International Journal of Grid and Distributed Computing
Vol. 9, No. 7 (2016), pp.13-22
http://dx.doi.org/10.14257/ijgdc.2016.9.7.02

Appraisal of the Most Prominent Attacks due to Vulnerabilities in Cloud Computing

Masood Shah[1] and Abdul Salam Shah[2*]

[1,2]*SZABIST, Islamabad, Pakistan*
[1]*engg.cisco@gmail.com,* [2*]*shahsalamss@gmail.com*

Abstract

Cloud computing has attracted users due to high speed and bandwidth of the internet. The e-commerce systems are best utilizing the cloud computing. The cloud can be accessed by a password and username and is completely dependent upon the internet. The threats to confidentiality, integrity, authentication and other vulnerabilities that are associated with the internet are also associated with cloud. The internet and cloud can be secured from threats by ensuring proper security and authorization. The channel between user and cloud server must be secured with a proper authorization mechanism. The research has been carried out and different models have been proposed by the authors to ensure the security of clouds. In this paper, we have critically analyzed the already published literature on the security and authorization of the internet and cloud.

Keywords*: Cloud Computing, Cloud Security, Software Platform Infrastructure (SPI), Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)*

1. Introduction

Two parties are involved in the cloud computing, one which provides services to other party known as a service provider. The second party is the user of these services, which is known as user or client [1]. The service provider charges money from the users of the services. These services are virtual, not real and can be used with the internet connection. The cloud assigns unique name and password to every client to connect to the cloud and use provided services [2]. The charges of service provider depend on the space, bandwidth, speed and level of security required. The clients are of three types, *i.e.*, mobile user, thin client (which have no personal storage or hard disk) and thick client. The data of the thin client is stored on the cloud server [3]. The thick client has its own hard disk for the storage of data, and simultaneously stored in the cloud as well. There are advantages and disadvantages of both thin client and thick client, for example the data of thin client cannot be accessed if the client machine misplaced. The drawback of thin client is that the complete data is being stored on the server. The advantage of the thick client is that the data can be accessed with rapid space as compared to the thin client which requires an internet connection to access the data [4].

There are different companies which offer cloud computing services. The Amazon has started elastic cloud computing and simple storage services in 2006. The Google has also launched cloud services. Blue Cloud launched by IBM, have a platform and data storage centers. The Microsoft has also introduced window azure in 2008 [5].

There are three types of cloud computing *i.e.*, public, private and hybrid. In the public cloud, services are public which can be accessed through the public network from anywhere. In the private cloud, the services are accessed through the private network. The

* Salam Sha is the corresponding author.

ISSN: 2005-4262 IJGDC

hybrid cloud is the combination of the public and private cloud, in which the services are private as well as public [6].

The services provided by the cloud are categorized by the Software, Platform and Infrastructure (SPI). The first layer of SPI model is the Software as a Service (SaaS). In SaaS, the user has been provided with software to use in a thin client. The second layer of the SPI model is the Platform as a Service (PaaS). In this, the service provider provides a platform to the user for developing software for use. The final layer of SPI model is the Infrastructure as a Service (IaaS). In IaaS, the user has to manage the resources such as storage, database and server [7]. The general architecture of cloud can be described as the authentication server, which authenticates the user, the second is a user, which uses the services and third is the servers that provide services to the user. The user authenticates himself through an authentication server, and after the successful authentication, the user gets permeation to use the services provided by the server [8-9].

The use of cloud is increased due to larger bandwidth and high speed of the internet. The people save their cost of storage, maintenance and security by using cloud services and pay to the service providers. The increased use of cloud has also exposed the cloud to the possible attacks from hackers and other vulnerabilities [10]. In this paper, we have carried out an appraisal of the most prominent techniques of security and authorization of the internet and cloud. The remaining paper is organized as the Section 2 contains Literature review, in Section 3 the critical analysis of the reviewed techniques is presented and finally in Section 4 the conclusion and future work of the study are provided.

