*
   Intruders (external and internal) use default passwords or exploits based on default system settings to compromise systems. The information about default passwords and settings are widely known and can easily be obtained from public documentation. Vendor-supplied defaults must always be changed and unnecessary default accounts be removed before a system is connected to the network.

2.2 Protect Cardholder Data

3. *Protect stored cardholder data*
   Cardholder data refers to any information present in any form on a payment card. The cardholder data must be protected by the entities accepting payment cards and unauthorized use has to be prevented. Methods like encryption, cutting, masking and hashing have to be used in order to transfer and process the data in an unreadable form. Only limited cardholder data should be stored on storage. Sensitive authentication data must not be stored after authentication.
4. *Encrypt transmission of cardholder data across open, public networks*
   Intruders exploit the misconfiguration of wireless network devices and weaknesses in legacy encryption and authentication protocols to gain access to CDE. Strong encryption and security protocols must be used to protect the cardholder data during transmission over open and public networks.

2.3 Maintain a Vulnerability Management Program

5. *Protect all system against malware and regularly update anti-virus software or programs*
   Malicious software (malware) such as viruses, worms and trojans can enter the network during approved business activities, e.g. via employee e-mail and the use of the Internet, and target to exploit system vulnerabilities. Anti-virus software has to be installed on all systems potentially affected by malicious software. The anti-virus software has to be capable to detect, remove and protect against all types of malicious software. It has to be ensured that the anti-virus mechanisms can not be disabled and are kept current, i.e. virus signature files are regularly updated and scans are executed.
6. *Develop and maintain secure systems and applications*
   Intrudes use security vulnerabilities to gain privileged access to the systems. Many of these vulnerabilities can be fixed by security patches provided by the vendors. Therefore, a process has to be established to regularly identify security vulnerabilities, rank them by risk (e.g. “high”, “medium”, “low”) and install applicable vendor-supplied security patches. Critical patches must be installed within a month after release.

2.4 Implement Strong Access Control Measures

7. *Restrict access to cardholder data by business need to know*
   The access to cardholder data must be limited to authorized personnel. Systems and processes have to be in place to control and restrict the access to the cardholder data. Access must only be granted on the base of business needs and in accordance with the job responsibility.
8. *Identify and authenticate access to system components*
   An unique identification (ID) has to be assigned to each person with access to

the CDE. Personalized IDs ensure that each individual can be held accountable for their actions. Using IDs, activities performed on critical data and systems can be restricted to authorized users only and be traced for auditing. An authentication system must be in place which implements the policies for adding, deleting and modifying user IDs and credentials. The authentication system has to effectively enforce protection, e.g. by limiting the number of access attempts and requesting regular password changes.

9. *Restrict physical access to cardholder data by business need to know*
   Physical access to systems that host cardholder data must be restricted to avoid unauthorised access to devices or data, and prevent removal or deletion of devices or hard-copies. Appropriate facility entry controls must be in place to limit and monitor the physical access to the systems of the CDE.

2.5 Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*
    All access to the cardholder data must be tracked and monitored. Logging mechanisms and tracking of user activities enable effective forensics and vulnerability management. The existence of logs in all environments allows for thorough tracking, warning and analysis in the event of a fault. Audit trails have to be implemented that link all access to the system to an individual user and allow to reconstruct events such the user access to the cardholder data and invalid access attempts. Regular reviews of logs and security events have to be established to identify anomalies and suspicious activities.
11. *Regularly test security system and processes*
    Vulnerabilities are continually discovered by both intruders and researchers. New vulnerabilities are often introduced by new software. System components, processes and custom software have to be tested regularly to ensure that security is maintained over time. Tests have to include the verification of the security controls for wireless access points, vulnerability scans of the internal and external network, penetration tests, intrusion detection and change detection for unauthorized modification.

2.6 Maintain an Information Security Policy

12. *Maintain a policy that addresses information security for all personnel*
    All personnel have to understand the sensitivity of the data and their responsibility to protect it. Strong security policies have to be enforced for the entire entity of the CDE and inform all personnel what is expected of them.

