A Defensive Measure of Cloud Server Security with Brief Solution

Sultan Anwar, Abdullah Al Mamun, Hassan Ali

Collage of Computer Science & Engineering
King Fahd University of Petroleum and Minerals
Eastern Province, Dhahran 31261, Saudi Arabia

Abstract *— the cloud computing is one of the rapid growing technology in IT industry during the past couple of years. Customers can access their data from anywhere in the world by using internet. Many of the large companies are offering cloud services nowadays. Security and protection of user data and processes is one of the major concerns in the cloud computing environment. This paper provides a brief introduction of cloud computing, various aspects of cloud model as well as service layers, security threats and challenges. Also provides a comprehensive classification of different threats with respect to various levels of cloud servers. This paper also aims to explore the underlying server level attacks and its defensive measures to cope with them. The security of the cloud computing environment requires further development and improvement by both industrial and academic researchers.*

Keywords *— Cloud Service Provider (CSP), Intrusion Detection System (IDS), Domain Name Server (DNS), Distributed Denial of Service (DDOS), Border Gateway Protocol (BGP).*

I. INTRODUCTION

Cloud computing is an internet based technology where data is maintained and stored in the centralized data center of a Cloud Service Provider (CSP). There are many reasons that IT solution providing companies are moving towards cloud computing environment. They get paid for the resources which their customers use on the basis of usage. There is a competition involved between different organizations and IT solution providers. Everyone wants to make sure that they be leading edge for their customers [1]. Many large companies like CNN, Amazon, eBay, Google, Microsoft are providing cloud services. But on the other hand, many of the standards like reliability, privacy and inter-operability still need to be defined. Industrial and academic researchers are participating with new solutions and ideas. Security is also one the major concern in cloud computing due to very less control on data. This results in many security threats and issues like information leakage, confidentiality, integrity and availability. Many companies had to shut down their services due to inability to tackle properly with the security threats and issues. Hence, it is very important for a CSP to keep in mind the security aspects of cloud computing. This paper focuses on server level security of cloud and its defensive measures. It is organized as follows: Section II gives a brief introduction of Cloud. Section III addresses a different aspect of cloud model and its layers. Section IV throws light on cloud computing benefits. Section V outlines some of the cloud computing challenges like Comfortibility, Confidentiality, Integrity, Availability etc. Section VI discusses about cloud computing security threats and also provides classification of threats on different levels of cloud. Section VII discusses about DDOS attack, as it affects the whole server, which in turn results in affecting all the layers of cloud. Section VIII gives a brief intro of IDS to cope with the aforementioned attack and discusses in tabular format some of the latest proposed methods with their pros and cons. Finally, Section 8 concludes the study.

II. WHAT IS CLOUD AND WHY

Cloud Computing is getting dominant in IT and business industry nowadays. It is an Internet based computing in which Virtual servers are shared and provide services such as resources, infrastructure, and software and platform devices [2]. The main purpose of Cloud Computing is that the consumers use only what they want and where ever they want. It also aims at reducing the cost of operation and maintenance of any software service. Cloud Computing clients need not to have the physical infrastructure themselves; rather they get these services as rent from third party. This also decreases the cost of maintenance and infrastructure. There are two things that cloud service providers should assure all the time: 1. Connectivity and 2. Availability; if there are not met, the whole organization will suffer with high costs [3]. However, with the information security point of view Confidentiality, Integrity, Assurance and Transparency are also important factors that need to be considered [4].

III. SERVICE MODEL OF CLOUD

Service model of cloud should be divided into five layers as shown in Figure 1:

A. Client

This is the top most layer of the Cloud. It comprises of hardware and software of any form that should support cloud computing. Forcing a car driver to fly an

aero plane will not work. Result is a big disaster. Hardware can be computers, notebooks, net books, tablets, mobile phones, other devices and software in the form of Operating Systems like

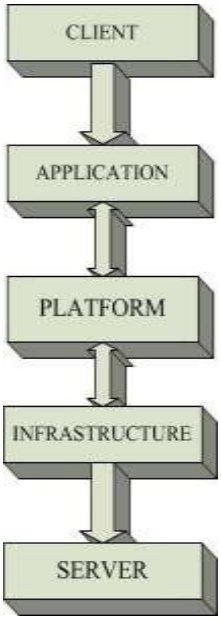

Fig. 1 Layered Service Model of Cloud

Microsoft, Android, Google Chrome OS, Linux or Browsers like Opera, Internet Explorer, and Chrome etc.