2. Literature Review

According to [11], there are so many security risks for users of the cloud computing services, for handling these hazards the possible types of attacks must be categorized so that solution of that can be found [12]. The author has proposed the idea of attacks possible in the cloud computing. The organizations are providing cloud services according to the cloud computing categorization. The cloud computing is still not matured in terms of security, and most of the researchers in published literature have focused on security and new categorization attack surface. The paper focused on the initial attacks and hacking efforts linked to cloud computing organizations and their systems. In the cloud computing there are three different contributor classes as user, cloud and service. In cloud computing, two contributors must involve in the communication. The attacks can be launched on any of these three contributor classes during communication. The contributor classes must be secured with a security interface or channel between the communicating parties, which depends on the service model that cloud have adopted like IaaS, PaaS, and SaaS.

The web server has a secure SSH protocol that provides a secure channel for the communication. Total of six interfaces coordinate when all three contributor classes communicate with each other. These six surfaces are exposed to attacks as well. The most well-known surface attack in cloud computing is server-to-user attack which is more vulnerable. The other most common attacks are buffer overflow attacks and SQL injection. The service user towards the service is a type of attack which is browser based attack that uses HTML-based services example of that is SSL certificate spoofing or phishing attacks on mail clients. The resource use up is another complex type of attack, which is triggering the cloud provider or denial of services. The attacks surface cloud system and user interfaces have no actual touching ends, both of them are present in between but the cloud system has a channel which can control their services, which is known as cloud control. The cloud customer uses cloud control to add new services, change services, and delete services. The next attack surface is user-to-the cloud provider, the common attacks on this surface is phishing, which causes a user to control the cloud

provider services. The cloud organization integrates every kind of attacks besides the running service on the cloud.

Stolfo *et. al.,* in [13] discussed the techniques of storing and protecting personal and business data on the cloud environment. The cryptography techniques do not provide full security to the data. The decoy technology supervises and senses unusual data access when an illegal access is detected and confirmed so the system produces a large amount of decay data for the attacker to cut off his access to the real user data. The data theft, it is the most serious attack in cloud computing. The top threat for cloud computing by cloud security alliance is when the attacker is malicious insider and majority of user know this threat. When the private key and password of a user got stolen by an insider attacker, he can use it to access all data of the original user without any intimation to the original user.

The fog computing is the mechanism that can provide security in cloud computing. This technology is used to initiate a disinformation attack for insider attack to not understand the real data of the specific user. The cloud computing environment is not trustworthy because when an attack is launched and the data is stolen, after that there is no mechanism to bring the stolen data back. So first priority should be to minimize the data loss by implementing more secure and trustworthy security feature, For example, preventive disinformation attacks. The user behavior profiling is a method to monitor the access of normal user *i.e.,* how many times and when a user have accessed the data from the cloud. This method is normally used in fraud finding the application. The abnormal data access can be detected with the volumetric information of the normal user. The authors have used method behavior profiling and decoy for securing information. In decoys, information honeypots are used and fake data has been produced to detect the illegal entry into the cloud. The decoy information will puzzle the attacker and attacker will not differentiate between the original and fake information stored as honeypots. Both of these technologies have been applied in a local file system to detect the unauthorized access of attacker. The experiments have produced good results with both technologies.

Yang *et. al.,* in [14] described the Distributed Denial of Service (DDoS) attacks and the mechanism to recover or trace back the attack. The DDoS attacks can cause huge loss to an organization in the form of degradation. The DDoS attack on the availability of services because cloud computing is completely based on resource sharing at different levels like network, application, and host level, so DDoS is a big threat to these resources. The authors have discussed different approaches like trace back approach, which is Service Oriented Architecture for the identification of exact information of the attack on cloud, another approach is detection.

