March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

Integrated Cloud Security Model for Cloud Based Power Monitoring Environment

Leoderic P. Serami[1],Thelma Palaoag [2]

[1] King's College of the Philippines, Bambang, Nueva Vizcaya, Philippines, [2] University of the Cordilleras, Baguio City, Philippines

Article Info
Volume 83
Page Number: 4751 - 4758
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 27 March 2020*

Abstract

Cloud Computing (CC) is the on - demand delivery of computing power, database storage, applications, and other IT resources via pay as you go internet cloud services platform. Due to its various advantages, CC is taking center stage in electrical power providers. However, security threats and attacks are mostly one of the problems due to CC's popularity in electrical grid agencies. The main objective of this study is to propose a security model that would prevent threats and attacks in cloud based power monitoring platform. Due to the lack of resources to gather data regarding common threats and attack in cloud based power monitoring, the researchers used Systematic Literature Review (SLR) as the method to come up with the appropriate solution for the proposed security model. Dedicated server deployment model was also used to create the proposed security model. Experts in the field of network security and smart system verified the acceptability of the proposed security model if it is feasible to use in cloud based power monitoring systems.

Index Terms: *Cloud Computing, power monitoring, security attack, security threats*

I. INTRODUCTION

During this Internet era, cloud computing (CC) apps became popular. The advent of this technology has made all things possible in business, such as outsourcing an information system's resources (N. Khan, 2018). According to the National Institute of Standards and Technology (NIST), CC is a model for enabling invisible, convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be successfully delivered quickly and released with minimal management effort or service provider interaction. This cloud model consists of five key features, three service models and four deployment models.

As a new computing model running on the Internet, cloud computing provides numerous new IT-based solutions and benefits to many organizations, such as moderate cost, agility, and high efficiency (K. Gai & S. Li, 2012). It is obvious that the use of cloud computing in many industries to improve business processes is a hot topic.

As stated in a feasibility study entitled "A Feasibility Study of the Platform as a Service Using Cloud Computing for a Global Service Organization," the use of cloud computing technologies to achieve value has become a popular approach for current companies (K. Gai, 2014). However, many companies have difficulty determining whether cloud-based services should be used and how cloud-based services can be leveraged to add value to their products or services. The key contribution of this research is that it provides a concrete example of a feasible approach to creating an effective strategy for using a cloud-based platform for small or medium-sized enterprises. Most development work and risks migrate to the cloud provider compared to the traditional software development process. Cloud

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

clients ' main task is to identify where the value can be added by leveraging cloud computing technologies and developing an appropriate strategy in the overall business process. Also, they found it beneficial for the company to use IT-based solutions. Business processes can be enhanced from an internal perspective through IT enabling. The agency would be able to maintain a positive financial status with the improvement of business processes and customer relationship. In the financial perspective, IT enablement can improve the cost structure, increase asset utilization, expand revenue opportunities and increase customer value. Improvements from different perspectives suggest that long - term shareholder value could be gained by the agency (K. Gai, 2014).

CC infrastructure can also be used in a power grid system. According to an existing research of CC, CC began to be deeply involved in grid sector globally, power grid agencies adopt CC models in their virtual power monitoring systems not only to take advantage of CC cost effective, CC provides computing solutions for intelligent management of the power grid. Emerging the cloudy platform of all levels in power grid enterprise will be gathered into online monitoring and service analysis system in the smart grid (J. Wang & C Li; N. Chaichi, et al, 2015).

In addition, CC has three major models such as public cloud, private cloud and hybrid cloud deployment models. Each model has its own characteristics, as the public cloud is open to the public. One of the advantages of the public cloud is that it can be larger than a private cloud and remove all the risks from customer shoulder to provider. One of the disadvantages of the public cloud is security and privacy issues that are resolved in private cloud; the primary purpose of the private cloud is to give the institution more control over resources, their data and security. In this model, the institution, a third party or a combination of them can own and manage the cloud infrastructure. The hybrid model is simply a combination of various private and public clouds, some in - house resources provided, and others provided third - party throw – out (C. Mukundha & K. Vidyamadhur, 2017; T. Diaby & B. B. Rad, 2017).