In [5], the fact that the PCI DSS 3.0 implies many changes compared to the version 2.0 is investigated. Even organisations which are already PCI DSS 2.0 compliant may encounter challenges when moving to the new version. The changes between PCI DSS 2.0 and 3.0 are identified and PCI DSS 3.0 is implemented at the example of the largest company for online payment services in Indonesia to measure an organisation's compliance level. As a result of this

research 182 new controls are identified which simplify the adoption of PCI DSS 3.0 by an organisation that is already compliant to the PCI DSS 2.0. The company was found to be 77.43% compliant to the PCI DSS 3.0 requirements. One of the recommendations in [5] is that the company should implement strict access controls to limit the access to card holder data as per PCI DSS requirement 7. The PCI Compliance Report from 2015 [6] shows that victims of data breaches struggle with establishing restricted access and access authentication more than other organisations. The report positively points out that the compliance with requirement 7 increased over the last year to 89% of all investigated companies in 2014. The compliance with requirement 8 for access authentication was at 69% in 2014. Some companies still have challenges with establishing appropriate handling of credentials (8.2) and preventing shared use of credentials (8.5).

3 Identity and Access Management for Cloud Services

With the adoption of cloud services, functions of the IAM have to be extended into the CSP. The following IAM functions are essential for the successful and effective management of identities when using cloud services [7]:

1. *Identity Provisioning and User Management*
   The existing processes for user management within an enterprise have to be extended to cloud services. Identity provisioning has to handle the secure and timely management of on-boarding and off-boarding the users of cloud services. The users of the cloud services represent either individuals or the organisation and are maintained by the CSP in order to support authentication, authorisation, federation, billing and auditing processes. The provisioning of the users for a specific cloud service has to be done with appropriate privileges and based on their roles as cloud service consumer, e.g. business manager, administrator, service integrator and end user. CSP have to provide APIs which support the provisioning of users and consumer organisations may use automated identity management solutions exploiting those APIs.
2. *Authentication and Credential Management*
   Authentication validates the credentials provided by a user. Organisations that become cloud service consumers have to invest into properly handling credential management, strong authentication and delegated authentication, and how trust is managed across multiple cloud services. Credential management involves the processes for managing passwords, digital certificates and dynamic credentials. One time passwords and strong authentication such as multi-factor authentication should be used to reduce for instance the impact of compromised password. Credentials may be stolen by various types of intrusion attempts such as phishing, key-logging or man-in-the-middle attacks. The impact of stolen credentials is fatal, data can be monitored or manipulated, and compromised valid user accounts can be used for denial-of-service attacks or obtaining root level access to VMs and hosts [8].

3. *Federation*
   Federation enables cloud service consumers to authenticate as users of cloud services using their chosen identity provider. The identity provider is an authoritative source which provides authentication of the users. The federation process requires that identity attributes are securely exchanged between a service provider and the identity provider. The service provider can be either an internally deployed application or a cloud service. Multiple federation standards exist today. The Security Assertion Markup Language (SAML) is a widely accepted federation standard and supports single sign-on (SSO). As organisations start to consume multiple cloud services, SSO becomes important in order to manage authentication across these different services consistently using a central identity provider.
4. *Authorisation and User Profile Management*
   Authorisation grants access to requested resources based on user profile attributes and access policies. The user profile stores a set of attributes which the CSP uses to customize the service and to restrict or enable access to subsets of functions of the service. For users which act on behalf of an organisation, some of the user's profile attributes, e.g. the user role, may be assigned by the organisation. The organisation is in this case the authoritative source for those attributes and owns the access control policy to be applied to the users. Organisations have to manage the profile attributes for their users of cloud service and have to confirm with the CSP based on their requirements that adequate access control mechanisms of the cloud resources are supported.
5. *Compliance*
   Cloud service consumers have to understand how CSPs enable compliance with internal and external regulatory requirements. When consuming cloud services, some of the information required to satisfy audit and compliance reporting requirements has to be delivered by the CSP.

The classification of different Identity Management Systems (IDMS) for cloud services are discussed in [9–11]:

1. *Isolated IDMS*
   A single server is used as service provider and identity provider. The system does not rely on a trusted third party for credential issuance and verification. User accounts are replicated from the on-premise user directory into the cloud environment. Using this approach introduces security exposures when sensitive data like passwords or keys are exposed into the cloud. Changes to roles and user ID removal become effective delayed as the replication occurs asynchronous.
2. *Centralised IDMS*
   The service provider(s) and the identity provider run on different servers. One dedicated server is used as identity provider for issuing and managing user identities, while any other servers are responsible for providing cloud services.

3. *Federated IDMS*
   Federation allows to manage user identities within an organisation using an on-premise user directory. Users of federated IDMS can use the same credentials for authenticating to different cloud services. User identities are validated using tokens issued by the identity provider and presented to the cloud service interface. A cloud-based form of federated IDMS are Identity Management-as-a-Service (IDMaaS) systems. In this case, a separate cloud service manages the identity, provides identity federation with other cloud services and allows an identity to be linked with multiple cloud services.
4. *Anonymous IDMS*
   The user's identity management information is not disclosed to others during authentication and the user is kept anonymous.