The Cloud Security Association have recognized some risk in cloud computing like neglect and dishonest using of cloud computing, malicious insider, vulnerabilities, data leakage, traffic hijacking, account service and insecure application programming interface. There are some defensive techniques for DDoS attacks like detection, identification, and filtration. For the detection of DDoS attacks wavelet spectral analysis, statistical methods and other machine learning techniques are used. The IP trace-back technique, Probabilistic Packet Marking (PPM) and the Deterministic Packet Marking (DPM) are used to identify the attack source in identification phase. The PPM has more advantages than DPM because PPM needs a reduced amount of traffic than ICMP to rebuild the path to recognizing the attack source but the negative aspect of PPM is that it requires additional calculation and packets in trace-back procedure also it may discover the incorrect source address. The DPM has been launched to overcome the weaknesses of PPM. The DPM is simple to put into service and utilize less overhead but the disadvantage is that it requires extra enough packets to recreate attack path.

The core purpose of SOA-Based Trace-back Approach (SBTA) is to trace back the actual cause of DDoS attacks in the cloud. The SBTA is positioned by a virtual machine in cloud network; it is scalable, flexible and compatible. The requests are sent to STBA for production after that put together by Web Services Description Language (WSDL) the

request messages of Simple Object Access Protocol (SOAP). The request messages of (SOAP), will be marked by STBA with a tag of cloud trace back in the header and the message of SOAP will be sent to the web server. The web server will send the response message of SOAP which will be sent back to the client by the web server as a part of HTTP response. If the message is from an attacker, the infected client can recover his cloud by the trace-back tag and can find the place from where the attack has been launched. For the defense against DDoS attacks the traffic control mechanism, ingress filtering is used to filter the traffic on route based packet. It drops the packets of IP address which is spoofed which did not be in the right place in upstream networks.

Duncan *et. al.,* in [15] discussed malicious insider which is known by every computer security industry. Whenever company's hire security-related employees like system administrator or IT security specialist, they seek reference check, family background and take interview so many times until satisfied. Even after employment the company keeps high-security checks on that employee. Despite these security checks imposed by the company, there are still vulnerabilities that trusted employee become insider attacker. The organizations use cloud computing due to the best security infrastructure. The report given by ENISA in 2009 gives the list of most significant classes of cloud definite risks [16]. The 2006 report of Eric and Shaw [17] shows that there is no such evidence of insider attacker all this is planned in advanced. The report also concluded that most of the insider events happened by the non-working experience of the specific work but although many of the attacks were considered in advance.

In cloud computing, the insider is present but the client did not know about it. The client has to rely on the service provider. The Internet Service Provider can read all the attachment and emails it has the ability to view the conversations that are not encrypted. Infrastructure as a Service basically runs the hypervisors and its manages many operating systems in a virtual machine on host operating system from which we can copy, move and backup [18]. The malicious insider can break the administrator password and can access all the data on customer virtual machine and obtain a complete history of the virtual machine. In Data Storage as a Service all the files of the users are stored on a server secured by a username and a password. But all these information are under the access of the administrator all the files can be opened and copied by the administrator. It is difficult to examine every individual file without forensic technique that can be used to observe the Metadata on upload and update.

According to Karnwal *et. al.,* [19], cloud computing is the grouping of distributed system, grid, and utility computing. These all are combined in the form of virtualization [20]. The distributed computing systems have changed the entire business on the internet. The facility of cloud can also be used by attackers like in SaaS, PaaS and IaaS, there might be some soft corners from which an attacker can launch an attack. In SaaS, the attacker can attack via the loophole in the programming interface as insecure Application Programming Interface (API) attacks on customer browser, firewall, and the account can be hacked. In PaaS the insecure application programming interface, unknown risk profiles. In IaaS the main soft corner for the attacker is data leakage in a virtual machine due to shared technology issues. These all are attacks on integrity, confidentiality and availability. So for these vulnerabilities, the paper focused on SaaS layer and application programming interface security.

