International Conference on Renewable Energies and Power Quality
(ICREPQ'16)
Madrid (Spain), 4th to 6th May, 2016
Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, No.14 May 2016

Security issues in cloud-based Smart Grid applications

Berthold Bitzer, Enyew Gebretsadik
South Westphalia University of Applied Sciences
Department of Automation Technologies
Lübecker Ring 2, 59494 Soest, Germany
Email: bitzer@fat-soest.de

***Abstract*— The restructuring process in power systems leads to future systems as smart grids for the usage of more renewable instead of classical nuclear power plants. In this area information communication and computation systems are playing a major role in monitoring and controlling applications in smart grid so that reforming the energy delivery system. In smart grid a vast amount of data is collected from every angle of the energy delivery network, from customer energy meters, energy generation units in the customer premises and third party players. This bi-directional information flow needs appropriate communication ways and the collected data has to be processed in a reliable, distributed, parallel and scalable computing resources. To address this demand cloud computing has a good potential and is considered to be a part of future solution. As a result several cloud-based smart grid applications are developed and being implemented. However, because of its nature of a shared pool of resources, cloud computing security and privacy are of particular concerns. Especially when it is used in sensitive area like electric utility applications. In this paper the security of cloud computing applications for power system is analyzed. The available security measures will be surveyed.**

***Index Terms*—Cloud Computing Security, Smart Grid, Cloud Computing**

I. INTRODUCTION

Utilities, network operators, demand response providers and customers are involved in today's smart grid to ensure the efficient delivery of energy where it is needed most. Bi-directional energy and information exchange takes place to enable smooth operation and reliable energy delivery system. Enormous amount of online and offline information is collected by these players for different uses. Processing and computing these data in time enables efficient monitoring and controlling of resources, directing energy to where it is most needed, make technical or administrative decisions and smooth operation of the energy delivery network. The coordinated information exchange and active participation of all the players who have roles in the power system operation is vital in minimizing down time and satisfy the customers need in terms of energy consumption management, predictions and quality energy delivery.

These smart grid applications are computation and data intensive which need a distributed, scalable and cost effective computation system only the likes of cloud computing can accommodate. However, with the internet providing the backbone for smart grid applications and their online presence highly exposed them to cyber-attacks that potentially disrupt power supply [3]. These threats may lead also for further evil activities that cause severe damages on the power delivery system. In this paper the feasibility study of the cyber-threats of cloud computing based smart grid application will be conducted and the possible counter measures to eradicate those threats will be investigated.

II. CLOUD COMPUTING

According to National institute of standards and technology (NIST) [1][2] cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." The computing resources can be networks, servers, storage, applications, and services. Cloud based systems are a sharing of an enormous amount of Information Technology (IT) infrastructures, such as computational and database resources in the form of service, which focus on maximization the efficiency of operation, scalability, maintainability and reliability by decreasing cost. These resources are provided in three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2] [6]. According to [5] a single cloud computing data center might have storage and computing capabilities tens or hundreds of times greater than all of the world's supercomputing facilities combined.

Cloud Computing can be divided into three categories according to their deployment model in which each of them do have different security levels [11][15][17][21].

- **Public Cloud:** A cloud in which service providers offer their resources as services to the general public. Public clouds offer several key benefits to users, including no initial capital investment on infrastructure and shifting of risks to infrastructure providers. However, public clouds lack fine-grained control over data, network and security settings, which hampers their effectiveness in

many business scenarios. The cloud services are accessible to everyone via standard internet connection. For instance Amazon AWS, Google, Microsoft Azure and etc…

- **Private cloud:** Also known as internal clouds, private clouds are designed for exclusive use by a single organization. A private cloud may be built and managed by the organization or by external providers. A private cloud offers the highest degree of control over performance, reliability and security. However, they are often criticized for being similar to traditional proprietary server farms and do not provide benefits such as no up-front capital costs. For instance, many organizations adopt their own private Cloud Computing these days, such as Sun Microsystem, Siemens AG and Oracle [17].
- **Hybrid cloud:** A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds. In this model users typically outsource non business-critical information and processing to the public cloud, while keeping business critical services and data in their control.

Fig. 1 shows the summary of cloud computing categories and their corresponding security levels.

