International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 6, No. 3 (Sept.-2018)

http://dx-doi.org/10.12785/ijcnt/060302

A Novel Detection and Prevention (DAP) Framework for Abuse of cloud service threat

Ishrat Ahmad[1] & Humayun Bakht[2]

[1,2]School of Management, Cardiff Metropolitan University, UK

Received: 15 May .2018, Revised: 20 Aug. 2018, Accepted: 26 Aug. 2018, Published: (1 Sept. 2018)

Abstract: Cloud security mitigation techniques has not reached the level of transparency and hence, the journey of understanding and accepting cloud computing services still remains uncharted for many organizations or individuals. While mitigation techniques for different security issues are actively being researched, however, there is still insignificancy in research on Abuse of Cloud Services threat, in particular. The threat has been identified as one of the top amongst nine by Cloud Security Alliance (CSA). The study proposes a Detection and Prevention (DAP) framework with fourteen major security measures for significant areas of concern in cloud business, operational and organizational. The key benefits of the framework are: it has improved the process of registration, resource allocation and asset inventory system. It has modeled an improvised human resource system for managing information processing facilities more efficiently, along with employee inventory system and malicious insider activity index. A universal cloud APIs process has been proposed to act as an integrator and decode service providers APIs to run business seamlessly. Furthermore, strategic plan for business continuity, disaster recovery and risk assessment processes have been proposed to define policies and procedures for running business during adverse circumstances. The security measures will be validated and evaluated with existing security infrastructure in cloud. The DAP framework is fully capable of providing better security preservation to the identified threat, which could be utilized for further development in cloud security infrastructure.

Keywords: Cloud Abuse Service, Botnet, DDoS, Malicious Insiders, Shared Technology Vulnerabilities.

1. Introduction

Despite the fact of potential business and IT advantages, the acceptance of cloud computing is still obfuscated as it is loaded with security challenges and complexities [1, 2]. It is the most actively discussed, researched and criticized technologies in IT. It is necessary to identify and mitigate security threats and risks by cloud service providers, in order to give organizations a sense of assurance that their assets are safe and secured.

While mitigation techniques for different security issues are actively being researched, however, the study shows that there is still insignificancy in research on Abuse of Cloud Services threat, in particular. Most critical cloud computing risks do not just cluster around privacy and security aspects, but also trigger by various operational, organizational, and managerial problems related to both cloud vendors and user companies [3].

Data privacy and security risks represent some of the significant challenges in the cloud. However, the most critical cloud computing risks do not just cluster around privacy and security aspects, but also trigger by various operational, organizational, and managerial problems related to both cloud vendors and user companies [1]. Furthermore, the study found out that there is lack in-depth discussion of business continuity, disaster recovery and risks assessment strategic plans that includes user training and awareness of cloud usages. Most prominent cloud security related incidents reported have been due to lack of concern or reluctant about technical infrastructure and management guidance maintenances.

The study proposes a Detection and Prevention (DAP) framework with fourteen major security measures for significant areas of concern in cloud business, operational and organizational. Future work will validate and evaluate the security measures with existing security infrastructure in cloud. The framework works as recommendations to business policy-makers, cloud service providers, customers and end-users on how to deal with this serious threat.

The rest of the paper is organized as follow. In Section 2, we discuss related work in the context of abuse of cloud

E-mail address: ahmad.ishrat611@yahoo.com, humayunbakht@yahoo.co.uk

service threat with associated risks and challenges. In Section 3, we propose a novel Detection and Prevention (DAP) framework with individual security measures to mitigate the security challenges and risks due to the threat. The feature and importance of each security measure are discussed in detail with figures where necessary. In Section 4, we discuss future data analysis and evaluation of the proposed security measures. At the end, in Section 5 we conclude with a summary.

2. Related Work

Several experiments have been carried out by other researchers to find out how easy and inexpensive it is to abuse cloud resources and conduct malicious activities without any interruption from cloud service providers, which are described as followings:

A research group [4] has conducted two experiments to launch DDoS malicious attacks from botClouds by abusing legitimate resources of a leading cloud service provider. The experiments have overloaded and obscured the web server, and performed click fraud on an online poll for votes. Neither visual analyses of the voting log and its timestamps have been detected, nor the service provider has terminated the server. The researchers have suggested in implementing comprehensive bot detection system and removal policy to proactively monitor malicious activities.

Thomas Roth, a German researcher, has conducted a brute force attack to crack a WPA-PSK protected network by renting a server from Amazon's EC2 and managed to generate 400,000 passwords per second into the system with just only 28 cents per minute [5].

A study [6] has identified a research experiment, which has been conducted by Pedram Hayati, an information security professional. The research has evaluated top five cloud providers' defense mechanism in preventing malicious usages of services, and for cyber-crimes to launch malicious attack. The result has showed none of the providers have reset, limited or terminated network traffic connection, no generation of alerts, or suspension of any accounts, as temporarily or permanently.

Two other studies [7,8] have identified similar kind of research, which has been conducted by Rob Regan and Oscar Salazar, two security associates for Bishop Fox, to create a legal botNet by using free available cloud resources. The researchers have further disclosed the reason for their devious scheme is to raise awareness of problems in security measures for abusing of cloud resources.