For request of resource in cloud environment, the customer's uses simple Object Access Protocol (SOAP) message. The SOAP relies on some other application layers. The SOAP message is written in XML that's why it can run on any platform. The Cloud Defender filter attacks, which have five stages. The HTTP DDoS attack can be filtered with four filters *i.e.,* Sensor, Hop Count, IP Frequency and Puzzle Resolver filter [21]. The XML DDoS attack can be detected by the Double Signature Filter. For the detection of suspicious messages, the sensor is used which monitors the coming requests if there is any imaginary raised in the request message number from a specific customer then these

messages can mark as doubtful IP otherwise it will be forwarded to the next filter. But if the request message is doubtful the request message will be dropped and the IP address will be sent to IP Trace Back.

Liu *et. al.,* in [22] discussed wireless Local Area Network Security. The Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) encryption protocols are very common but they have some weaknesses [23, 24]. The predictive judgment is an attack algorithm which is tailored to the atmosphere of cloud computing. Wireless Local Area Network (WLAN) utilize wireless path as a broadcast medium and the technology radio frequency for information sending and receiving. The wireless network has security issues of identity cheating, eavesdropping, and message tampering [25]. IEEE 802.11 standard for a wireless network which is for identity verification and data encryption, it makes the wireless network more secure and enhanced. The encryption technology has been defined by IEEE 802.11 standard which gives protection to data transmission. The integrity of data is authentic and encrypted. The WPA relates to data encryption technology that provides high standard and gives good security level as of wired network. The RC4 is an algorithm used for wired network security, that is nonlinear and of the high level, it has 10 times more speed than Data Encryption Standard (DES). It enlarges the short key of the user to a particular extent N-bit stream. The RC4 is made of two algorithms Key Schedule Algorithms (KSA) and Pseudo-Random Generation Algorithm (PRGA). It is used for building sequence related key as stream cipher of code disk. The WPA Wi-Fi Protected Access is an advanced version of WEP in IEEE 802.11-2004.

Kholidy *et. al.,* in [26] discussed cloud intrusion detection dataset and masquerade attacks on cloud computing. Masquerades attack is one of the most serious attacks on cloud system because it has huge amount of resources. In cloud system for detection of masquerade attacks sequence alignment technique and semi-global alignment, the technique is used. For the improvement of some technique the Heuristic Semi-Global Alignment Approach (HSGAA) is developed that calculates the finest alignment present session to the same user training sequence. All the security parameters like firewalls or some security protocols are worthless because the attacker act like a legal user. The actions/attacks of masquerade are tampering with secret information and deletion of some serious resources, using copy illegally software, eavesdropping and spoofing other users. Many of the attacks leave some log files which are directly linked with user log analysis and host-based IDS used for detection mechanism. The audit or inspection can be done in the different environment by several profiling methods. In UNIX environment, user command list program and system calls can be used for audit. All these approaches are compared using same user datasets. In a Windows environment, the log sources are an application, system, and security. The windows applications and windows operating system correspondingly use system and application log sources. The Local Security Authority Subsystem Service (lsass.exe) writes to security log directly. The masquerades detection in network atmosphere considers user network behavior.

The Log Analyzer and Correlator System present binary log files together by Unix Basic Module, security, service log files and application of windows event log system, and the data which is in the form of raw packets. The Solaris Parser binary, event data writes to the local file system by Solaris C2 audit daemon. The audit events of files are converted to readable text format and the output is stored in the same order in the file as entered by the same user. The file is analyzed by log analyzer and correlator component. The following information is extracted, username, user id, time, day, directories, files, system Calles, session id, login source, session id, attributes and arguments for system calls. The windows parser converts the encoded windows security event, service log files and application to human readable form.