4 PCI DSS Requirements for Identity and Access Management

The PCI DSS requirements impose a set of requirements related to IAM, in particular the requirements for strong access control are related to the IAM functions [2]. In [12], an approach for migrating PCI DSS compliance to an Infrastructure-as-a-Service (IaaS) provider is described. The article emphasises the shared responsibility of organisations and CSPs for ensuring PCI DSS compliance for the IAM related requirements. Typically, IaaS providers enable PCI DSS compliance at the physical infrastructure level, and support multi-factor authentication and role-based policies, while the users of the organisations have to perform the IaaS account management.

4.1 Identity Provisioning and User Management

PCI DSS requirement 8 formulates the detailed requirements for managing identity within the CDE[1] [2]:

1. All users of the CDE must receive a unique ID before allowing them to access components of the CDE or cardholder data (8.1.1).
2. Strong processes for managing the life cycle of the user IDs must be in place. User accounts must be valid and be associated with a person currently present in the organisation. Changes such as adding new user IDs, modifying or deleting existing ones must be performed under the control of these processes (8.1.2).
3. User IDs of terminated users must be revoked immediately (8.1.3).
4. User accounts which are not used within the last 90 days have to be removed or disabled (8.1.4).
5. User IDs of external vendors should only be enabled during the time period when needed and be disabled when not in use. Timely unlimited access to the CDE by vendors increases the risk of unauthorised access. The use of the user IDs has to be monitored (8.1.5).

[1] The numbers in parenthesis refer to the specific PCI DSS requirements.

6. Security policies and operations procedures for identification must be documented, in use and known to all affected parties (8.8).

4.2 Authentication and Credential Management

PCI DSS requirement 8 demands the implementation of the following authentication and credential management related features by the IAM system of the cloud services [2]:

1. Authentication to the CDE must be done by using the user ID and at least one of methods (8.2):
   (a) Something you know (password, passphrase)
   (b) Something you have (smart card, token device)
   (c) Something you are (biometric)
2. Two-factor authentication must be used when accessing the CDE from remote networks. Two of the three authentication methods above have to be used for authentication (8.3).
3. Strong processes to control the modification of credentials have to be established (8.1.2).
4. The number of attempts to use invalid credentials for an user IDs has to be limited. After not more than six attempts the user ID has to be locked out (8.1.6).
5. Once an user ID is locked out due to too many attempts with invalid credentials, the lockout duration has to be at least 30 min or until an administrator enables the user ID again (8.1.7).
6. Re-authentication is required after a session is idle for more than 15 min (8.1.8).
7. All credentials must be rendered unreadable using strong cryptography during transmission and when stored on storage (8.2.1).
8. Before the modification of any authentication credentials, the identity of the users has to be verified (8.2.2).
9. Passwords and passphrases must have a minimum length of at least seven characters and contain both numeric and alphabetic characters (8.2.3)
10. Passwords and passphrases must be changed at least every 90 days (8.2.4).
11. When a user changes the credentials of its user ID, it must to be ensured that the new password or passphrases is not the same for any of the last four passwords or passphrases used before (8.2.5).
12. Passwords and passphrases for first-time use or upon reset have to be unique for each user and must be changed immediately after the first login (8.2.6).
13. Group, shared or generic IDs and passwords must not be used for authentication (8.5).
14. Authentication policies and procedures must be documented and communicated (8.4).
15. Security policies and operation procedures for authentication must be documented, in use and known to all affected parties (8.8).

4.3 Federation

The PCI DSS does not give any explicit requirements related to federation. The identity provider for authenticating users when working with federation belongs to the CDE. In case of cloud services which are used as identity provider, the provider of the services is to be treated as TPSP from the perspective of the CDE and the requirements of the PCI DSS apply to it.

4.4 Authorisation

The authorisation functions of the cloud IAM have to support the following requirements of the PCI DSS [2]:

1. Access to the components of the CDE and cardholder data must to be limited to users whose job requires such access (7.1).
2. Based on the job responsibilities and functions, access needs and required privileges have to be defined for each user role (7.1.1).
3. The access of privileged user IDs must be restricted to the least privileges necessary to perform a job responsibility (7.1.2).
4. Access must only be assigned based on the user's individual job classification and function (7.1.3).
5. Privileges must be assigned to users according to their job classification and function, and only after documented approval (7.2.2, 8.1.1).
6. The access control system must be set to "deny all" for all components of the CDE and only grant access to users with the need to know as per their assigned role and privileges (7.2, 7.2.1, 7.2.3).
7. Direct access to the databases containing cardholder data is restricted to only database administrators. All other access to the database is through programmatic methods using dedicated application IDs. Application IDs are restricted for only the use by applications (8.7).
8. Security policies and operation procedures for restricting access to cardholder data must be documented, in use and known to all affected parties (7.3).

