A Review on Security Issues and their Impact on Hybrid Cloud Computing Environment

Mohsin Raza[*1], Ayesha Imtiaz[*2], Umar Shoaib[*3]
Faculty of Computer Science and Information Technology
University of Gujrat, Gujrat, Pakistan

Abstract—The evolution of cloud infrastructures toward hybrid cloud models enables innovative business outcomes, twin turbo drivers by the requirement of greater IT agility and overall cost-containment pressures. Hybrid cloud solutions combine the capabilities of both public clouds along with those of on-premises private cloud environments. In order to key benefit with hybrid cloud model, there are different security issues that have been shown to address. In this paper, we explain security issues in detail such as to maintain trust and authenticity of information, Identity management and compliance which is influencing in enterprises due to migration of IT cloud technologies are increasingly turning to hybrid clouds. Here, work outcomes with comparative study of different existing solution and target the common problems domains and security threads.

Keywords—Hybrid cloud; migration; security issues; security techniques

I. INTRODUCTION

Cloud computing topic has lot of rapid innovation on Internet from cloud service provider such as Amazon, Open Stacks EC2, through different types of virtual data centers operate across different types of IT environments. Gaining the several benefits, cloud computing provides a more elasticity enabling the on demand approach to an elastic pool of shared computing [1], [2]. In the past few years, several business enterprises are go mainstream that by rapid provisioning the cloud resources and to leverage the scale inherent in IT Infrastructure to cut costs and modernize IT operational for service delivery requirements rather than need of purchasing their own expensive IT infrastructure.

Today many enterprises for cost savings IT cloud technologies are increasingly turning to hybrid clouds, allowing them to combine the benefits of building private and public clouds as well as to leverage the scale inherent in their existing IT Infra-structure to cut costs and modernize IT operational agility for service delivery requirements.

Recently, survey covered that many enterprises are rapidly adopting a multi-cloud approach using different cloud service vendors to support their IT infrastructure [3]. According to survey respondents, Microsoft Azure use 58%, and Amazon Web Services use 52% as their cloud platforms providers. Additionally, Google Cloud use 19%, Oracle Cloud use 9%, and RackSpace use 7.3%.

Hybrid cloud computing is about aggregation and integration of computer, networking, applications, storage, security and management into unified, orchestrated management framework which enables enterprise IT and developers to leverage scale, flexibility and cost savings of existing in-house IT investment tools, systems and privacy policies scale to manage in the enterprise data center with their newly adopted cloud services[4], [5]. The IDC report predicts more than 80 per cent of IT enterprises will commit to hybrid architectures [6]. Hybird models are shown in Fig. 1.

A Hybrid cloud includes a few addition features as discussed below.

A. Integration of Infrastructure and the Application Environment

Hybrid cloud platform is the capability spinning up workloads or virtual machines for infrastructure as a service same in both private and public clouds.

B. Interconnectivity

The parallel processes in which two coexisting environments communicate and interact facilitate the exchange of data, VMs and applications among individual clouds.

C. Portability of Applications

Using cloud aware development builds systems from re-usable components that will work the same across cloud environments.

D. Monitoring and Management across Cloud Environments

In a Hybrid clouds, monitoring and management is essential for the health of the system, visibility into system health across clouds is crucial

In spite of such significant benefits, migration of IT cloud technologies from enterprises have important aspect over privacy, integrity, security concerns and compliance considerations due to reliability on multi cloud vendors such as Microsoft, Amazon and Google [7]. The descriptive study in this paper is summarised with a view to discuss and different security issues that have been shown to address. The approaches to counter security issues in Hybrid model are numerous with huge risks which have been kept out of scope [8].

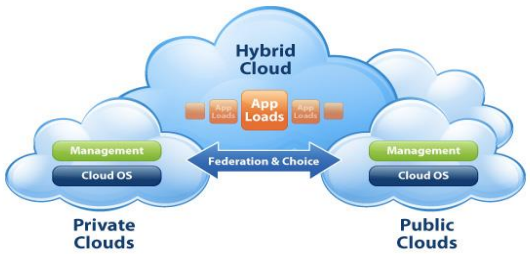

Fig. 1. Hybrid Cloud Model.

There are different security issues such as Data protection, migration issues, security management policy, to maintain trust and authenticity of information, Identity management and compliance and shared technology are the major security issues [9]. The rest of the paper is summarized as follows. In Section 2, we give an overview on work outcomes with comparative study of different existing solution and target the common problems domains and security threads from cloud, incompatible network policies. Section 3 presents hybrid cloud approach, there are different security issues that have been shown to address. Section 4 presents the conclusions of this research.