Riquet *et. al.,* in [27] discussed coordinated attacks on a large scale and its impact on the cloud. The Firewalls and Intrusion Detection System are used for security using port scan. The load balancing, virtualization management, security, and fault tolerance are

other characteristics of cloud computing. The firewall placed between two networks so that all traffic may pass through the firewall. The firewall filters authorized traffic that meets the conditions of security policy. The network-based intrusion detection system analyzes and captures different packets and detects attacks. The host-based intrusion detection system analyzes the collected information of the individual system. The distributed intrusion detection system in which raises the alarm when any intrusion is detected. The detection of attack is mostly carried out by anomaly-based detection and pattern matching. The all known patterns are detected with the signature in pattern matching. For the pattern matching, it is necessary to keep the database up to date. In anomaly base detection, an attacker can behave like a normal user, in that case, logarithmic logic is the best solution for detection of intruders. The Snort and commercial firewall are the alternative security solutions. The Snort analyses network traffic in real time on the basis of signature. The commercial firewall can work as an IDS and also a network firewall.

Khorshed *et. al.*, in [28] have highlighted some threats in cloud computing and proposed machine learning techniques for detection of threats. The shared technology vulnerabilities is a threat. In unknown risk profile the lack of transparency, for audit logs or provided unwillingly. It is noticed that some security related data are provided unwillingly to the user by the cloud provider. The user can not react to some attacks until they occur, so for this purpose, authors have suggested "Proactive Attack Detection" model. The model has two main goals, *i.e.*, the attack can be detected at the very first stage and when an attack is occurring. The model informs the user that what kind of attack is happening. The experiment with Amazon Elastic Compute Cloud (EC2), by the researcher of California University and Massachusetts Institute of Technology, has shown that there is a possibility of making the internal infrastructure of cloud and detects the location of the specific virtual machine. In that experiment attack script is generated that will be used in attacking tools, in documented attack, the information is described by security websites and different blogs. The script has many advantages including it can be run at the attacking time, and simultaneously on many virtual machines. The experiment has been carried out in a single cloud environment. Tools have been used on the basis of nature of the data. In the attack situation, the most common data has been collected from the network packets to send and receive data, *i.e.*, round trip and processing time and cup usage. For an alert generation, machine learning techniques have been used, for the known attacks. Every type of attack has a different set of attributes of the computer network system may alter. There are eight things which make the complete set are as follows, a set of packets sent, set of packets retrieved, packets lost, disk read and write data, memory usage, CPU utilization, failure counts, and admin log on have a shot.

Sqalli *et. al.*, in [29] discussed mitigation techniques and Economic Denial of Sustainability (EDoS) attacks in cloud computing. The DDOs attack can harm the economic resources of the cloud provider. The EDoS attacks can control zombies remotely, for the undesired request to cloud service by flooding. For the selected filtering the mitigation technique must be extremely intelligent, if not it can also become a utility for attackers as a source of EDoS attack. The EDoS Shield is a Novel mitigation technique. The proposed architecture has a verifier node, the requests are forward in the verifier node. The verifier node performs verification process and updates the system for a black and white list of IP address. The cloud watch is auto scaling technique by Amazon. The EDoS attacks can be mitigated by overlay base approaches, and the effect of EDoS attacks can be reduced by Cloud Watch as a control technology. The clients have to give proof of work to the server, before committing its resources to the client. The dedicated approach, for mitigation of EDoS attacks, is the Self-verification proof of work (sPoW). The V node updates the list used by the virtual firewall. If the request is verified, the source IP address request will be added to the white list. But if the request fails the IP address of the source will be added to the blacklist and all the packets will be dropped.

The attacks can be categorized into groups by Cosine Similarity Algorithm as used in [30]. The grouping will help to identify the attacks if similar kind of attack launched in future.

The strengths and weaknesses of the above reviewed techniques are summarized in the Table 1.