CC also has three major service models and these are Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS). IAAS provides on - demand access to infrastructure resources, including servers, storage devices or network devices, pay - as - you - use access. In addition to infrastructure, PaaS also provides developers with an operating system (e.g., Windows Azure). SaaS provides a software provided by a vendor and made available for public use (e.g., Gmail, and Hotmail), which is usually delivered through a public cloud provider (A. Akande et al., 2013; T Diaby & B. B. Rad, 2017).

Many electric suppliers nowadays provide virtual power monitoring where suppliers and customers can interact conveniently. New power monitoring environment and communication technologies have been introduced in many years using information and communication technologies such as Smart Grid (SG) and Web - Based Power Monitoring. In SG, a vast amount of data is collected from every corner of the energy delivery network, from customer energy meters, energy generation units in the customer premises and third party players (B. Bitzer, 2015; R. Campbell, 2018).

Since CC is an Internet driven technology, it also brings many benefits and disadvantages for the power monitoring systems (A. Apostu et al., 2015; A. Apostu et al., 2014; J Shayan et al, 2013). The benefits include cost efficiency, collaboration, increased flexibility, increased availability, and reduced impact on the environment and user satisfaction (S. Ayob, 2016; S. Müller, 2015; A. Dar & D. Ravindran, 2018).

Existing researches on CC usage in power monitoring only focuses on CC frameworks,

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

security and implementation, and there is a lack of studies that explicitly focus on the benefits and challenges of CC adoption and usage in the power grid context, particularly in electric suppliers and electric cooperatives. However, there are still problems faced with such technological phenomena. Online power monitoring security threats are persistently innovative. These threats are evolving continuously to find new ways of stealing and harming the existing systems. These threats are also growing rapidly online (P. Suryateja, 2018; A. Javaid, 2013). There are some types of threats directly or indirectly related to the power monitoring system such as threats to viruses, spyware threats, Trojan threats, and denial of service. One of CC's biggest disadvantages is security and confidentiality (H. Ahmed, 2014). In addition, data privacy and security are major concerns for every cloud user as well as cloud providers, as mentioned in the study entitled " Security Threats On Cloud Computing Vulnerabilities " Thus, understanding these concerns and how they can be addressed systematically is really important (T. Chou, 2013; N. Kajal et al, 2015).

The researchers' objectives in this paper are: 1) to identify the security threats and attacks commonly faced with cloud based power monitoring system; 2) to propose a security model to prevent the common threats and attacks in a cloud based power monitoring environment; and 3) to evaluate the acceptability of the proposed security model in cloud based power monitoring environment. A systematic literature review (SLR) was used to provide information and analysis on the research objectives. SLR is essentially a process in which the researcher identifies, assesses and interprets all available literature and empirical evidence in an attempt to provide answers for specific research questions.

II. RESEARCH METHODOLOGY

In this study, the researchers used a Systematic Literature Review (SLR) to gather topics and information to support the research. A Systematic Literature Review (SLR) identifies, selects, and critically appraises research in order to answer a clearly formulated question. The systematic review should follow a clearly defined protocol or plan where the criteria are clearly stated before the review is conducted.

The dedicated server deployment model was used to create the proposed security model for the cloud based power monitoring environment. Dedicated server deployment consists of routers, switches and servers. For public Internet connectivity, the service provider will connect to multiple Internet service providers (ISP). In addition, some service providers will provide a private network between customer servers for remote management and private network communication.

An evaluation was also conducted to assess the acceptability of the proposed security model. 9 IT experts in network security and e-learning platform made the evaluation of the model. The standard used was ISO/IEC 25010:2011 to determine the acceptability of the proposed security model. The following table shows the measurement of the Likert tool.

Scale	Average Range	Description
1	0.0 - 1.0	Not Accepted
2	1.1 - 2.0	Accepted
3	2.1 – 3.0	Highly Accepted

Table 1. Likert Scale for the Acceptability of the Proposed Security Model

The not accepted description means the created security model is not accepted as a security mechanism for a cloud based power monitoring environment. Accepted for standard security mechanism and highly accepted for beyond standard security mechanism.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

III. FINDINGS AND DISCUSSIONS

A. Threats in Cloud Based Power Monitoring Applications

This part shows the threats faced in cloud based power monitoring applications based on the SLR.