The current state of intrusion detection and prevention system for abuse of cloud services has been analysed in a study [7]. However, the abuse detection analysis was only for IaaS environment and but not for PaaS and SaaS, which are equally important and needed as much attention. According to another study [9], attackers can launch malware injection attack within PaaS or SaaS by developing their own malicious module or application and trick as a valid instance for service delivery. Existing intrusion detection and prevention techniques are only of limited use due to high level of control over the resources, hence making them more complicated. Moreover, the privacy policies in service providers' term of use and policies were about generic online operations and not specific to cloud offerings. The study [7] has not provided any finished solutions, but with some possible approaches for improvement of abuse detection. The researcher has stated that conventional intrusion detection systems cannot be constructive for detection of abuse in cloud environments, hence further suggested for 'abuse detection and prevention system' that automatically take corrective action on detection of abuse or malicious activity [7].

Another study [10] has explored and investigated the scope of 'abuse of cloud computing' and has served as an introductory research effort to warrant more extensive research on this particular context. A related study [9] has identified the fact of having weak registration process in obtaining cloud services and lack of effective security controls lead to cyber criminal activities. The study has encouraged other researchers to conduct more extensive research of proactive security techniques to prevent unauthorized and illegal access to sensitive organizational data in cloud [9]. The study has investigated the scale and scope of malicious insiders risks and impacts on business operations and proposing safeguarding sensitive information, implementing technical defensive approaches and conducting periodic vulnerability assessments. However, other defense approaches are also need to be considered, such as lack of maintaining standard hiring procedures or practicing code of conducts and real time audit trail process monitoring.

A defense mechanism through economic measures to deter attacks from abusing of cloud services has been proposed in a study [11]. The mechanism works by paying a transaction fees as virtual or real currencies to service providers before invoking the service. However, the challenges are also evident as the exchange rates between virtual and real world currencies keep fluctuating. Also, the service providers could have malicious intention for abusing services. On the other hand, digital currencies are dealt by pseudonymous identifiers, with no real world information, however, they can be trace back only through users' cryptographic public keys. The study has number of challenges from the proposed system, such as, to determine deposit value, as the cloud customers may get detracted due to payment system; transaction cost needs to be defined for different type of transactions; Bitcoin exchange rates and costs;

cryptographic public key reuse by malicious user and deposit returns by malicious providers.

Over the years, the research community has focused more into technical aspects of cloud security, even traditional insider threat has been studied for decades, but cloud insider threat issues have not received much attention and some serious approaches are needed to overcome the impact of it [18]. A study [3] has showed that critical cloud computing risks do not just hover around security and privacy aspects, but also affect legal, operational and business management areas. It seemed that various managerial and organizational employee related problems, from both cloud providers and customers, can also trigger potential failure of cloud computing adoption. Security threats can occur from both outside and inside of the organization [13]. A malicious insider is just another major issue to consider that can have easy access to potentially sensitive information and can involved into an organized crime. System administrators with high privilege roles can access to multiple customers' data, residing on same physical servers, to leak or sell to other parties of interest.

A study [12, 13] has discussed in relation to malicious insiders as rogue internal employees or stakeholders could exploit technological vulnerabilities or privileged roles to conduct nefarious activity for a fortune by selling sensitive data or for future businesses purposes. An approach has been proposed in [14] by enabling a security team for remote administrators during operations and maintenance. Data protection techniques could also be as effective for defense if diligently applied [15]. However, an activity predictive model is required to observe and analyze suspicious behaviour of potential invader, to monitor and track malicious activities by stakeholders, to help in rapid decision support system and quick responses for business recovery. Management channel processing, reporting and awareness need to be integrated with organizational policy and service level agreements.

A study [17] has proposed to strict initial registration and validation processes. The authors have further suggested in establishing multi-level authentication process to access the cloud services. Another study [13] has proposed to strengthen the registration process and credit card fraud check. The study has also proposed in implementation well-established rules and regulations for network administrators. However, security regulations should not be only for network administrators, but the business rules and regulations along with the responsibilities should be concerned and practiced by all the stakeholders associated with cloud business organizations.

In relation to the discussion above, the study has found out that there is a lack of security standard defined for Abuse of Cloud Services threat and has addressed the fact as a research gap. To the best knowledge, no similar work existed by the time of publication. According to Cloud Security Alliance [7 19], Abuse of cloud services has been identified as one of the top threats in cloud computing. The threat can leverage major security challenges like DDoS, BotNet or BotCloud attacks, while other challenges like Shared Technology vulnerability or Malicious Insiders issues can be as constructive for abusing cloud resources and services.

Few other studies [13, 16, 20-27] have also identified the threat and its consequences. However, they have only conferred about the importance of implementing mitigation techniques for the identified threat, but no standard methods have been suggested. Other related studies [7, 9, 11, 17, 28] have been done on particular context to formulate strategies for the identified threat, but failed to provide a holistic overview of the issues apart from few generic suggestions, and hence required a defined model of security controls that would be accepted by both academia and IT industry. A generic cloud security framework is required to assess and evaluate organizational security objectives, which would be beneficial for both cloud customers and service providers.