B. Cloud Application

This is the second layer of the cloud. Application related services of Cloud are found here. We can get access of those services and applications via hosted desktop, remote client or browser. It eradicates the need of running and installing the application on consumer's computer and thus eliminates the burden of ongoing operation, support services and software maintenance.

C. Cloud Platform

This is the mid layer of the Cloud. Computing Platform as a Service is provided by this layer. Computing platform makes changes in the server's settings and configuration according to a surge in demand. It sends configuration settings in the upper or lower layers according to the type of services provided by CSP. Also acts as a means of communication for upper and lower layers.

D. Cloud Infrastructure

The second last layer of Cloud is Cloud Infrastructure. The function of this layer is to provide IT infrastructure by using Virtualization. Virtualization means distributing or piercing a piece of hardware which can be scaled in terms of RAM, Disk, CPU and other components. Virtualization is the formation of a virtual version and not the actual version of Hardware platform, operating system, network resources or storage devices. These are then interlinked with others for resilience and additional capacity [5]. This will result in benefits to the clients; rather than buying software, servers, network equipment or space; clients use these resources as a completely outsourced service. The amount of resources consumed will typically reflect the level of activity and cost.

E. Server

The last layer of cloud computing is the server layer. This layer provides computer hardware/software products that are explicitly designed for the delivery of cloud services. They may include cloud-specific operating systems, applications, platform, multi-core processors or the any combination of the above. There are other service layers as well, such as Hardware as a Service - HaaS, Communication as a Service - CaaS, Security as a Service - SECaaS, Monitoring as a Service - MaaS, Storage as a Service - STaaS, Desktop as a Service - DESKaaS, Compute Capacity-as-a-Service - CCaaS, Database-as-a-Service - DBaaS, IT-as-a-Service - ITaaS, Business Process-as-a-Service - BPaaS etc. These are not part of actual service model of cloud. These are the extended services as shown in Table 1. Depending on the services provided by CSP they become part of a basic 5 layered model. For Example CSP wants to provide DESKaaS to clients. We will need support of application layer because DESKaaS will be an application as a deliverable. And we know that application layer provides application related services. DESKaaS related services will extend basic application layer. Moreover, DESKaaS will also be needing support of Infrastructure Layer to provide Virtualization environment. So DESKaaS's virtualization related services will extend Infrastructure Layer as well as shown in Figure 2. The Platform Layer will provide DESKaaS's computing configuration related services in the upper and lower layers. Finally, server will provide DESKaaS product as a delivery to clients.

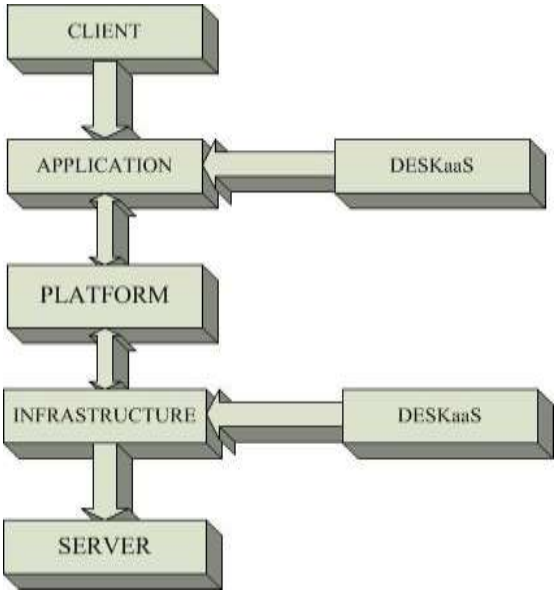

Fig. 2 DESKaaS Model

TABLE I
SUMMARY OF CLOUD LAYERS AND SERVICES

Layers	Services
Client	Client Requirements
Cloud Application	Application as a Service AaaS
Cloud Platform	Platform as a Service PaaS
Cloud Infrastructure	Infrastructure as a Service IaaS
Server	Actual Service Provider
Extended	- HaaS - CaaS - SECaaS - MaaS - STaaS - DTaaS - CCaaS - DBaaS - ITaaS -BpaaS