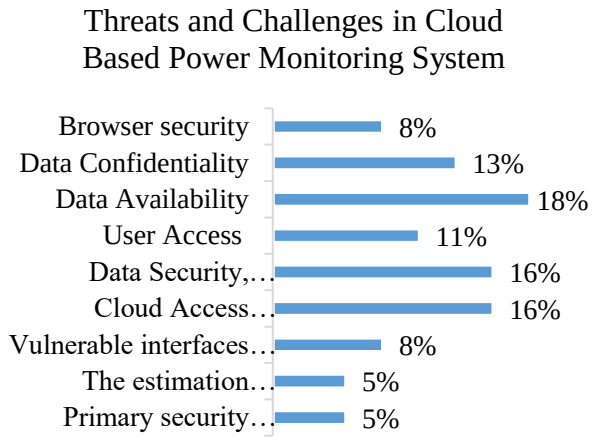

Fig.1. Percentage of Threats and Challenges in Cloud Based Power Monitoring Applications

• Primary Security Considerations. In the system, the attention or management of running standards is required regarding the usefulness of the assets as they are shared with third party customers. Most services are not similar to those from cloud systems in characterizations. Therefore, when transferring utility services from cloud devices to different exceptional systems, it will come across a little subject.

• The Estimation Process for Applications in Security System. It is a process that plays a vital role in deploying any innovative step for cloud process protection orientation and utility. It has priority based features and involves organizing new methodologies that are conducive to secured purposes.

• Data Breaches. A data breach is an incident of security in which information is accessed without permission. Infringements of data can hurt businesses and consumers in various ways. They are an expensive expense that can harm lives and reputations and take time to repair them. It is the deliberate or unintentional release to an untrusted environment of secure or confidential information. Cloud providers organize security rules to protect their environments. Organizations themselves are ultimately accountable and responsible for protecting their own cloud information or data. Data integrity, security of storage, data backup and maintenance policies are considered as key solutions for avoiding cloud data breaches.

• Vulnerable Interfaces and APIs. Cloud providers often use a set of APIs to create an interface for their customers to communicate with cloud services. Every cloud service and utility provides APIs. Customers and IT companies use these communication interfaces. Inappropriate use of interfaces will result in threats such as transmission of content material, clear - text authorization, erroneous authorization, etc. due to the fact that interfaces will be the system's uncovered thing. Because of these threats, cloud services such as IaaS, PaaS and SaaS will affect. This can be eradicated by using a suitable protection technique for the interface of cloud providers and by providing a successful authentication method.

• Cloud Access Methods Security Issues. Cloud computing is based on the online disclosure of resources. In the case of web applications–SaaS: (1) SOAP, REST and RPC Protocols. In the case of web services and APIs – PaaS and CML APIs: (2) remote connections, VPN and FTP. In the case of VMs and storage services – IaaS, these resources can be opened via (3) web browsers (HTTP / HTTPS). Security controls should target those protocol - related susceptibilities to protect and ensure data transfer between the cloud platform and consumers.

• Data Security, Privacy & Control Risks. Data security and privacy risks are mitigated by data encryption and the handling of these rudimentary risks is the responsibility of the CSP. The storage provider should offer encryption schemes and

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

scheduled data backups to ensure data integrity, confidentiality and availability.

• User Access. The customer is fully responsible for managing all security controls of the software. These include control of application access, IAM, patching software, protection of viruses. One of the risks is how a customer faces CSP's privileged status and security issues such as eliminating fault, damaging data, and migrating data.

• Data Availability. Clients no longer have data on the cloud when the client data is uploaded into the cloud. Personal data and information about the Cloud of the customer, if not available either lost or heck, the original data is difficult to recover.

• Data Confidentiality. For users to store their private or confidential data in the cloud, data confidentiality is important. To ensure confidentiality of data, authentication and access control strategies are used. Cloud computing issues of data confidentiality, authentication, and access control could be addressed by enhancing cloud reliability and confidence.