3. Detection And Prevention Framework

The Detection and Prevention framework is a concept with preventive security mechanisms for cloud technical and business infrastructure. The framework, in Figure 1, is laid out into three vertical layers, as Cloud Infrastructure, Security Challenges and corresponding potential Impacts from individual challenge due to Abuse of Cloud Services threat.

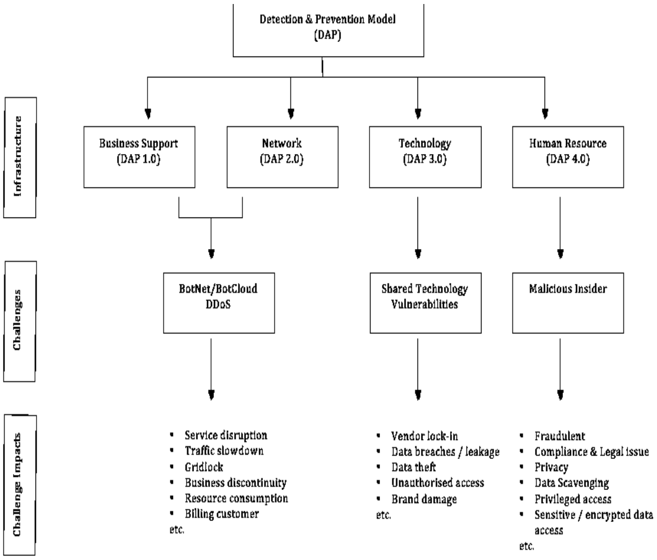

Figure 1. Detection and Prevention (DAP) Framework

The Cloud Infrastructure is divided into four major cloud components, as Business Support, Network, Technology and Human Resource. The security measures have been categorized according to these four cloud components, and are discussed elaborately in next following sections:

A. Strategic Plan

Cloud service providers and customers need to understand the importance and benefits of the process for business to recover from adverse circumstances. Cloud customers also need to make sure that service providers have strategic plans for business continuity, disaster recovery and risk assessment plans in places.

1) Business Continuity Process: A Business Continuity plan should have policies and procedures for business running, departmental plan for management and teams, their roles and responsibilities, emergency contacts, course of actions and direction, compliance and controls according to business requirements etc. Having a business continuity plan will help to recommencement of business activities.

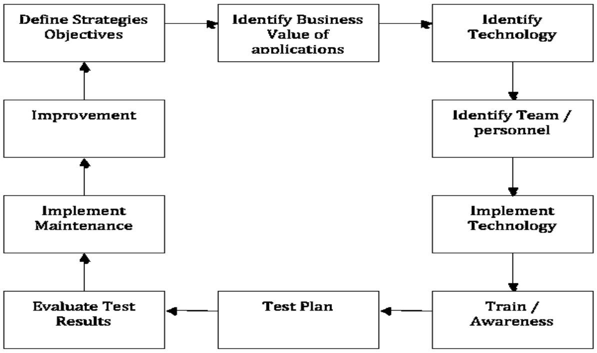

Figure 2. Business Continuity Process

In Figure 2, steps for Business Continuity planning processes, as an example, are provided. First, the objectives under each business strategies must be defined. The next is to define the applications for running the objectives. The resources, tools and technologies and team members must be allocated with defined roles and responsibilities. Next to implement the application, followed by testing and maintenance. Proper user training and awareness must be provided as well. The last steps are to test, evaluate and maintain the plan and review for further improvement.

2) Disaster Recovery Process: A Disaster Recovery plan should include the processes that will backup all fundamental elements like data, applications, offsite information access etc. Data, applications, databases or other services can be replicated to a cold VM backup, so when needed, the application and workload, or part of it, can be brought up at once.

An example of steps for Disaster Recovery planning processes is provided in Figure 3. Firstly, the disaster recovery team has to be selected, then to identify all the possible risks and vulnerabilities of the affected system. Next to identify the business impacts for recoveries requirement. The onwards steps are to develop, test, evaluate and maintain the plan and review for further continuous improvement.

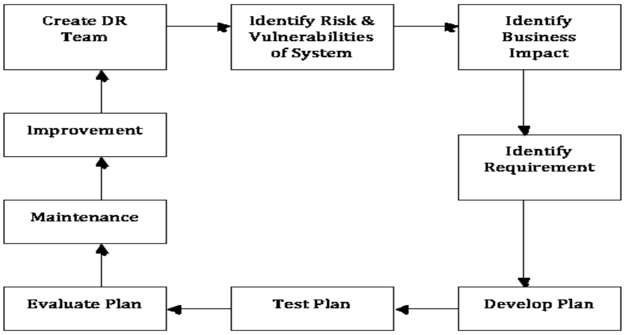

Figure 3. Disaster Recovery Process

3) Risk Assessment Process: A Risk Assessment plan should include to analyse the triggering events of the risk, consequences to assets, severities, frequencies, how to reduce, cost, benefit, incur etc. It develops strategies to manage risks and control its implications. Although it is impractical to have a risk free services, but an effective and efficient risk assessment with mitigation techniques may provide a reliable and cost-effective business infrastructure. Before transferring data and applications to any cloud service, a customer should consider performing a risks assessment of their assets, and parallelly check cloud service provider’s standard level and security measures in control to lessen any potential risk. Figure 4 shows the steps as an example during Risk Assessment plan.