IV. MAJOR CHALLENGES

Cloud computing on one hand has lots of benefits and advantages but on the other hand faces many challenges too. Some are as follows:

A. Comfortability

One of the largest concerns of the Cloud Computing is security. Users are not comfortable in handing their data to third parties, as it is kept on their servers. Although a lot of companies entitle that their servers are free from any type of malwares and threats, but still it's a great concern because different people from all over the world have access to the server.

B. Confidentiality

Confidentiality is also another major concern that affects Cloud Computing success. It is very important for CSP to ensure the customers that their data/information will be kept confidential. Sensitive or any private information will not be accessed by any individual other than him.

C. Integrity

It is very important to ensure that information be modified only by authorized persons in any cloud environment. [8]

D. Availability

Availability means the cloud services should be up and running for all the time. The consumer gets required services whenever and wherever he wants.

E. Accountability

Accountability means holding responsible for any destructive behavior on a cloud. For example, if some disaster occurs due to which data is lost or damaged. Who will be held responsible consumer or CSP? Both blame each other. It should be ensured that we are able to keep track all events going on in cloud for later auditing purposes [9] [10].

F. Transparency

Details of the server need not to be known to the clients e.g. the location of server, capacity, configuration etc. Since they are interested only in the services that provided by CSP. [4]

G. Less Control of Data

Data or Information can only be accessed when cloud services are up and running along with internet connection. So, you have less control over your own data. It is the responsibility of CSP to provide services 24/7. Moreover, feasibility analysis should be done; Services should be designed and provided in accordance with the capacity of bandwidth available in the respected zone or area.

V. SECURITY AND THREATS

Security is one of the major concerns in cloud computing. There are many studies which classify security threats in cloud on the basis of different

service models in a cloud environment. [11] Classifies the cloud attacks based on Confidentiality, Integrity and Availability of data along with the existing defensive measures. Based on the discussion in [12] [13] breaches can occur at different levels of cloud. Attacks affect the application, network and server levels [14]–[18] as described in fig 3. So security is needed at various levels of cloud. They can be classified as follows:

Fig. 3 Classification of Threats

A. Application Level

The application level security attacks are defined in the Table II. Some of the application level attacks are browser specific.

B. Network level

Some of the network level security attacks are defined along with their functionality, preventive and defensive measures in the Table 3.

TABLE III PART-ANETWORK LEVEL ATTACKS AND DEFENSES

Attack	Method	Defensive Measure
BGP Hi-jack	This protocol is attacked when an incorrect advertisement of IP addresses related to the Autonomous system (AS) is done. Also it is found due to bad AS.	Secured AS.
Sniffing	Captures network packets flowing through the network and reads the information in it if it is not encrypted.	Encrypt data. Sniffing detection based on RTT and ARP [20]
DNS	When a user tries to access server, it routed to some others cloud/server.	Use DNSSecu Extensions.

TABLE II APPLICATION ATTACKS AND DEFENSES

Attack Name	Method	Browser Specific	Defense
CAPTCHA Breach	CAPTCHAs are developed to prevent exploitation and unsolicited messages.	Yes	Use multifaceted backgrounds, Increase string length, Overlap letters,
Cookies Poisoning	Manipulation of cookies to achieve unauthorized access.	Yes	Use Web based Firewalls, use encryption. Regularly clean cookies.
Backdoors	An script is written onto applications that creates backdoor to gain unauthorized access.	No	Debugging options must be disabled after used.
Injection Attack	A malicious code is injected. Therefore gaining access to the resources as a legitimate user while making the valid users wait.	Yes	List applications that customers usually run, properly utilizing FAT.
Virtual Machine	Due to the vulnerabilities in the Virtual Machine Manager (VMM).	No	Monitor the guest VMs, minimizing information leakage. [19]
XSS	A malicious piece of code is injected and user considering it to be legitimate executes it on his machine.	No	Avoid hitting unknown links using mouse, use Active Content Filtering.
SQL Injection attacks	A malicious code injected into standard SQL code.	Yes	Use Parameterized Queries, Validate the type and format.
Man in the Middle	Third party tries to listen to the information.	No	Encrypt data

ICMP Flood	Floods the target by ICMP packets resulting in consuming bandwidth.	ScreenOS (firewall)
Reused IP	When a user leaves a network, his IP address is re-issued to some other user. It may become accessible to the new user.	DNS cookies and caches should be flushed on every used.