• Browser Security. Every application process assignment in the cloud system needs to take the centralized servers. Since the browsing system is the only tool that customers can use cloud service, it is more important to frame and design modem web browsers with certain security mechanisms standards.

B. Security Attacks in Cloud Based Power Monitoring System

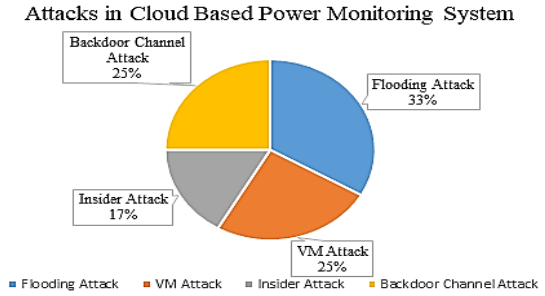

Fig. 2 Percentage of Attacks in Cloud Based Power Monitoring System

• Flooding Attack. A flooding attack is a type of denial of service (DDoS) attack aimed at making a server unavailable to legitimate traffic by consuming all available server resources. The attacker can overwhelm all available ports on a targeted server machine by repeatedly sending initial request for connection (SYN) packets, causing the targeted device to slowly or not at all respond to legitimate traffic.

• VM Attack. This attack actually occurs in the IaaS Service layer of any cloud based application. According to A. Duncan et Al., Low-Technology and Higher-Technology attacks are the two types of VM attack. These attacks allow attacker to attack the client data without detecting.

• Insider Attack. This attack means that any target system has a legitimate access or knowledge of the attacker. According to Infosec, this is the common threat to security for an organization that uses cloud services. As mentioned, insider attack caused nearly 40 percent or 75 percent of security threats in the cloud system.

• Backdoor Channel Attack. This attack is a method to bypass any security mechanism to enter a network by bypassing the "front door". This is the most common method to collect data from a target system. According to NetSkope Inc. on "Cloud Report" dated February 2018, attackers can take advantage of existing legitimate backdoor or install their own after initial hacking to use them for future attacks.

C. Proposed Security Model

The following figure shows the proposed security model of the cloud based power monitoring environment. The different elements of the proposed model are also discussed.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

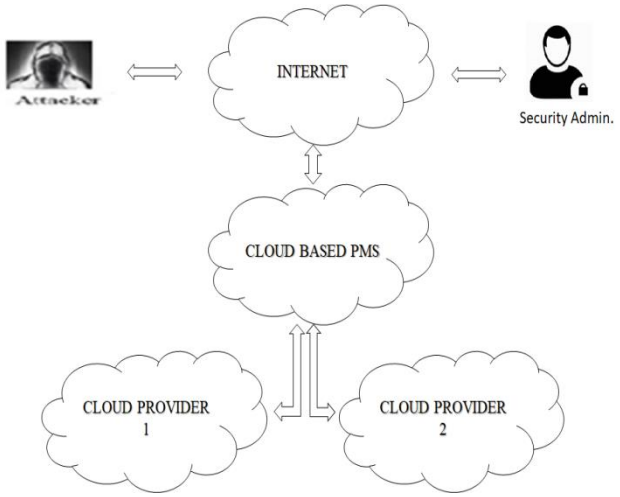

Fig. 3 Proposed Security Model

• Client. Client represents the personnel assigned to access the services of the cloud based power monitoring system. The client could only open the power monitoring application from the cloud through entering its own authentication like username and password.

• Attacker. Attacker is the other term for hacker or intruder. Hacker is the one that has gained unauthorized access from the cloud. Attacker is hacking to gather information and perform malicious activities from cloud-based power monitoring application. This can be accomplished by populating security attacks such as indoor attack, flood attack, VM attack, and BDC attack.