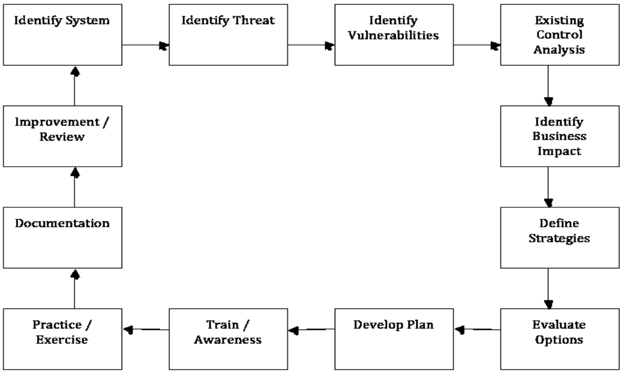

Figure 4. Risk Assessment Process

The initial step is to identify the system under risks. Then to identify the possible threats and vulnerabilities points. Next to identify and analyse all the existing security controls for the identified points. Identify the business impacts in order to define the strategies for the risks assessment of the system. Then is to evaluate all the possible options and to develop the risks assessment plan. Adequate user training and awareness must be provided in order to handle the applications during an adverse situation. The last two steps are proper documentation so that they are accessible when needed, and review for further continuous improvement.

B. *Audit Control Process*

Audit Control Process with proper planning must be implemented and maintained to evaluate system internal and external control design and effectiveness for any risks through annual audits. Objectives must be listed with all internal and external applicable policies and procedures, like, list of software, operating systems, network topologies, IP addresses, firewall, intrusion detection systems, system access, system administration processes, backup, recovery etc. Departmental responsible individual must get involved from early stage during audits. It is recommended to have third party auditors with security experiences of great extent. Auditor's report must summarize organizational security infrastructure, sources of threat, intrusions exploitation possibilities, impact and risks of service interruptions, incur, recommended measures, future concern and security enhancements.

C. *Registration Control Process*

To establish Registration Control Process, in order to practice secured verification and validation registration procedures for new accounts. It will help to manipulate and store all information related to registration process, and will be separated from storage of data and application. The control process should have strong multi-level authentication, user-level and cloud-system-level, for remote access.

D. *Financial Concession System*

A financial concession should be claimed as a deposit, through digital currency or real world currency, based on organizational or individual's requirements of the cloud services and a new subscription or an existing client. The deposit amount could be large compare to existing client, and the cloud service provider can terminate the account and keep the deposit fees during any discrepancy.

E. *Warning System*

Login forewarning message can let user know the rights and consequences to access the site. Such type of deterrent control will prevent potential attackers to start any malicious activity.

F. *Asset Inventory System*

An Asset Inventory system for both physical and virtual should be implemented with proprietor's details, users details, data and application type, system purpose, peripherals connection, software configurations, shared resources if any etc. Additionally, their data and application can be categorized according to the high target values. This will help continuously to evaluate, direct and monitor during allocation and management of software and hardware resources for individuals, whilst in use for maintenance resource performance targets. Dynamic host configuration protocol (DHCP) server logging can be used for Asset Inventory system and to detect unknown resources.

G. *Resource Allocation Process*

Multi-tenancy is one of the key features of cloud computing and hence cannot be avoided, so, an innovative Resource Allocation Process must be implemented carefully by the service provider in order to address consumptions of resources by each cloud user, such as bandwidth, computing process, storage, process power etc. in order to keep track of usage during adverse situations and hence to maintain resource performance targets. Review and approve mechanisms for resource allocation registrations, with a given threshold value, must be maintained and instant action to be taken for any resource management abnormalities through audit trails, and can generate security alarm to Management Channel Process. The process must be able to identify co-residence activities, otherwise, it should be avoided and physical servers should be dedicated for an instance with high service fees.

The Resource Allocation Process must be separated from the Asset Inventory System and the Registration Control Process, so that the security posture of the process can be updated without depending on other service components.

Figure 5 below shows an example of resource allocation process.

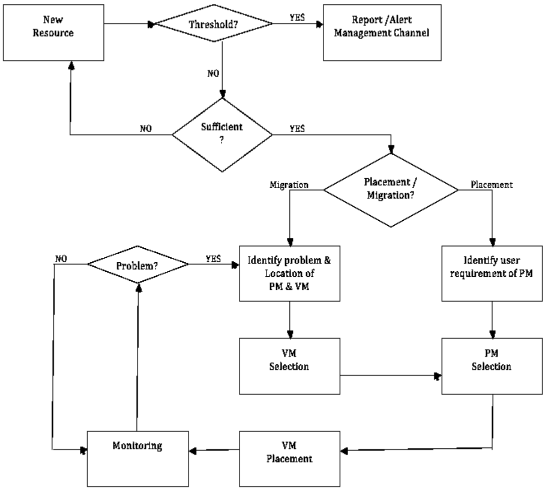

Figure 5. Resorce Allocation Process

H. Malicious Insider Activity Index

Following are some discussed points that are highly recommended to consider, while having security measures in places so to control malicious activity by internal people within the organisations.