3. Critical Analysis

Table 1. Appraisal of Techniques

Ref.	Focus Area	Weakness	Strengthens
[11]	Attacks surface. A taxonomy for attacks on cloud services.	The attacks like denial of services, a man in middle and brute force attacks are possible in this architecture.	In the communication, the hash function is used for the integrity of the data and stopping different attacks, if user access new service then they will again authenticate with the cloud system.
[13]	For computing: mitigating insider data theft attacks in the cloud.	The attacks like a man in middle, masquerade attacks are possible in the authentication process and hackers also get information during communication of trusted authority and hardware.	The user behavior profiling and decoys provide high-level security, and by fake information, the attacker is confused. The suggested file system architecture can easily be implemented.
[14]	The defense of DDoS attacks for cloud computing.	DDoS attack is a big threat for availability and more computation is required for probabilistic packet marketing. It may also trace the wrong source address.	The virtualization techniques take much load from the client while SBTA and cloud filter is efficient in cloud computing. The service oriented architecture is compatible and scalable. Trace back the source of attacks.
[15]	Insider attacks in cloud computing.	All attacks are pre-planned and most insider attackers are motivated by financial gains due to which company is going through economic loss.	The data owner has faith on the cloud provider. Incidents can be detected by various methods and CERT and RAND classify the malicious insiders.
[19]	A comber approach for protecting cloud computing against XMML DDoS and ATTP DDoS attacks.	The XML and HTTP based DDoS attacks are common in the web-based environment and data leakage in a virtual machine.	The cloud is web based, provides shared resources and has the facility of server-based computing using the huge database and provides the pay per user advanced facility.
[22]	A predictive judgment method for WLAN attacking based on cloud computing environment.	The WLAN security is difficult to guarantee because certain algorithms which can crack the WPA and WEP. The huge capacity of users causes a major decline in	The WLAN has strong extension and TKIP and WPA2 are strong protocols while encryption provides safety controls to information broadcast and security.

		conformance.	
[26]	CIDD: A cloud Intrusion detection dataset for cloud computing and masquerade attack.	The traditional Information Technology solutions have less threat than cloud computing. For detection of masquerades basic network statistics is used but due to legal restriction host, data cannot be accessed.	The sequence alignment technique used to detect masquerades attacks focus on semi global alignment technique. The detection solutions are based on host-based user profiling. The misuse detection applies a statistical approach.
[27]	The large scale coordinated attacks: Impact on the cloud security.	In network attacks, the first phase is port scan, low-speed rate port scan is not detected by an IDS because they execute slowly. By distributed attacks, the IDS can be evaded very easily.	For protection, IDS and firewall are used. To detect large-scale coordinated attacks, collaborative intrusion detection system is introduced. The architecture specified in this paper is easily implemented but experts are needed.
[28]	The trusted issues that create a threat for Cyber Attacks in cloud computing.	Unwillingly log and audit data is provided to users by the cloud provider. Instant monitoring is restricted for cloud provider by privacy law and new loopholes are opened due to the rapid development of cloud computing.	The proactive attack detection model and machine learning techniques are introduced to detect top attacks. The system “pay as you go” provided by cloud computing.
[29]	EDoS-Shield – A two steps mitigation technique against EDoS attacks in cloud computing.	Selectively filter the malicious traffic is disastrous and cloud watch is not an efficient practical solution for EDos attacks.	Virtual firewall is used to mitigate the EDoS attacks. Verifier nodes are used for updating of the white and black list. Cloud watch as a control technology by Amazon to reduce the effect of EDoS attacks.

4. Conclusion and Future Work

The papers for this study have been selected having valuable work done on the vulnerabilities, security and authorization of cloud computing. The appraisal of the papers has revealed that still, some gaps exist in every technique, as it is understood that a single technique does not cover all the aspects of security. Every technique has few advantages as well as disadvantages from the security point of view, the security threats still exist in cloud computing. There is a need of deep research to overcome the security threats and enhance the security and strong authorization mechanism. The next step of the study will be to propose a model for the implementation of authentication mechanism for the enhancement of the security in cloud computing.