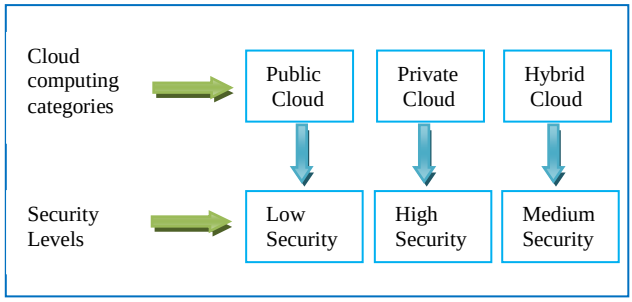

Fig. 1 Cloud Computing Categories and their security level

Some of public cloud computing services providers' security considerations are stated in [17] are presented as follows: -

Amazon Web Service (AWS)

In terms of security, Amazon Virtual Private Cloud (VPC) is a secure and seamless bridge between a company's existing IT infrastructure and the AWS Cloud. Amazon VPC enables enterprises or users for security matter to connect the existing infrastructure to a set of isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing management capabilities such as security services, firewalls, and intrusion detection systems to include their AWS resources [18]. Amazon also uses multi-factor-authentication method to provide users multiple authentications methods to access their data [22].

Microsoft Windows Azure

Microsoft has designed the Azure platform with security in mind, building in a number of different security features. An important aspect of securing data is verifying the identities of those who request to access it. Microsoft has .NET Access Control Service, which works with web services and web applications to provide a way to integrate common identities. Applications determine whether a user access is allowed [19].

Google Cloud Platform

Google has a reputation for highly reliable, high performance infrastructure, with Google cloud platform one can take the advantage of years of knowledge that Google has run massively scalable and performance driven systems. In terms of security, privacy and data protection policies apply to Google's applications and App Engine applications. Google cloud platform has taken several measures to protect the customer´s code and application data [20], such as secure service APIs, Authenticated Access and Data Encryption.

Fig. 2 summarizes some of the public cloud computing providers and some of their corresponding security measures.

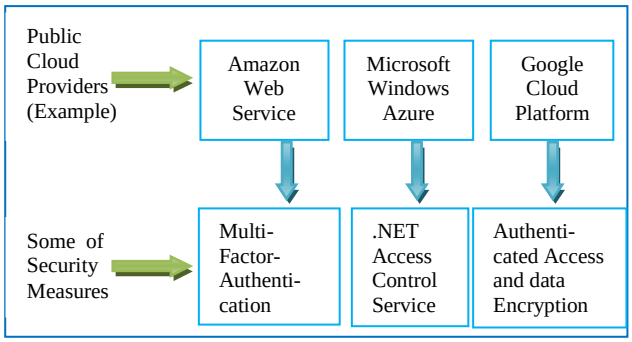

Fig. 2 Some of Public Cloud platforms and their security measures

In migrating application to a cloud infrastructure, there are different challenges to face such as security, Service Level Agreement (SLA) management, regulations and scalability. Sometimes it may not necessary to move everything to the cloud. For an enterprise providing an active social community networks, which experiences growth on its storage and computing infrastructure, public cloud computing is good enough for their operation. For critical infrastructures that demand high workload and security public cloud may not be enough by itself. Organizations and large enterprises which have invest heavily in datacenter and that have concerns with security and compliance regulations should take private cloud computing as an option.

III. Security and Privacy in Cloud Computing

Cloud computing system has two parts, the client side and the cloud side, which are connected through internet [7]. Cloud providers own a large number of networked servers with low expenses. This infrastructure consists of massive pooled systems that are linked together and works with virtualization techniques to provide a high performance of data storages and runs along-side with a local network connection that can runs from a few to

trillions of computations per second depending on the demand. The client initiates the process by sending a service request. The client service request is executed after the system management finds the required resources. At the end the execution results are sent to the client.

Security and privacy is the main concern in cloud computing [7] [11]. The virtual computing environment in cloud computing system require the user to transfer data throughout the cloud which further causes a security and privacy concerns [8] [10]. These privacy and security threats are summarized as follows:-

Information Security: - focuses on the availability, confidentiality and the integrity of data. The user may lose control of the data as the data is out sourced to the cloud. Unauthorized access also causes the question of data integrity. Another issue is that the failure of cloud providers to properly secure portions of its infrastructure result in the compromise customer data [7]. Access control to sensitive data is difficult to realize in public cloud computing because localization of data is not possible. Protecting data in the application, platform and infrastructure level is not possible in a conventional ways. Protecting data integrity, availability and confidentiality is one of the critical aspects of cloud computing security [12].