It is necessary to define job roles and responsibilities for employees, suppliers and other stakeholders based on the business requirements and hierarchy level of management. The guidelines of the responsibilities, employment contractual, termination agreement and training process should clearly state the security rules and procedures for handling organisational assets and information processing facilities. If further needed for business purposes, Data Protection Act is to be signed by stakeholders. It is also advisable to both cloud service providers and customers to have a strict screening policy for employees, including character references and criminal activities records. During merging between organizations, all employees' background records must also be examined according to business requirements. During employment termination phase, constrain all physical or remote access to organization system.

Unit managers must be more alarmed and vigilant for malicious insiders on-premises, to make sure that employees are complying with the agreement policies and maintaining code of conduct. At tele-working sites, employees must established and follow physical security controls.

Organisations must produce restriction process for installation of software on operational system by unauthorised users. There should be restrictions or limitations to any modifications or alterations of software packages, even by authorised users.

Managers must have control on the level of access or revoke access to sensitive information by all employees except the one who needs to perform their job. The role of administrators for regular tasks and the ones for backup and restoration tasks should be clearly separated.

It is recommended to have security measures for protection by using firewalls, spyware, and antivirus software. No internal network access should be allowed to trusted business partners. Cloud customers are advised to store their encrypted data in cloud system without including the keys.

Managers are recommended to use audit trials process to observe individual accountability. Employees should be trained and briefed clearly audit log. Keystrokes from the audit trails used by malicious insiders can be examined and assessed to find the damage and can restore back from the incident. Management can trace back through the audit log analysis and can easily inspect the user's actions.

A Malicious Insider Activity Index should be developed, to count and analyse the disruptive or suspicious behaviour of potential invader, based on users' random searches, working after office hours, inconsistency behaviour, background records and demographic profile as drug, alcohols, debt, credit etc. Other activities like any breach of contract agreement, VM mismanagements, reckless screening practices of employers, and many more issues can also be used to analyse and develop a predictive model to reckon any possible attack. The Index can also be helpful for Management Channel Process in rapid decision support system and quick response during adverse circumstances.

I. Employee Inventory System

To keep a list of physical and information system access accounts to individuals during their tenure, so to audit the accountability of the departed employee. Will be easy to put constraint to organizational system during employee termination phase.

J. Audit Trail Process

Audit trails analyses system management, operational and technical infrastructure and can record in greater level the lists of access controls by the user, system or application or some outside source. Real-time potential security breaches, intrusions, technical problems, data loss or corruption recovery by reconstructing the data files, protect service transactions and insider's engagement in any unauthorised activity can be detected easily, with analysis further of any errors, damages or poor performances of system behavior and can generate alarm to concern person. The confidentiality of audit trail records and information must be protected from unauthorized access and with encryption methods.

K. Management Channel Process

To implement a Management Channel Process in order to get immediate access to the exact relevant information and to detect, analyse and respond to complex security incidents and mitigating risk during security crisis in no time, even through remote assistance.

Employees from different departments must be trained about the security issues, and should report immediately to the appropriate personnel or team so to avoid and recover from any critical incident. All the reported incidents should be properly documented and reviewed and evaluated at regular intervals, so to have adequate knowledge and training during adverse circumstances.

In Figure 6, at first, the process starts with new reporting message, to identify the problem and location from the reporting message. Then is to allocate the team for guidance for the problem. Next is to analyse the impact from the problem, so to identify the security controls to be taken as initiative. New security controls must be created for the problem if there is none. The new controls must be tested, evaluated and documented before applying for resolving the problem. Next is to respond back to the reporter for further actions to be conducted and to update the incident databases. Proper user training and awareness must be provided in order to handle the same problem in occurrences again. The final step is to keep monitoring all the time so to detect any problem and report back to control it without any delay.

Figure 6 shows an example of the steps in Management Channel Process.

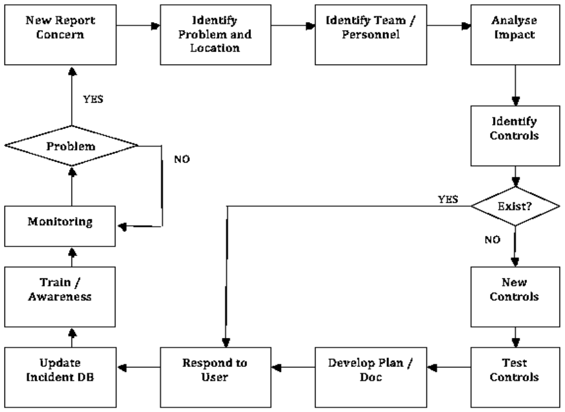

Figure 6. Management Channel Process

L. *Universal Cloud APIs (UCA) Process*

To implement Universal Cloud APIs (UCA) process to standardized APIs and data format for users' data and application migration process; such compatible APIs amongst service providers will help to increase the accessibility of multiple cloud service providers' services during security incident and to avoid data lock-in or data unavailability issues. The process should act as an integrator to decode between APIs so to run services seamlessly. The process can also look for technical design flaw, software failures and version update intervals in order to avoid any risks of vulnerabilities or weak points in cloud technical infrastructure.