References

[1] S-T. Liu and Y-M. Chen, "Retrospective Detection of Malware Attacks by Cloud Computing", 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, **(2010)**, pp. 510-517.
[2] F. Zhou, M. Goel, P. Desnoyers and R. Sundaram, "Scheduler Vulnerabilities and Coordinated Attacks in Cloud Computing", 2011 IEEE International Symposium on Network Computing and Applications, **(2011)**, pp. 123-130.
[3] M. Uddin, J. Memon, R. Alsaqour, A. Shah and M. Z.A. Rozan, "Mobile Agent Based Multi-Layer Security Framework for Cloud Data Centers", Indian Journal of Science and Technology, vol. 8, no. 12, **(2015)**, pp. 1-10.
[4] M. Anwar, "Virtual Firewalling for Migrating Virtual Machines in Cloud Computing", 2013 International Conference on Information & Communication Technologies (ICICT), **(2013)**, pp. 1-11.
[5] http://www.businessinsider.com/why-amazon-is-so-hard-to-topple-in-the-cloud-and-where-everybody-else-falls-2015-10, Retrieved on 14-05-2016.
[6] Y. Benslimane, M. Plaisent, P. Bernard and B. Bahli, "Key Challenges and Opportunities in Cloud Computing and Implications on Service Requirements: Evidence from a Systematic Literature Review", 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (Cloud Com), **(2014)**, pp. 114-121.
[7] H. Mohamed, L. Adil, T. Saida and M. Hicham, "A Collaborative Intrusion Detection and Prevention System in Cloud Computing", AFRICON, 2013 **(2013)**, pp. 1-5.
[8] Q. Chen, W. Lin, W. Dou and S. Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), **(2011)**, pp. 427-434.
[9] D. Riquet, G. Grimaud and M. Hauspie, "Large-Scale Coordinated attacks: Impact on the Cloud Security", 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), **(2012)**, pp. 558-563.
[10] S. Raja and S. Ramaiah, "An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection", International Journal of Fuzzy Systems, **(2016)**, pp. 1-16.
[11] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services", IEEE 3rd International Conference on Cloud Computing, **(2010)**, pp. 276-279.
[12] A. S. Shah, M. Fayaz, A. Shah and S. Shah, "Risk Management Policy of Telecommunication and Engineering Laboratory", International Journal of Hybrid Information Technology (IJHIT), vol. 9, no.4, **(2016)**, pp. 281-290.
[13] S. J. Stolfo, M B. Salem and D. A. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", IEEE CS Security and Privacy Workshops, **(2012)**, pp. 125-128.
[14] L. Yang, T. Zhang, J. Song, J. S. Wang and P. Chen, "Defence of DDoS Attack for Cloud Computing", 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), **(2012)**, pp. 626-629.
[15] A. J. Duncan, S. Creese and M. GoldSmith, "Insider Attacks in Cloud Computing", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, **(2012)**, pp. 857-862.
[16] D. Catteddu and G. Hogben, "Benefits, Risks and Recommendations for Information Security," Online, 20, November 2009, http://www.enisa.europa.eu/activities/risk-management/files/ deliverables/cloud-computing-risk-assessment.
[17] D. Eric and Shaw, "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations", Digital Investigation, vol. 3, no.1, **(2006)**, pp. 20-31.
[18] A. Waqas, A. W. Mahessar, N. Mahmood, Z. Bhatti, M. Karbasi and A. Shah, "Transaction Management Techniques and Practices In Current Cloud Computing Environments: A Survey", International Journal of Database Management Systems, vol. 7, no. 1, **(2015)**, pp. 41-59.
[19] T. Karnwal, T. Sivakumar and G. Aghila, "A Comber Approach to Protect Cloud Computing Against XML DDoS and HTTP DDoS Attack", IEEE Students' Conference on Electrical, Electronics and Computer Science, **(2012)**, pp. 1-5.
[20] M. Uddin, A. A. Rahman, A. Shah and J. Memon, "Virtualization Implementation Approach for Data Centers to Maximize Performance", Asian Network for Scientific Information (ANSINET), vol. 5, no. 2, **(2012)**, pp. 45-57.
[21] A. G. Memon, S. Khawaja and A. Shah, "Steganography: A new Horizon for Safe Communication Through XML", Journal of Theoretical and Applied Information Technology, vol. 4 no.3, **(2008)**, pp. 187-202.
[22] R. Liu and J. Li, "A Predictive Judgment Method for WLAN Attacking Based on Cloud Computing Environment", 2010 International Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), **(2010)**, pp. 22-25.
[23] A. Shahzad, S. Musa, M. Irfan and A. Shah, "Key Encryption Method for SCADA Security Enhancement", Journal of Applied Sciences, vol. 14, no. 20, **(2014)**, pp. 2498-2506.