TABLE III PART-B

C. Server level

Server level security attacks are defined along with their functionality, preventive and defensive measures in the Table 4.

TABLE IV
SERVER LEVEL ATTACKS AND DEFENSES

Attack	Method	Defensive Measure
DoS	Flooding the server with the number of requests than can't be handled.	IDS
DDoS	Target systems are attacked with the help of several compromised systems (Zombies).	IDS

TABLE V
IDS PHASES

Phases	Method		Description	Drawbacks
Detection	Misuse Detection	Signature Based	Compare similarity of the patterns with the recorded patterns.	Signature is updated frequently.
	Incongruity Detection	Machine Learning	Identify based on statistical measures.	False positive alerts.
Identify	IP Trace-back		IP Trace-back Approach	
Prevention	Block		Block traced IP's	

VI. DISTRIBUTED DENIAL OF SERVICE

This attack is done in two phases, we name them as IP^2. *i.e*. Intrusion Phase and Installation Phase. In former phase the invader tries gather zombies as much as he/she can. First tries to compromise easily targeted zombies and by the help of these; tries to compromise the difficult ones. Once all the required zombies are compromised there comes later phase in which DDOS attack tools are installed on compromised zombies in order to attack primary victims. The first documented attack was done in mid of 1999 on a computer in University of Minnesota [21]. In 2000, some of the NATO sites were attacked. Moreover servers of many popular companies like CNN, eBay, Amazon, Yahoo were also became a victim of DDOS attacks. According to the Eighth Annual Worldwide Infrastructure Security Report in 2012, 14% percent of the cloud attacks are backed by DoS attacks [22].

VII. INTRUSION DETECTION

As discussed in previous sections that DDOS attack prevents the cloud user from accessing the required set of services. One of the best methods for detection and prevention of DDOS is by using Intrusion Detection System (IDS). An IDS reports the administrator to take proper action by observing the network and system for any malicious activity. IDS are normally installed on virtual machines. However, it can also be installed on physical machines as well. By [23] IDS can be categorized as Host based Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS), Distributed Intrusion Detection System (DIDS) and Hybrid Intrusion Detection System. HIDS monitors the internal computers; attacks like system calls, file system changes and application log can be detected. However, it can be compromised by malwares – Preventing HIDS from detecting malicious activity [24] [26]. NIDS on the other hand monitors incoming and outgoing traffic over the network. Its disadvantage is its poor visibility of the internal network. Now there was problem that all these IDSs employed were single threaded. To support distributed environments, DIDS were proposed and are widely used [25]. Hybrid Intrusion Detection Systems are combination of any of the above categories. All of the above mentioned categories are implemented in the form of sensors. Table 5 illustrates different phases of IDS, respective methods/techniques along with description and drawbacks. With the passage of time, many IDS methods have been proposed to counter Server- level attacks. Table VI throws light on some of the latest methods that have been proposed along with their pros and cons.

TABLE VI RECENTLY PROPOSED IDS METHODS AND THEIR DRAWBACKS

Year	Title	Technique	Drawbacks
2008	Collaborative P2P Architecture	An IDS checks each IP packets header and saves its address along with a counter. When a counter reaches a certain limit, it means an attack has happened [27].	Setting a threshold level is not sufficient.
2009	Layered	Each layer should have both Network-based sensors and host based sensors. The IDS sensor VMs detects malicious activity and generates alerts with the help of Event Handler [28].	Complex architecture and output is not standardized.
2010	CLAD	When new connection request comes, this services checks whether that request is an HTTP request. Only http requests are allowed [29].	Good for small scale.
2011	Packet Filtering	Confidence Based Filtering method is used [30].	The cost of pre-attack processing power is high.
2012	SOA	It's an approach based on SOA. It is used to trace the source of DDOS attack. In this method all requests are sent to SBTA (SOA Based Traceback Approach). SBTA then puts traceback mark tag in the packet's header. Then this packet is sent to the Web Server [31].	Increasing number of attack packets decreases defense performance.