II. Related Work

Security in the hybrid cloud is still a major concern for many IT organizations.

Undale et al. [10] describes comparison and performance review of AES, Blowfish and RC6 Symmetric cryptographic algorithm in hybrid cloud application with standard cryptographic techniques, such as Proxy encryption, ABE (Attribute based encryption)with its types. To make an efficient solution and to make an NP Complete solution of image encryption problem on hybrid cloud environment.

Gharat et al. [11] introduce several techniques have been developed for secure data and authentication and to maintain trustworthiness. For trust management system using feedback filtering approach will be explained. In this paper addresses different methods for data protection includes Single Encryption, Multitenancy and Multi level Virtualization, Authentication model including several scenarios.

Rao et al. [12] discusses big data Security using Hybrid Cloud are widely used, the traditional cryptographic methods are not suitable for big data. We are implementing the modified approach for the image and text encryption using method in which image is cut down into pieces and their pixel values get modified by using noise values. We proposed a approach for the efficient decryption technique by keeping the existing shuffling technique. With the encryption technique we have used steganography for text data storage. In this paper, our aim is to achieve the image and text data privacy using hybrid cloud.

Sanjay et al. [13] focused on to identify the security threats in a hybrid cloud architectures for enterprises and suggested control method to access the data in Hybrid cloud approach using multi factor authentication from on-premises Active Directory. Federated Identities between on premises directory solution using Federated ID for the Identity infrastructure services is detailed. This paper suggests a security solution, which leveraging Active Directory Federation Services from the security of their user credential for organization, by creating Federated Trust Framework. To achieving federation trust is relying on various authentication servers such as Microsoft Active directory services.

Anukrati and Dubey et al. [14] address some challenges to consider when migrating to hybrid clouds and techniques can addressed in hybrid infrastructure securities can be provide to protect encryption and decryption communication, key based security algorithms which are countered authentication and authorization techniques secured over the intra cloud communication in which an automatic, intelligent migration service in hybrid cloud relay on agent technology. In this research paper major areas of focus on a group of unified Identity & Access Management and privacy frameworks across cloud computing applications or services.

Hardayal and Shekhawat et al. [15] mainly concern the security risks and solutions in hybrid cloud computing for electronic governance. This study summarizes major security issues based on a precise literature review. Federated Identity in organizations for authentication of cloud service should address the challenges and solutions according to lifecycle of identity management, available authentication methods in trustworthy manner, integrity and confidentiality protection ensures. Data in transit is generally security risk lies, so encryption technique should be implies for data and finally suggests the feasible security solutions.

Patil et al. [16] introduce a secure Hybrid Cloud approach for encrypted deduplication of data using key generation. We propose secure hashing algorithm for avoiding deduplication, which generates a unique key for each file. The generated key is stored in private cloud and Key generation process involves inside the public cloud. For security consideration to encrypt the data before updating data into the cloud becomes necessary. For achieving authorized deduplication along with protect data security, hashing algorithm is used which makes technique very secure, to protect data from unauthorized access.

Following major problems are observed during the study. In the Table I below a comparative study about security issues in Hybrid cloud:

TABLE I. COMPARATIVE STUDY

S. No	Title	Author	Research	Year	Problem Domain
1.	Survey of Color Image Data Privacy in Hybrid Cloud	Bharati Kale, Onkar Undale,	How to improve performance and compare image data privacy with standard cryptographic algorithm and techniques in Hybrid cloud.	2015	To protect image data privacy
2.	Survey on Establishing Authentication Based Ttrust , Data Security in Hybrid Cloud	Dilip Motwani, Mithil Gharat,	Suggest different methods to protect data for Trust, Data Security, and Authentication including different scenarios.	2013	To maintain trust, protection of data security and authentication
3.	Big data Security using Hybrid Cloud	V.P Rao, Gaurav Khandar, Manas Kulkarni, Shubham Nayab	Big data Security by implementing the modified approach for the image and text encryption named as attributed based encryption for the protecting our data from the unauthorized access.	2015	A novel solution for securing the image and text data by using hybrid cloud
4	Discusses Security concerns for Enterprises Migrating to Hybrid Model	Sangwan, Sachin, Sanjay, Shabnam, Sunita Sangwan	In this research address the various security issues in Hybrid migration and Hybrid deployment proposed a solution for securing Authentication using federated ID for Federation identity in hybrid security.	2015	To identify the security issues for Enterprises in hybrid cloud.
5.	Addressing Security in Hybrid Cloud	Sandeep Sahu, Gunjita Shrivastava, Anukrati Dubey	Presents an automatic, intelligent migration service in hybrid cloud based on agent technology, Exploit migration service between our platform and ITRI public cloud on Hadoop.	2013	Proposes a secured intra cloud communication mechanism.
6.	Evaluation Hybrid Cloud in Electronic Government associated Security Risks Analysis and Solutions	D.P. Sharma and Hardayal Shekhawat	Various security issues identity, application, data, information, network and security issues and related solutions in current era that can decelerate its speed in government sector during adaptation.	2012	Security issues and solutions in Hybrid cloud especially for Electronic governance
7.	Survey on securely Hybrid Cloud Distributed Key Generation Authorization for Encrypted Data Deduplication	Navnath Kale, Akanksha Patil ,	Propose secure hashing algorithm for avoiding deduplication, which generates a unique key for each file and also use encryption techniques for security related to data from unauthorized access.	2015	To achieving authorized deduplication with protect data security