[24] A. Shahzad, S. Musa, M. Irfan and A. Shah, "Deployment of New Dynamic Cryptography Buffer For SCADA Security Enhancement", Journal of Applied Sciences, vol. 14, no. 20, **(2014)**, pp. 2487-2497.
[25] M. F. Ali, A. Bashar and A. Shah, "SmartCrowd: Novel Approach to Big Crowd Management using Mobile Cloud Computing", 2015 International Conference on Cloud Computing (ICCC), **(2015)**, pp. 1-4.
[26] H. A. Kholidy and F. Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", Ninth International Conference on Information Technology – New Generations, **(2012)**, pp. 397-402.
[27] D. Riquet, G. Grimaud and M. Hauspie, "Large-Scale Coordinated Attacks: Impact on the Cloud Security", Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, **(2012)**, pp. 558-563.
[28] M. T. Khorshed, A. B. M. S. Ali and S. A. Wasimi, "Trust Issues That Create Threats for Cyber Attacks in Cloud Computing", IEEE 17th International Conference on Parallel and Distributed Systems, **(2011)**, pp. 900-905.
[29] M. H. Sqalli, F. Al- Haidari and K. Salah, "EDoS-Shield – A Two Steps Mitigation Technique against EDoS Attacks in Cloud computing", IEEE International Conference on Utility and Cloud Computing, **(2011)**, pp. 49-56.
[30] A. Ahad, M. Fayaz and A.S.Shah, "Navigation through Citation Network based on Content Similarity using Cosine Similarity Algorithm", International Journal of Database Theory and Application, vol. 9, no. 5, **(2016)**, pp. 9-20.

Authors

Masood Shah, enthusiastic and high-achieving IT professional, has completed MS degree in Computer Science from SZABIST, Islamabad, Pakistan in 2016. He did his Bachelor of Information Technology from Agricultural University, Peshawar Pakistan in 2012. He has completed short courses and diploma certificates in CCNA (Cisco Certified Network Associate), MCSE (Windows Server 2003), Cybercrime, Cyber Security, Networking. He is a young professional having exceptional technical and analytical skills, with over 3 years' experience of Computer System/ Network Administration, Information System Support & Security, Network and Server support. He has worked with Techno-ed Pvt Ltd Islamabad, Money Link Exchange Peshawar, and Waseela-e-Taleem - Benazir Income Support Programme.

His research area includes Cloud Computing, Cyber Security, and Cryptography.

Abdul Salam Shah, has completed MS degree in Computer Science from SZABIST, Islamabad, Pakistan in 2016. He did his BS degree in Computer Science from Isra University Hyderabad, Sindh Pakistan in 2012. In addition to his degree, he has completed short courses and diploma certificates in Databases, Machine Learning, Artificial Intelligence, Cybercrime, Cybersecurity, Networking, and Software Engineering. He has published articles in various journals of high repute. He is a young professional and he started his career in the Ministry of Planning, Development and Reforms, Islamabad Pakistan. His research area includes Machine Learning, Artificial Intelligence, Digital Image Processing and Data Mining.

Mr. Shah has contributed in a book titled "Research Methodologies; an Islamic perspectives," International Islamic University Malaysia, November, 2015.