The target can be obtained, by considering a singular common programmatic point of contact, which can cover the whole cloud infrastructure stack and emerging cloud technologies. The value of APIs integration applications is gaining importance because the focus of the trend is on the cloud, mobile and IoT as means for business development and digital transformation.

M. *Network Security Control Process*

To maintain Network Security controls process by implementing appropriate detective controls like IDS and Firewalls with proper configuration. The process will monitor VMs, memory and on the virtual hard drive in order to detect DDoS attacks and monitor operating system process to detect BotNet command and control attack. The process is to monitor and report of any suspected infringement within inside and outside the network. A process should be implemented with the capabilities of tracing back the malicious attack accessible points through Audit Trail process.

Unlike traditional ones, Cloud-based Firewalls are necessary to be deployed at strategic points with proper configuration so to check incoming and outgoing traffic, to or from the Internet, and limiting any potential damage from taking place within the virtual and local network. Hypervisors needs to be protected from intruder who might take control of the underlying OS and may disrupt or even shutdown the whole cloud services. IDS must be implemented at inbound and outbound boundaries to observe and track abnormal activities, which are often overlooked by firewalls, and send alerts to system administrator. Application gateway should be used to access network from remote location or home, and hence constraining from establishing any unknown connection.

N. *Information Security Control Process*

To establish Information Security Controls process in order to have policies and procedures in line with organizational human resource maintenance standard and requirements. The process must have strict screening policy to follow during employment recruitment phase, and all employees should be acknowledged and affirmed to agreements. Training program for new employees must comply with business requirements, and should encourage using management channel to report any security incident.

Updated policies, guidelines and documents can be published to company's website or portal. The Audit Trail process should be used in order to keep set of records in greater level the lists of user activities while using systems and applications processes. Management must scrutinize around the organization in order to spot any security holes or any infringement of business rules and regulations, and must have control on the level of access or revoke access to sensitive information by all employees.

No access to program source code by unauthorised users, and limit to any modifications of software packages. Address Information Security controls during project development; consultation from special security group and authority bodies; Regular monitoring and maintaining up-to-date applications and technical infrastructure.

Cryptographic controls and policies should be applied for sensitive data. Encryption implementation should be easier, and must be able to ensure customers about their data and application security controls, both in transit and at rest. Trained for unsafe email and link; Having anti-spam filters or right software to avoid unwanted emails.

Figure 7 below shows an example with a flow diagram for cloud Human Resource System (HRS) processes management activities.

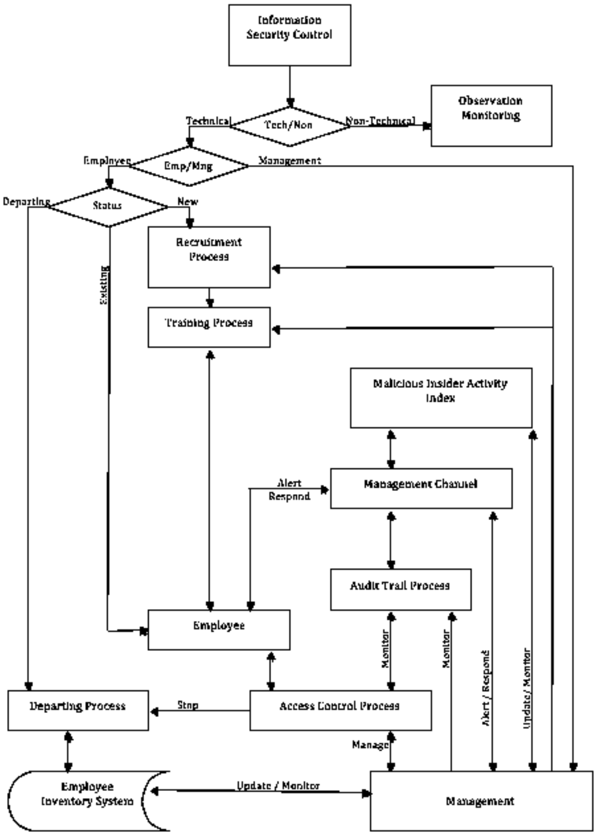

Figure 7. Cloud Human Resource System (HRS) Flowchart

HRS starts based on technical or non-technical information security controls. For non-technical part, management needs to observe and monitor employees' activities, as stated in their job roles. For technical sides, the HRS will inquire for regular employment or management level of process. For employment, the HRS again inquires for the employee's status. If it is a departing employee issue, the management process update Employee Inventory System and revoke or limit all access controls and notify further to the Management Channel Process for observation of any malicious activity through Audit Trail Process. Or else if, the inquire has accepted as new potential employee, then the HRS will update the employee as candidate activities into Recruitment Process, followed by Training Process. Else the HRS has accepted as existing employee, then it will directly take to Employee Process for activities like update profile, account access or training etc. The Management Process has connection to all other processes in the HRS such as, with access control process, the management gives access control or revoke to accounts for other users; with Audit Trails Process, the management can monitor the activities of a system or user access; with Management Channel Process, the management can take immediate action to any incident report; with Malicious Insider Index Activity, the management can update, view or monitor malicious insiders activity records for review or improve security controls.