VIII. CONCLUSION

In this study, cloud computing with its layers, benefits, security threats and challenges are briefly introduced. Also provided a different aspect of basic 5 layer model of cloud; Other common layers like HaaS, CaaS, SECaaS, MaaS, STaaS, DESKaaS, CCaaS, DBaaS, ITaaS, BPaaS etc. are not actual layers. Depending on the services provided by CSP, these layer become part of aforementioned basic model. Extensive study of cloud computing benefits and threats is done. Security is needed at different levels of cloud. Threats to cloud computing are categorized along with their functionality and defensive measures in Tables II, III and IV. Moreover, with regards to Server Level Security, DDoS attacks are one of the most dangerous attacks on cloud as they affect other layers as well. Many methods have been proposed, but IDS is best because it can not only detect but also prevent DDOS attacks. Table V provides a view on different IDS phases. Finally, in order to help researchers, TABLE VI enlists different methods recently proposed over the past few years. Every IDS Method has some pros and cons. A proper study is needed in shaping appropriate IDS for specific cloud service or an environment. Future work is to provide cloud computing environment taking into consideration, security aspects of cloud. Security of the cloud environment requires further development and improvements by both industrial and academic researchers.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, Introducing New Services in Cloud Computing Environment, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Rabbani, Imran M., Abad A. Shah, and Muhammad Aslam. "Evolution of Cloud Computing and its Future."

[3] Perry, G., Minimizing public cloud disruptions, Tech Target, [online]. Available at: http://searchdatacenter.techtarget.com/tip/Minimizingpublic-cloud-disruptions, 2011.

[4] Kanday, Rajeev. "A survey on cloud computing security." Computing Sciences (ICCS), 2012 International Conference on. IEEE, 2012.

[5] http://searchservervirtualization.techtarget.com/definition/virtualization
(accessed in May 2015)

[6] Parameshwari, V., et al. "Cloud ComputingAn Advanced Study Using
ANFIS."Int. J. Novel. Res. Eng & Pharm. Sci 1.04: 24-28. 2014

[7] http://wwwimages.adobe.com/content/dam/Adobe/en/products/acrobat/pdfs/acrobatX it challenge.pdf, iTs next challenge: Three key trends in document collaboration and exchange Meeting knowledge workers demands in 2011 and beyond, 2011, pp.1

[8] Allan A. Friedman and Darrell M. West Privacy and Security in Cloud Computing Issues in Technology Innovation the Center for Technology Innovation at Brookings 2010.

[9] Pearson, S., Toward Accountability in the Cloud Internet Computing, IEEE, 2011.

[10] Nakahara, S.; Ishimoto, H. A study on the requirements of accountable cloud services and log management Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium, 2010.

[11] Gehana Booth, Andrew Soknacki, and Anil Somayaji, Cloud Security: Attacks and Current Defenses, 8th Annual

Symposium On Information Assurance (Asia13), June 4-5, Albany, New York , 2013, pp.56-62.

[12] K. Vieira, A. Schulter, C. B. Westphall, and C. M.Westphall, Intrusion Detection for Grid and Cloud Computing, IEEEComputer Society, Vol. 12, July/August 2010, pp.38-43.

[13] Anindita Saha1, Abhijit Das A Detailed Analysis of the Issues and Solutions for Securing Data in Cloud, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 4, Issue 5, Sep-Oct. 2012, PP 11-
18.

[14] Rohit Bhadauria and Sugata Sanyal,Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques., International Journal of Computer Applications 47(18) , June 2012, pp:47-66

[15] N Jeyanthi, N.Ch.S.N Iyengar, P C Mogan Kumar, Kannammal A
2013 An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment, International Journal of Communication Networks and Information Security, Vol. 5, No. 2, pp. 163-173.

[16] S. Roschke, F. Cheng, and C.Meinel,Intrusion Detection in Cloud, 8th IEEE International Conference on Dependable, Automatic and Secure Computing, pp.729 734.