III. PROBLEM STATEMENT

The security issues in hybrid cloud include:

- Security controls and data protection
- Identity and access management
- Secure movement of data and workloads across data centers through transport security and network firewalls
- Securing data residing and processed in third-party environments through encryption and tokenization
- Compliance with regulatory and policy requirements
- Poorly constructed SLAs
- Reconfiguration issues
- Shared technology issues

Working with hybrid cloud still requires implementing proper data security and Integrity among these main security issues. In fact, Identity and Access Management involved in data security issues [17]. Data security refers to data confidentiality, integrity, authentication (CIA) in cloud [18].

A. Compliance with Regulatory and Policy Requirements

Not only you have to compensate public cloud and private cloud provider are in compliance audit practices, but you also must demonstrate coordination of other third parties or open-source tools between both clouds is compliant [19].

B. Poorly Constructed SLAs

Many cloud providers such as Amazon, Microsoft, Google and IBM support a large amount of customers by enhancing their web services. To make sure that public cloud provider can demonstrate the infrastructure meet those commitments, options and incentives detailed in the service level agreement (SLAs) [20]. To make trusted private cloud lives up to that similar to the SLA.

C. Reconfiguration Issues

Several issues are resulted due to migration of components from the private cloud to the public cloud due to reconfiguring components in hybrid cloud such as addressing, firewall and component placement [21].

D. Shared Technology Issues

Virtualization technologies are mostly approach in hybird model [22]. VMWare, Microsoft Azure and Amazon EC2 Cloud Storage are few IT Infrastructure services. In virtualized environment, IaaS provider partitioned Virtual Machines (VMs) to multiple clients running on virtualization platform to access same physical server. There is a more prone for accessing data in one virtual machine from another virtual machine on same physical server [23].

Demonstrating threats in hybrid cloud security to introduce a secure authentication framework for hybrid cloud services is required [24]. So we will target numerous threats is shown in Table II and are as follows:

- Man in the Middle Attack (MITM) due to lack of encryption.
- Denial of Service Attacks (DoS) and Distributed Denial of Service Attacks (DDoS).
- Location certification attack.
- Cross Site scripting attack by inside attacker.
- Failure to identify and authenticate.
- Unprotected API exploits sensitive data to malicious attacks.

TABLE II. SECURITY THREATS IN HYBRID CLOUD ENVIRONMENTS

Attack	**Description**
Man in the Middle Attack	Attacker can modify and intercept communications and deploy third party involvement.
Smurf Attack	Attacker uses spoofed IP addresses for purpose of hiding the identity to generate flooded with traffic at the victim machine.
Denial of Service	DoS attacks try to render web service unavailable to users.
Side-Channel Attacks	Attacker gains information about the cryptographic technique.
Viruses and Worms	Attacker may use certain bad source code to compromise.
Tampering with data	An attacker may modify or fabricate information.
Cloud Malware Injection attack	Attacker inject implement of a maliciously service in cloud

IV. CONCLUSION

Hybrid cloud computing is inexorable paradigm where computing is on demand service of private and public both cloud. Emerging technologies related to any application should consider the several possible security threats. The various security issues presented would definitely useful the cloud users to suitable choice and hybrid cloud vendors to handle such kind of threats efficiently. Also, a study of hybrid model a framework of security and requirement of cloud security has been exploited and target with problem considerations. It continuously reduces burden of bulk of cost savings and complexity on users. Organization feels secure about their data against security considerations and fault interruptions. It suggests a robust way of serving user through modernize IT operational agility for service delivery requirements.