• Cloud Security of the Cloud Power Monitoring. This cloud is the repository the power monitoring security mechanisms. This is one of the best strategies to protect cloud-based power monitoring, which means that this cloud can prevent any intruder who wants to gain access from the cloud-based power monitoring application being published. Aside from having typical security mechanism in the cloud based power monitoring system, additional preventive measures should be applied.

a) Tunnel Web Application Firewall. A web application firewall (WAF) is a HTTP application firewall. In an HTTP conversation, it applies a set of rules. These rules generally cover common attacks such as cross - site scripting (XSS) and injection of SQL.

b) SSL/TSL. The SSL successor protocol is Transport Layer Security (TLS). TLS is an upgraded SSL version. It works much the same way as the SSL, using encryption to protect data and information transfer.

c) Rate Limiting. Rate Limiting is used to control incoming and outgoing traffic to or from a network. For example, let's say you use the API of a specific service that is configured to allow 100 requests per minute. If that limit exceeds the number of requests you make, an error will be triggered. The rationale behind the implementation of rate limits is to enable better data flow and increase security by mitigating attacks like DDoS.

d) 2FA. Two - factor authentication (2FA), sometimes referred to as two - stage verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves in order to better protect both the credentials of the user and the user's access resources. Two - factor authentication provides a higher level of assurance than one - factor authentication (SFA) methods in which the user only provides one factor - typically a password or passcode. Two - factor authentication methods rely on users providing both a password and a second factor, usually either a safety token or a biometric factor such as a fingerprint or facial scan.

e) Hardware ID. The Hardware ID (HWID) is a set of numbers and letters (only capital letters) that identify your computer uniquely with any of our software. The HWID consists of eighteen (18) characters e.g. 098H52ST479QE053V2 and is used to unlock the software on a computer. The software activation process uniquely identifies a given computer through proprietary mechanisms (HWID). This HWID is linked to certain computer hardware elements such as Hard Disk ID, CPU ID and BIOS Info. When one of the software is first running on a computer, it runs in trial (unregistered) mode and displays a dialog.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4751 - 4758

f) Fail Over/Load Balancer. Failover is an operational backup mode in which secondary system components assume the functions of a system component (such as a processor, server, network, or database, for example) when the primary component becomes unavailable by either failure or scheduled downtime. The procedure involves automatically unloading tasks to a component of the standby system so that the procedure is as seamless to the end user as possible.

Prevention Tools	Threats in Cloud Based Power Monitoring	Attacks in cloud Based Power Monitoring
Tunnel Web Application Firewall	Data Breaches, Browser Security	Backdoor Channel Attack, Insider Attack
SSS/TSL	Data Security and Privacy	Insider Attack
Rate Limiting	User Access	Flooding
2FA	User Access, Data Confidentiality	Insider Attack
Hardware ID	Data Breaches	VM Attack
Fail Over or Load Balancer	User Access	VM and Flooding Attacks

Table 2. The Prevention Tools Used for the Proposed Security Model

• Cloud Region. This is one way to protect the cloud-based power monitoring application. This means the other cloud is the other alternative in using the power monitoring application once the other cloud has failed due to any threat. This is also an easy way for the client to access the cloud-based power monitoring service.

• Security Admin. The Internet is full of cyber threats from hackers who want to steal and sell corporate data on the black market. In order to protect against these cyber threats, security roles are more important than ever. Security administrators are the first step in defending and monitoring a company for suspicious activity either inside the local network or outside Internet traffic. Security administrators have a distinct ability from other IT administrators, making the job a stressful yet rewarding career.

D. Evaluation of the Proposed Model

Experts evaluated the proposed security model. The result of their evaluation has the mean rating of 2.97, which means that the model was deemed highly acceptable. This implies that the model can be implemented to different electric providers that use Cloud-based power monitoring environments.

IV. CONCLUSION

Cloud based power monitoring applications provides ease for electric providers to enhance their power monitoring experience by being able to receive services that can be accessed at their most convenient time without no worries. There are many benefits of using cloud computing such as cost efficiency, improved accessibility, and etc. However, there are still threats that are faced affecting the affectivity of cloud computing in power monitoring environment. These threats include data breaches, data integrity and privacy bypass, browser security, and etc. On the other hand, there are tools that are already existing to prevent these threats to happen like IPS, IDS, and NIDES and other external preventive tools. Though, in order to enhance the functionality of CC in power monitoring, a new security model was proposed. This model has been evaluated with a high acceptability rating and it is recommended that this should be imposed in cloud based power monitoring environment.