4.5 Compliance

In order for cloud services to be conform with the PCI DSS, the following mechanisms for tracking user activities using audit logs have to be established [2]:

1. All user access to cardholder data must be logged (10.2.1).
2. All actions taken by an user with root or administrative privileges must be logged (10.2.2).
3. All access to audit logs must be logged (10.2.3).
4. All invalid access attempts must be logged (10.2.4).
5. All activities of user management and elevation of privileges must be logged (10.2.5).
6. The initialization, stopping or pausing of the audit logs must be logged (10.2.6).

7. Creation and deletion of system-level objects must be logged (10.2.7).
8. User identification, type of event, date and time, success or failure identification, origination of the event and identification or name of the affected data, system component or resources must be logged at least for each of the above events (10.3).
9. Time-synchronization of all clocks must be implemented to ensure events captured in different logs can be correlated (10.4).
10. Audit logs must be secured so that they can not be altered (10.5).
11. Audit logs must be reviewed regularly, and in particular all security events and logs of critical components daily (10.6.).
12. Audit logs must be retained at least one year, with a minimum of three month to be available immediately (10.7).
13. Security policies and operation procedures for monitoring all access to network resources and cardholder data must be documented, in use and known to all affected parties (10.8).

5 IAM Methods for Cloud Services

Methods for cloud IAM are investigated by multiple authors. In [13], a model for identity and trust management in cloud environments is proposed. In this model, both CSP and users have to register to a trusted authority and obtain a certificate access token. By validating the user's certificate, the CSP can be sure that the user's request comes from an authentic source. A high performance IAM system on the base of OpenStack Keystone is proposed in [14]. An intrusion tolerant identity provider is described in [15] and an approach for federation and SSO on the base of claim-based identity management is discussed in [16].

Strong user authentication is a requirement of the PCI DSS. The methods published in [17,18] are described below in detail. In [17], a method is proposed which combines different security features such as identity management, mutual authentication and session key agreement between users. Based on two-factor authentication and two different communication channels, the following authentication flow is described:

1. A smart card is issued to the user. The data on the smart card is encrypted using secret numbers for both the user and server.
2. The user logs into a terminal using a smart card, user ID and password. The authenticity of the user is verified based on the smart card, user ID and password.
3. The user sends from the terminal a login request to the cloud server.
4. The cloud server generates a one-time key and calculates some hash string.
5. The cloud server sends back the hash string to the terminal.
6. The cloud server sends the one-time key to the mobile phone of the user via SMS.
7. The user enters the one-time key into the terminal and the key is validated based on the hash string and data on the smart card.

8. An authentication request is sent to the cloud server using the data of the smart card, the user ID and the one-time key.
9. The cloud server checks if the maximum legal time of an authentication session is not yet passed.
10. The cloud server calculates the validation data based the authentication request and verifies the user's identity.
11. The cloud server authenticates the user by calculating a session key which is sent as a hash string back to the user's terminal.

Methods with communication via two channels and authentication using additional one-time keys are already used by some financial institutes today. The proposed method enhances these existing mechanisms by combining them with additional flows for user and server authentication and secure encoding of messages. The method fulfils the PCI DSS requirement 8.3 to use two-factor authentication when interacting with cloud services within the CDE from remote networks. In order to use the method in a PCI DSS compliant environment, the other requirements for authentication and managing credentials must be satisfied as well. The methods assumes that the user's password is only stored on smart card. In this case, the terminal software would have to ensure that the requirements for password such as minimum length and difference from previous passwords are ensured.