Network Security: - security issue may rise when a data is transferred from client to the cloud and at time of inter cloud data transfer through available networks. These attacks to the network can be [7],

- ***Distributed Denial of Service attack (DDOS)*** in which a user is denied the access to certain services due to high network traffic that brought the network down,
- ***Man in the Middle Attack*** in which the attacker makes direct connection with the victims and relays messages between them making them believe that they are taking each other,
- ***IP Spoofing*** scenario when an intruder gain unauthorized access by creating TCP/IP packets using somebody else's IP addresses,
- ***Port Scanning*** and ***Packet Sniffing***

Cloud malware injection attack: - the injection of malwares service, application or virtual machine into the cloud system [12].

Account and service hijacking: - the control of cloud provider infrastructure by hacking into a web site that is hosted in cloud service provider and secretly installing their software [12].

Violation of compliances: - the fulfillment of all legal requirements may not be met as cloud provider's process data in their own convenience and in their specific jurisdictions in all countries around the globe [9].

Insecure application programming interface: - unsecured APIs may case a security problems as cloud service providers depend upon API to deliver services to their customers [12] [16].

Bankruptcy of providers and subcontracting: - data centers or platforms may be transferred to third party because of bankruptcy or providers may undertake subcontracting part of the services without the knowledge of the user so that there is a risk data is not protected [9].

Abuse and nefarious use of cloud computing: - the use of the available computing power of cloud's infrastructure to attack any target by spreading malware and spam [12] [16].

General Security issues:-there are also other concerning issues regarding cloud computing. one of them is unknown ***Data Location*** in which most of the time the providers doesn't reveal the exact location of the data centers, the data flows are indefinite and sometimes the software the providers process and store the data isn't clear so that there may be a violation of privacy laws [7], ***Data Sanitization*** where the user wants to remove important information from the cloud platform and database after termination of contract and completion of cloud computing operation [7] [12] [13].

IV. Privacy and Security in Smart Grid

The traditional power system operation is known for its privacy and regulatory matters. Which is a contradictory culture to the resource pooling and sharing of cloud computing. However the growth of smart grid application for consumers forces the electric utilities to share electricity usage and operational information with external services [3]. The third party service providers are another entities involved in data and information exchange in today's smart grid systems. While planning to deploy smart grid application to the cloud computing a proper definition of the level and the type of information to be exchanged must be outlined. The question, which type of data has to be shared, what level of access is provided for each party, has to be clearly answered. As the communication between the cloud computing and smart grid domain is mainly through internet protocols, they can be easily exposed to cyber-attacks. These attacks may not only cause the power disruption but also power theft and altering energy usage information. So the privacy and security issues of the implementation of smart grid application in cloud computing platforms need further study and investigation.

Major participants in smart grid, their roles, security and privacy concerns which are shown in Fig. 3 are analyzed in [3].

A. Consumers

These are participants consume electric energy and they can be either Residential, Commercial or Industrial consumers each of them participated in data and information transfer in different level with the utility depending on their demands. Some are willing to share data and involve in demand response scheme set out by the utilities. These information from the user may be energy usage, type of equipment used, production level in which the knowledge and use of the information for malicious activities against the consumer in any way

possible by external parties may cause a negative impact to the consumer.

B. Utilities

Utilities are the back bone of the smart grid systems. In cloud-based smart grid application utilities are forced to push measurement data from the user, process and store it in the cloud. Handling this sensitive information in a shared pool of resources may expose for different attacks and the violation of regulations, privacy and security of the customers.

C. Third party service providers

In addition to consumers and utilities, in today's smart grid third party service providers' involvement is very common providing different range of services to the consumers and utilities. However, regulatory norms may restrict smart grid data to flow out of the utility infrastructure and hence require the third party providers to deploy the services within the sandboxed environment provided by the utility in the cloud. This causes the privacy concerns for their proprietary products.