4. Data Analysis and Evaluation

In future, data collection and analysis will be conducted in order to validate and evaluate the proposed framework. The primary goal of the data collection and analysis for the proposed DAP framework is to find out about the real-world existing cloud security systems and how the participants will respond with the propositions.

The study will use Design Science Research Methodology to define the construct, model and methods to outline the possible courses of action and a preferred approach of an idea for framework with security measures in cloud computing. According to March and Smith [29], the significance of the research is the development of any set of construct, model, methods and instantiations addressing the same existing artifact on significant improvement, and hence actual performance evaluation is not required at this stage.

According to Yin [30], developing a theoretical framework based on the literature review and from predicted propositions helps to organise and direct the analysis of the collected data. For the study, a conceptual framework has been developed based on the literature review, which has helped to get the opportunity to understand the key ideas and relationships for data collection. Some pre-defined propositions will be devised before undertaking data collection and analysis.

The search scope of the literature has been mostly confined within year of 2006 to 2017, as the concept of 'cloud computing' has begun to evolve in 2006 [31]. However, in order to broaden the background and other related areas like grid computing or service oriented architecture and to study research methodology, few papers and books prior to 2006 have been also considered. Most of the sources were from conference proceedings and journals of Google Scholar, ACM Digital Library, ScienceDirect, IEEEXplore and SpringerLink. Apparently, very few researches were found on Abuse of Cloud Services threat, even though it has been considered as one of the top threat by CSA [19].

The data collection will be from highly experienced IT professionals, CIO of service providers and users, cloud researchers involved in developing and implementing cloud based solutions across the globe (Europe, USA and Asia). The variation in job proficiencies and knowledge of respondents will enable the study to accumulate data from different aspects of cloud computing security and privacy issues practices within different industries.

Most of the questions will be designed to divulge into two parts, one is to comprehend the existing organisational infrastructure of the respondent and the other part is whether the respondent agrees to the attributes of the proposed model. The questions will reflect across information security controls, human resource security, business continuity, disaster recovery, risk assessment plan, roles and responsibilities, resource management, user access management, media handling, operational procedures and responsibilities, incident report and management, backup and recovery, information security incidents and managing quality of information technology and services.

The data analysis is to run a test on the dataset with a model of defined expected responses. The data collected for the research will be mainly qualitative, non-numeric data, which will be quantified for analysis to draw and verify the defined propositions for conclusions. The data analysis will be assessed to produce understanding of the observable fact of existing cloud security and will provide improvising recommendations in security of cloud business infrastructure.

The study will help to evaluate the conceptual Detection and Prevention (DAP) framework with existing studies and security controls in various organizations and will help to validate the proposed security measures for the identified challenges from Abuse of Cloud Services threat.

Conclusion

From preliminary studies no universally adopted security standard is evident for Abuse of Cloud Services threat, but only conflicting laws, regulations and different perceptions of protecting organizational privacy. The study has proposed a Detection and Prevention (DAP) framework with security measures to mitigate and overcome the security risks and challenges from the threat. The framework has provided recommendation to business policy-makers, cloud service providers, customers and end-users on how to deal with this serious Abuse of cloud services threat. The research has shown the identified security challenges and the non-trivial nature of extension of existing knowledge in a new version of the problem usually because technology changes.

The extensive research on Abuse of cloud services threat in this study is only at a preliminary stage that can help other researchers to advance more investigation in this increasingly significant research area. The conceptual security measures of Detection and Prevention framework can only be used as a direction of new practical solutions to prevent challenges from Abuse of Cloud Services threat. However, to complement the research work, the processes from the framework can be implemented and deployed in other related research projects to investigate for generalisability. Based on the results from this research work, the Detection and Prevention (DAP) framework confirms very promising ways of preventing security threats, hence it is not only beneficial for cloud service providers but also to cloud customers' organization as well.

References

[1] I. Ahmad, H Bakht, U Mohan, "Cloud Computing – A Comprehensive Definition", J Comput. Manag. Stu., Vol 1, Issu1, pp.1-8, 2017.

[2] Ahmad I, Bakht H, Mohan U.: Cloud Computing – Threats and Challenges. J Comput Manag Stud Vol 1, Issu1, pp.1-12, 2017.

[3] A. Dutta, G. Peng, A. Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of IT Experts", J Comput. Inf. Syst., Vol 53, issue 4, pp. 39-48, 2013.

[4] Clark K, Warnier M, Brazier FMT.: BOTCLOUDS The Future of Cloud-based Botnets? In: NLnet Found., 2011. Available at: http://homepage.tudelft.nl/68x7e/Papers/botclouds.pdf.

[5] T. Roth, "Breaking encryptions using GPU accelerated cloud instances", In: Black Hat Tech. Conf., pp. 1-8, 2011. Available at: https://media.blackhat.com/bh-dc-11/Roth/BlackHat_DC_2011_Roth_Breaking_encryptions-wp.pdf.

[6] H. Badi, G. Doyen, R. Khatoun," A Collaborative Approach for a Source based Detection of Botclouds" In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). pp. 906-909, 2015.

[7] J. Lindemann," Towards abuse detection and prevention in IaaS cloud computing", Proc - 10th Int Conf Availability, Reliab Secur ARES, pp. 211–217, 2015. doi: 10.1109/ARES.2015.72.