[17] Jeyanthi, N. , Iyengar, N.Ch.S.N. 2012, "Packet resonance strategy: A spoof attack detection and prevention mechanism in cloud computing environment", International Journal of Communication Networks and Information Security, Vol. 4, No. 3, pp. 163-173

[18] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi, A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model, International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 3, March 2013.

[19] Ristenpart, Thomas, et al. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[20] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1.2 (2011): 136-146.

[21] Gary C. Kessler Defenses Against Distributed Denial of Service Attacks,
4th edition of the Computer Security Handbook, November 2000

[22] http://pages.arbornetworks.com/rs/arbor/images/WISR2012 EN.pdf,
Worldwide Infrastrucutre Security Report, vol 8, [2012] (accessed in May 2015)

[23] Sina Manavi, Sadra Mohammadalin, Nur Izura Udzir, Azizol Abdullah, Hierarchical Secure Virtualization Model for Cloud. In the Proceeding of the International Conference on Cyber Security, Cyber Warfare And Digital Forensic (Cybersec2012), pp 219-224,IEEE, June 2012.

[24] M. Laureano, C. Maziero, and E. Jamhour, Protecting host-based intrusion detectors through virtual machines, Computer Networks, vol. 51, no. 5, pp. 1275-1283, Apr. 2007.

[25] S. Ros, F. Cheng, and C. Meinel, Intrusion Detection in the Cloud, 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729-734, Dec. 2009.

[26] F. Azmandian, M. Moffie, and M. Alshawabkeh, Virtual machine monitor-based lightweight intrusion detection, ACM SIGOPS, vol. 45, no. 2, p. 38, Jul. 2011.

[27] Radwane Saad, Farid Nait-Abdesselam and Ahmed Serhrouchni, A Collaborative Peer-to-Peer Architecture to Defend Against DDoS Attacks.
In 33rd IEEE conference on local computer network, pp. 427-434, IEEE, September 2008

[28] Sebastian Roshke, Feng Cheng, Christoph Meinel, Intrusion Detection in the Cloud. In Eighth IEEE International Conference on Dependable,Autonomic and Secure Computing, pp. - 729-734, IEEE, October 2009

[29] Ping Du, Akihiro Nakao, DDoS Defense as a Network Service. In International Conference on Network Operations and Management Symposium, pp.-894-897, IEEE, April 2010

[30] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, In
Ninth International Conference on Dependable, Autonomic and Secure Computing, pp.-427-434, IEEE, Jan 2011

[31] Yang, Lanjuan, et al. "Defense of DDoS attack for cloud computing." Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on. Vol. 2. IEEE, 2012.

[32] Hisham A. Kholidy, Fabrizio Baiardi, CIDS: A framework for Intrusion Detection in Cloud Systems. In Ninth InternationalConference on Information Technology-New Generation, pp. 379-385, October 2012

Abdullah Al Mamun received his B.S. degree in Computer Science & Engineering from Dhaka University of Engineering & Technology, Bangladesh, in 2012, the M.S. degree in Computer Engineering from King Fahd University of Petroleum and Minerals, in 2016 (possible date). He was a Part time Research Assistant, with Department of Renewable Energy, Research Institute, KUPM in 2015, 2016 respectively. His research interests include Bigdata Analysis and Machine Leering. At present, He is studying MS in Computer Engineering in KFUPM.

Hassan Ali received his B.S. degree in Computer Engineering from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2013 and continuing the M.S. degree in Computer Networks form King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He was in faculty of Electrical Engineering department in Govt. College of Technology, Lahore, Pakistan in 2014. His research interests include Distributed Systems, Heterogeneous communications and Real time publish subscribe Operating systems and software. At present, He is engaged in Smart Grid communication interoperability and its standards.

Sultan Anwar received his B.S. degree in Computer Engineering from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2013 and continuing the M.S. degree in Computer Networks form King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He was an assistant DCO in Pakistan Telecommunication Co. Limited. He is a research assistant with faculty of College of Computer Science and Engineering King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. His research interests include Wireless Sensor Networks, Network Security schemes, and Geographical Information Systems. At present, He is engaged in Pipeline leak detection techniques using wireless sensing nodes.