To implement a secure smart grid applications in cloud computing platforms the following security requirements has to be fulfilled:- cryptographic and key management, compliance and audit, identity and access management, security policies, security incidents management, risk analysis and management, addressing vulnerability in virtualization, portability and interoperability, security awareness and training [12]. The most important protection goals in cloud computing platforms are confidentiality, integrity, availability, authenticity, accountability, and pseudonymity and privacy protection [15]. According to [14] the following predefined security goals have to be established to implement a cloud-based smart grid applications and services.

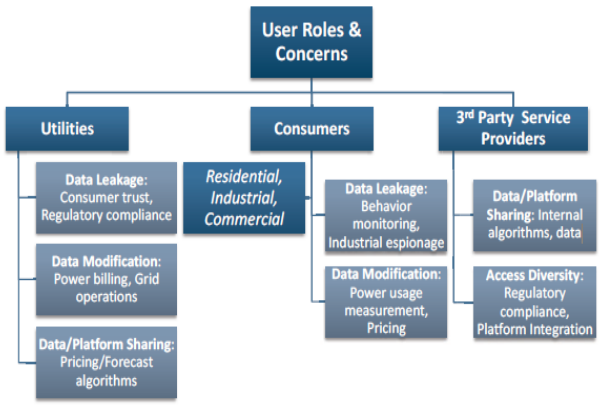

Fig. 3 User roles and their security concerns in a Smart Grid [3]

Confidentiality: - the confidentiality characteristic requires authorizations to ensure that information cannot get into the possession of subjects who don't have the appropriate rights [15]**.** In smart grid information is considered highly sensitive and needs to be guarded from unauthorized access, use or modification. Especially in public cloud platforms where information and data is processed in shared services [14].

Integrity: - Data, messages and information are considered to have integrity if they are trustworthy and cannot be tampered with [15]. In smart grid the content of the data has to be persistent, accurate and consistence though out the communication channels. The data generated from the smart grid has to be accurately transferred, processed and stored in the cloud and vise versa [14].

Authenticity: - information is authentic if it can be reliably assigned to the sender, and it can be proved that this information has no longer been changed since it was created and distributed [15] it is the process of ensuring the data source is trusted and an authorized. To insure authenticity cryptographic methods such as Message Authentication Codes, digital signatures can be used [14].

Availability: - the system has to operate satisfactorily at any point in time. Power outages or other similar incidents shouldn't affect customers, the system and data should be available even in these situations [14].

Accountability: - this requires actions to be clearly assignable to an actor in the system and ensures that the authorship of an event or action in the system cannot be rejected [15].

Privacy: - in smart grid protection of users information is very important. Different information is collected from the end user in which the protection of privacy is crucial. This information can be user's electric consumption profile, electric loads and machines used. Storing this information in public cloud may violet the privacy of the customers. Therefore, privacy represents an important requirement for cloud-based smart grid applications [14].

Access Control: - as the cloud computing stores the data in a shared environment it is very important that to identify whoever accessing to the data and any service provided and to place data access policies. In the Smart Grid sensitive data and information is transferred and communicated between measurement units, sensors, actuators and control stations. It is a must to allow access to this information for authorized personnel only.

Table **I** summarizes the predefined security goals in smart grid applications.

Table I summary of predefined security goals in smart grid applications

No.	Predefined security goals in smart grid	Characteristics
1	Confidentiality	Unauthorized access
2	Integrity	Trustworthy and cannot be tampered
3	Authenticity	Not altered
4	Availability	Available at anytime
5	Accountability	Authorship is known
6	Privacy	Protection of information from 3rd party

7	Access Control	Access only for an authorized personnel

V. MITIGATION MEASURES

Cloud computing providers have to implement a security control to maintain the customer's data security, privacy and compliance to necessary regulations. Both providers and users need to come to an agreement to include a business continuity and data backup plan in case of security breach. To eradicate in full or to reduce the concerns of cloud computing security and privacy several mitigation procedures, method and actions has to be taken until the cloud computing system has a better security and privacy protection in place.