Another method focusing on strong user authentication is proposed in [18]. The suggested model uses virtual device authorisation (VDA) and adds an authentication agent to the user's web browser. VDA is a Software-as-a-Service (SaaS) application that acts as an gateway to other cloud services. The VDA is used to identify the ownership of private devices and to establish the linkage between the clients and the cloud services. A cloud service user may register multiple devices in the VDA for either temporary or permanent authentication to communicate with a cloud service. During the registration of a device, approval is obtained that the device is allowed to access the cloud service and the unique access code of the authentication agent is generated by the VDA using the device's MAC address, the access type (permanent or temporary) and an user-provided passcode. The authentication agent is sent to the client and installed into the user's web browser. When the user makes a request to a cloud service, the authentication agents confirms the identity of the user based on the passcode. Once the VDA receives confirmation about the identity of the user, the VDA validates the authorisation of the device. With the proposed method, a CSP can restrict the access to cloud services for only approved devices and users. The method leaves it open to establish further mechanisms for user authentication for each of the cloud services. The method implements a form of two-factor authentication (1. something you have - an uniquely identified and approved device and 2. something you know - the user's passcode) and addresses therefore requirement 8.3 of the PCI DSS. As with the other authentication method described previously, it is necessary to also establish mechanisms to satisfy the other PCI DSS requirements for authentication and credential management. For instance, a re-registration of each

device will be required at least every 90 days, as the passcode is used for generating the unique code of the authentication agent.

6 Conclusions

In this article, the PCI DSS was analysed for the IAM specific requirements and how they are related to the use of cloud services. Two existing methods for authenticating cloud services were analysed. Both methods fulfill the PCI DSS requirement 8.3 for two-factor authentication. With respect to the IAM related requirements of the PCI DSS, it was found that current research primarily focuses on the requirements for strong authentication. Further research needs to be done for establishing effective methods that address the other PCI DSS requirements for IAM in cloud environments.

References

1. Third report on card fraud, European Central Bank, February 2014. https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf
2. Payment Card Industry (PCI) Data Security Standard Version 3.2, April 2016. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf
3. Shaw, A.: Data breach: from notification to prevention using PCI DSS. Colum. JL Soc. Probs. **43**, 517 (2009)
4. PCI Data Security Standard (PCI DSS) 3.0 Information Supplement: Third-Party Security Assurance, August 2014. https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf
5. Shihab, M., Misdianti, F.: Moving towards PCI DSS 3.0 compliance: a case study of credit card data security audit in an online payment company. In: 2014 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 151–156, October 2014
6. PCI Compliance Report, Verizon 2015. http://www.verizonenterprise.com/pcireport/2015/
7. Kumaraswamy, S., Lakshminarayanan, S., Stein, M.R.J., Wilson, Y.: Domain 12: guidance for identity & access management v2.1. Cloud Secur. Alliance (CSA), **10** (2010)
8. Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. **13**(2), 113–170 (2014)
9. Habiba, U., Abassi, A., Masood, R., Shibli, M.: Assessment criteria for cloud identity management systems. In: 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 188–195, December 2013
10. Ma, X.: Managing identities in cloud computing environments. In: 2015 2nd International Conference on Information Science and Control Engineering (ICISCE), pp. 290–292, April 2015
11. Understanding and Selecting Identity and Access Management for Cloud Services, Securosis, June 2013. https://securosis.com/assets/library/reports/Understanding_IAM_For_Cloud_Full.pdf
12. Ensuring PCI DSS Compliance in the Cloud, Cognizant (2014). http://www.cognizant.com/InsightsWhitepapers/Ensuring-PCI-DSS-Compliance-in-the-Cloud-codex879.pdf

13. Nida, Teli, B.: An efficient and secure means for identity and trust management in cloud. In: 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA), pp. 677–682, March 2015
14. Faraji, M., Kang, J.-M., Bannazadeh, H., Leon-Garcia, A.: Identity access management for multi-tier cloud infrastructures. In: 2014 IEEE Network Operations and Management Symposium (NOMS), pp. 1–9, May 2014
15. Barreto, L., Siqueira, F., Fraga, J., Feitosa, E.: An intrusion tolerant identity management infrastructure for cloud computing services, In: 2013 IEEE 20th International Conference on Web Services (ICWS), pp. 155–162, June 2013
16. Singh, A., Chatterjee, K.: Identity management in cloud computing through claim-based solution. In: 2015 Fifth International Conference on Advanced Computing Communication Technologies (ACCT), pp. 524–529, February 2015
17. Choudhury, A., Kumar, P., Sain, M., Lim, H., Jae-Lee, H.: A strong user authentication framework for cloud computing. In: 2011 IEEE Asia-Pacific Services Computing Conference (APSCC), pp. 110–115, December 2011
18. Fatemi Moghaddam, F., Khanezaei, N., Manavi, S., Eslami, M., Samar, A.: UAA: user authentication agent for managing user identities in cloud computing environments. In: 2014 IEEE 5th Control and System Graduate Research Colloquium (ICSGRC), pp. 208–212, August 2014