[8] Anderson M.: Black Hat 2014: How to Hack the Cloud to Mine Crypto Currency. IEEE Spectrum, 2014. Available at:

[9] https://www.bishopfox.com/news/2014/08/iiee-spectrum-black-hat-2014-hack-cloud-mine-crypto-currency/

[10] M. Omar M, "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing", In: Handbook of Research on Security Considerations in Cloud Computing. IGI Global, pp 31–40, 2015.

[11] Y. A. Hamza, M. D. Omar, "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing", Int J Comput Eng Res 3: pp. 22–27, 2013.

[12] J. Szefer, R. B. Lee, "BitDeposit: Deterring Attacks and Abuses of Cloud Computing Services Through Economic Measures", Proceedings of the Workshop on Assured Cloud Computing (ACC), pp. 1-6, May 2013

[13] M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques", J Adv Comput Sci Technol Vol 3, issue 2,: pp. 202–213. (2014). doi: 10.14419/jacst.v3i2.3588

[14] T-S. Chou, “Security Threats on Cloud Computing Vulnerabilities”, Int J Comput Sci Inf Technol, Vol 5, No. 3, pp. 79–88, 2013.

[15] S. Bleikertz, M. Schunter, Z. A. Nagy, M. Schunter, “Secure Cloud Maintenance - Protecting wordloads against insider attacks”, 2012 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS’2012), 2012.

[16] W. R. Claycomb, A. Nicoll, “Insider Threats to Cloud Computing: Directions for New Research Challenges”, 2012. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.409.9789&rep=rep1&type=pdf

[17] S. Mewada, U. Singh, P. Sharma, “Security Enhancement in Cloud Computing”, Int J Sci Res Comput Sci Eng, Vol 1, Issue 1, pp.:31–37, 2013.

[18] M. Kazim, S. Zhu, “ A survey on top security threats in cloud computing”, Int J Adv Comput Sci Appl., Vol 6, No 3, pp.109–113, 2015.

[19] M. Kandias, N. Virvilis, D. Gritzalis, “The Insider Threat in Cloud Computing”, Int. Workshop on Critical Information Infrastructure Security. pp 93–103, 2011.

[20] CSA, The Notorious Nine Cloud Computing Top Threats in 2013, Cloud Security Alliance - The Notorious Nine, 2013.

[21] M. A. Hossain, S. Taslima, “A Study on Threatened Risks for Cloud Computing Security- How to Overcome These Risks”, Int J Adv Res Comput Sci Softw Eng., Vol 6, pp. 86–89. 2016.

[22] M. Rahaman, M. Alam, S. Islam, T. Rahman T,” An Effective Cloud Computing With its Security in the Cloud: A Smart Survey”, Int J Eng Sci Comput. Vol 6, pp. 6999–7003, 2016. doi: 10.4010/2016.1670

[23] V. Ashktorab, S. Taghizadeh, “Security Threats and Countermeasure in Cloud Computing”, Int J Appl or Innov Eng Manag., Vol 1, pp. 234–245, 2012.

[24] Kaur S, Khurmi S.: A Review on Security Issues in Cloud Computing. IJCST Int J Comput Sci Technol, Vol. 7, Issue 1, pp. 54-56, 2016.

[25] Al-Attab BS, Fadewar HS: Security Issues and Challenges in Cloud Computing. Int J Emerg Sci Eng 2:22–26. (2014).

[26] J. Singh, “Cyber-Attacks in Cloud Computing: A Case Study”, Int J Electron Inf Eng., Vol 1. pp.78–87, 2014.

[27] A. Aich, A. Sen, “Study on Cloud Security Risk and Remedy. Int J Grid Distrib Comput”, Vol 8: pp. 155–166, 2015.

[28] K. Lee, “Security Threats in Cloud Computing Environments”, Int J Secur Its Appl., Vol 6, pp. 25–32, 2012.

[29] A. Shahzad, A. Litchfield, “Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable”, Australas Conf Inf Syst, pp. 1-16, 2015.

[30] S. March, G. Smith, “Design and natural science research on information technology”, Elsevier - Decis Support Syst Vol. 15, pp. 251–266, 1995.

[31] R. K. Yin R, “Case Study Research Design and Methods”, 3rd edition, Sage, Thousand Oaks, 2003.

[32] Li Z, O’Brien L, Cai R, Zhang H.: Towards a Taxonomy of Performance Evaluation of Commercial Cloud Services. IEEE 5th Int Conf., pp. 344–351, 2012.

[33] doi: 10.1109/CLOUD.2012.74

Dr. Ishrat Ahmad has achieved her PhD degree from Cardiff Metropolitan University, UK. She has done her BSc in Computer Science and Engineering and MSc in Data Warehousing. She is a Software Quality Assurance Engineer by profession. Email: ahmad.ishrat611@yahoo.com

Dr. Humayun Bakht is a Director of Studies / PhD supervisor at the Cardiff Metropolitan University / London School of Commerce. Dr. Bakht is a regular contributor of both academic and non academic articles. He has also authored several books including ‘Mobile Ad-hoc Networking’ and ‘A Roadmap to PhD’. Email: humayunbakht@yahoo.co.uk