Technical measures: - possible technical practices to avoid any attack against information, network, servers and several resources in the cloud computing systems are:-

a) *Open Authentication (OAuth):-* is a method for publishing and interacting with protected data and provides users access to their data while protecting account credential. It also allows users to share part of their data to the service provider [7].

b) *Multifactor authentication (MFA):-*it is a security system that requires more than one method of authentication from independent categories of credentials to verify the cloud user's identity for access. It simply adds an extra layer of protection on top of user name and password [22] [23].

c) *Security Assertion Markup Language (SAML):-* it is an XML-based standard for communicating authentication, authorization and attributes information among communicating partners [7].

d) *Physical security:* - the physical security of cloud computing systems encompasses the facilities and building services in which cloud computing systems are located [15].

e) *Transport Layer Security (TLS) and Secure Socket Layer (SSL):* - are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP [7].

f) *Public Key Infrastructure:* - it is an integration of procedures, programs, technical mechanisms, policies and cryptographic mechanisms to enable a wide range of users to communicate in a secure and predictable fashion [24].

g) *OpenID and open decentralized standard for user authentication and access control.* It allows user to log onto many services using the same digital identity [7].

Administrative measures: - before implementing applications in cloud computing a well organized analysis and assessment of the safety measures of the cloud computing provider has to be in place and these assessments are provided in [9]. Fig. 4 shows the summary of administrative measures that have to be taken to ensure a secure cloud computing service planning, operation, management, audit and proper termination.

a) **Planning phase: -** developers need to consider some certain criteria in order to implement or deploy an application to the Cloud computing, such as :-

- How critical is the application?
- What security level is required?
- How is the average peak load of the application?
- What type of specifications (CPU, Memory, storage, bandwidth) does the application need?
- How wide is the bandwidth between the user and the cloud computing provider?
- How much data does the user send and how often?

In this phase the detail of security analysis of the provider has to be studied. Assess the provider's data centers, facilities for limiting the public cloud to certain regions. Control options for the data flow and the services offered. Which data protection law apply and the user requirements for different alternatives needs to be included in this phase.

b) **Contract phase: -** a well narrated contract has to be prepared. The aim of this phase is to agree on a complete and verifiable terms of reference or Service Level Agreements (SLA) to ensure the quality and information security in cloud. In this agreement the following, but not limited, issues are included, the audit rights, the definitions of measurable indicator for availability, performance, confidentiality and integrity, security monitoring and handling of incidents and finally the arrangements for the termination of cloud services.

c) Deployment phase: - in this phase the planning and creation of security concepts considering the deployment and the operation phase is taking place. The deployment and testing of data outsourcing carried out according to the established security concepts.

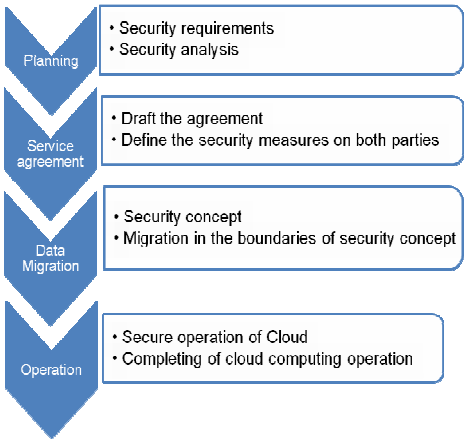

Fig. 4 Cloud computing service planning and management for secured operation [9]

d) Operation phase: -the operation has to be takes place according to the contract and the predefined security concepts. Security monitoring needs to be carried out in this phase and quick safety actions needs to be taken accordingly in case a deviation is detected from agreed level.

e) Termination phase: - the termination also takes place based on the contract agreement. The provider must delete the data and has to prove the user the data is not restorable.

Table II Summary of security problems and the corresponding possible counter measures

No.	Security Problem	Possible Counter Measures
1	Information Security	Open Authentication, MFA, SAML, Public Key Identification, OpenID
2	Network Security	Transport Layer Security and Secure Socket Layer
3	Account and Service hijacking	Public Key Identification, OpenID, MFA
4	Violation of compliances	Proper Audit of compliances in administrative measure
5	Bankruptcy of Providers	Administrative measures
6	Data Sanitization	Proper termination of contract which can be included in administrative measures

Table II summarizes the security problems and the corresponding possible counter measures. Both the administrative and technical security and privacy measures can be used to easy the security and the privacy threats imposed by out sourcing data to the cloud computing and using different resources of the cloud computing framework for several sensitive applications and infrastructures.