REFERENCES

[1] N. Khan, "Cloud Security Threats and Techniques to Strengthen Cloud Computing Adoption. Cyber Security and Threats: Concepts, Methodologies, Tools, and Application," University of Salford, Uk, pp. 18, 2018

[2] K. Gai and S. Li, "Towards Cloud Computing: A Literature Review on Cloud Computing

Published by: The Mattingley Publishing Co., Inc.

and Its Development Trends," Institute of Electrical and Electronics Engineers, 2012

[3] K. Gai, "A Feasibility Study of Platform-as-a-Service Using Cloud Computing for a Global Service Oranization," Journal of Information Systems Applied Research, Vol 7, pp. 28-42, 2014

[4] Jianjun Wang, Cunbin Li, "Design of an Online Monitoring System for Intelligent Power Network Based on Cloud Computing Technology," pp. 1473-8031, ISSN 1473-804x online

[5] Nina Chaichi, Joal Lavoje, Sopheil Zarrin, Rafaa Khalifa, Felix Sie, "A Comprehensive Assessment of Cloud Computing for Smart Grid Applications: A Mulitiple Perspectives Framework," Management of Engineering and Technology (PICMET), 2015 Portland International Conference on IEEE, pp. 2541-2547, 2015.

[6] Dr. Chinthagunta Mukundha, K. Vidyamadhuri, "Cloud Computing Models : A Survey. Advances in Computational Sciences and Technology," ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 747-761, 2017

[7] Tinankoria Diaby, Babak Bashari Rad, "Cloud Computing: A review of the Concepts and Deployment Models," I.J. Information Technology and Computer Science, 2017, 6, 50-58, 2017

[8] Berthold Bitzer, "Application of Cloud Computing for Power Systems," Engineering and Industry Series. DOI:10.22618/TP.EI.20151.192018, 2015

[9] Akande, A.O., N.A. April, and J.-P. Van Belle, "Management Issues with Cloud Computing," Proceedings of the Second International Conference on Innovative Computing and Cloud Computing. ACM, 2013

[10] Anca Apostu, Florina Puican, Geanina Ularu, George Suciu, Gyorgy Todoran, "Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud," Recent Advances in Applied Computer Science and Digital Services. ISBN: 978-1-61804-179-1, 2015

[11] J Shayan, A Azarnik, S Chuprat, S Karamizadeh, "Identifying Benefits and Risks Associated with Utilizing Cloud Computing" The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, 2013

[12] Sether, Ayob, "Cloud Computing Benefits," 10.13140/RG.2.1.1776.0880, 2016

[13] Müller, Sune & Holm, S.R. & Søndergaard, Jens, "Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. Communications of the Association for Information Systems" 37. 10.17705/1CAIS.03742, 2015

[14] Richard J. Campbell, "The Smart Grid: Status and Outlook.," Congresional Research Service. 7-5700, 2018

[15] Dar, Ab & Ravindran, Daks, "A Comprehensive Study On Cloud Computing," International Journal of Advance Research in Science and Engineering. Vol. 07. PP. 235-242, 2018

[16] Suryateja, Pericherla, "Threats and Vulnerabilities of Cloud Computing: A Review," International Journal Of Computer Sciences And Engineering. 6. 10.26438/ijcse/v6i3.298303, 2018

[17] Javaid, Adeel, "Top Threats to Cloud Computing Security," SSRN Electronic Journal, 10.2139/ssrn.2325234, 2013

[18] Hamza Ahmed, "Cloud Computing Security threats and Countermeasures," International Journal of Scientific & Engineering Research, Volume 5, pp. 206-215, 2014

[19] Te-Shun Chou, "Security Threats On Cloud Computing Vulnerabilities," International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, pp. 79-78, 2013

[20] N. Kajal, N. Ikram and Prach, "Security threats in cloud computing," International Conference on Computing, Communication & Automation. pp. 691-694. doi: 10.1109/CCAA.2015.71484, 2015