REFERENCES

[1] Anupama Prasanth, "Cloud Computing Services: A Survey," International Journal of Computer Applications (0975 – 8887), Volume 46– No.3, May 2012.

[2] Veerawali Behal and Rydhm Beri, "Cloud Computing: A Survey on Service Providers," International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 10 | March 2016

[3] Nitin Kumar, Shrawan Kumar Kushwaha and Asim Kumar, "Cloud Computing Services and its Application," Advance in Electronic and Electric Engineering, Volume 4, Number 1 (2014), pp. 107-112.

[4] Caifeng Zou, Huifang Deng and Qunye Qiu, "Design and Implementation of Hybrid Cloud Computing Architecture Based on Cloud Bus," IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, 2013.

[5] M. Posey, "Journey to the Hybrid Cloud," White Paper Sponsored by: VMware, IDC #242798R2, September 2015.

[6] "Hybrid Cloud 101: Hybrid Cloud Computing - Intel" Intel IT Center Solution Brief | The Path to Hybrid Cloud, September 2013.

[7] K. Annapureddy, "Security Challenges in Hybrid Cloud Infrastructures," Aalto University, T-110.5290 Seminar on Network Security, 2010.

[8] A. Dubey, G. Shrivastava and S. Sahu, "Security in Hybrid Cloud," Global Journal of Computer Science and Technology Cloud and Distributed, Volume 13 Issue 2 Version 1.0 Year 2013.

[9] A. Kumar, "A Comparison of Security Challenges in Public and Private Clouds," International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 3 Issue 3 January 2014.

[10] O. S. Undale and B. Kale, "Achieving Big Data Privacy for Colour Images via Hybrid Cloud," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 11, November 2015.

[11] M. P. Gharat and D. Motwani, "Survey on Establishing Trust, Data Security and Authentication In Hybrid Cloud Computing," International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 11, November 2013.

[12] V. P. Rao, G. Khandar, M. Kulkarni and S. Nayab, "Big data Security using Hybrid Cloud," International Engineering Research Journal (IERJ), Volume 1 Issue 9 Page 957-659, 2015.

[13] Sanjay, S. Sangwan, Sachin and S. Sangwan, "Addressing Security issues for Enterprises Migrating to Hybrid Cloud Computing Model," International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 6 Page 3618 – 3622, 2015.

[14] A, Dubey, G. Shrivastava and S. Sahu, "Security in Hybrid Cloud," Global Journal of Computer Science and Technology Cloud and Distributed, Volume 13 Issue 2 version 1.0 Year 2013.

[15] H. S. Shekhawat and D. P. Sharma, "Hybrid Cloud Computing in E-Governance: Related Security Risks and Solutions," Research Journal of Information Technology, 4(1): 1-6, 2012.

[16] A. V. Patil and N. D. Kale, "A Secure Authorized Hybrid Cloud Distributed Key Generation for Encrypted Deduplication of Data," International Journal of Science and Research (IJSR), Volume 4 Issue 7, July 2015.

[17] K. Subramanian, "Hybrid Clouds," A whitepaper sponsored by Trend Micro Inc, 2011.

[18] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: issues and current solutions," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, pp. 485–498, 2016.

[19] "Critical Security and Compliance Considerations for Hybrid Cloud Deployments," Advisory by 451 Research, Dec 2015.

[20] J. Morin, J. Aubert and B. Gateau, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," https://www.researchgate.net/publication/232617525, 19 May 2015.

[21] M. Hajjat, X. Sun, Y. E. Sung, D. MAltz, S. Rao, K. Sripandikulchai and M. Tawarmalani, "Cloudward Bound: Planning for Beneficial Migration of Enterprise Applications to the Cloud," In SIGCOMM'10, August 30 - September 3 2010.

[22] T. Pradhan, M. Patidar, K. Reddy and A. Asha, "Understanding Shared Technology in Cloud Computing and Data Recovery Vulnerability," InternatIonal Journal of Computer SCIenCe and technology, IJCST Vol. 3, ISSue 4, oCT - DeC 2012.

[23] B. Singh, J. Singh and S. Kumar, "Virtualization Techniques and Virtualization Challenges in Cloud Computing: A Review," IJCAT - International Journal of Computing and Technology, Volume 2, Issue 6, June 2015.

[24] A. Michael, A. Foladoyin and A. Oluyemi, "Threats to Hybrid Cloud Security," International Journal of Scientific & Engineering Research, Volume 9, Issue 2, February-2018.