VI. CONCLUSION

In today's information driven smart grid different parties of players are involved to optimize the overall energy delivery network. Utilities, network operators, demand response providers and customers have to work hand in hand in order to obtain the smart grid we are envisaged. This further requires bi-directional energy and information exchange to enable smooth operation and reliable energy delivery system. Huge amount of online and offline information need to be exchanged among them and enormous data are collected by these players for different uses.

To help the power system industry in processing, computing and storing of such big data, researchers are looking for different solutions. Cloud computing is one of the proposed solution which is expected to provide a platform for future smart grid applications. It is indicated that cloud computing can provide a clean, highly reliable, elastic, distributed and scalable computing resources to host smart grid applications. However, the security issue in cloud computing environment especially in public cloud is a big concerns to deploy a critical infrastructures' data and information such as the likes of smart grid to a platform where computation systems, data storage and services are shared among several users around the globe. In this paper the security threats in cloud computing is surveyed, the security requirements that have to be fulfilled before deploying a smart grid application to the cloud is indicated and the possible mitigation technique and procedures are suggested. It is highly recommended to demonstrate the proposed methods and solutions with actual cloud-based smart grid application before a full scale implementation in real smart grid.

REFERENCES

[1] Peter Mell and Timothy Grace "The NIST Definition of Cloud Computing" NIST Special publication 800-145 Sep, 2011.

[2] George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367.

[3] Y. Simmhan, A. Kumbhare, B. Cao and V. Prasanna "An analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds" *University of Southern California , Los Angeles CA 90089*, cloud computing IEEE international conference 2011.

[4] Kenneth P.Birman, Lakshmi Ganesh, and Robert van Renesse "Running smart Grid control software on cloud computing architectures" *Department of Computer Science, Cornell University, Ithaca NY 14853*.

[5] Xi Fang, Satyajayant Misra, Guoliang Xue and Dejun Yang "Managing Smart Grid Information in the Cloud: Opportunities, Model, and Applications", Arizona State University, Tempe, AZ, USA, IEEE vol.26, p.32-36, 2012.

[6] John Viega and McAffee, "Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.

[7] L.Ertaul, S.Singhal, and G.Saldamli, "Security challenges in Cloud Computing".

[8] James F. Ransome and John W. Rittinghouse, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

[9] http://www.computerwoche.de/a/ratgeber-it-sicherheit,2363872 accessed on 1st October 2015.

[10] John Harauz, Lori M. Kaufman and Bruce Potter, "Data Security in the World of Cloud Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4, pp. 61-64.

[11] A. Malik, M. Nazir, "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences, Vol 3, No.3, pp.390-394March 2012, ISSN2079-8407.

[12] A.Younis, M. Merabti and K. Kifayat "Secure Cloud Computing for Critical Infrastructure: A Survey", School of Computing and Mathematical Sciences, Liverpool John Moores University, UK, ISBN: 978-1-902560-27-4, 2013.

[13] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in ASIACCS '10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 282–292.

[14] B.Genge, A.Beres and P. Haller, "A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids" UPEC2014, Cluj-Napoca, Romania.

[15] W.Streitberger and A. Ruppel, „Cloud Computing security, protection goals, Taxonomy, Market review" Fraunhofer Research institution AISEC, published on 25 Sep 2009.

[16] S. Srinivasamurthy and David Q. Liu, "Survey on Cloud Computing Security", Indiana University-Purdue University Fort Wayne.

[17] Remeo Ravelonjanhary, "Cloud Computing" master thesis submitted to *Westphalia University of Applied Science Department of Automation Technology, 2010*.

[18] Amazon Elastic Compute Cloud Getting Started Guide

[19] http://www.microsoft.com/windowsazure/windowsazure/

[20] https://cloud.google.com/security/ accessed on 26 Oct 2015

[21] Community Clouds supporting business ecosystems with cloud computing, Siemens IT Solutions and Service, Siemens 2010. http://www.sourcingfocus.com/uploaded/documents/Siemens_Community_Clouds_Whitepaper.pdf Accessed on 13 Oct 2015.

[22] https://aws.amazon.com/iam/details/mfa/

[23] https://azure.microsoft.com/en-us/services/multi-factor-authentication/

[24] H. Kharche and Deepak S. Chouhan, “Building Trust In Cloud Using Public Key Infrastructure” International Journal of advanced computer science and applications, Vol. 3, No. 3, pp. 26-31, 2012.