An Analysis on Secured Live Migration in Cloud Environment

R.Jayamala
Assistant Professor
Department of CSE
University College of Engineering,
BIT Campus, Anna University,
Tiruchirappalli
jayajasmine07@gmail.com

A.Valarmathi
Assistant Professor
Department of Computer Applications
University College of Engineering,
BIT Campus, Anna University,
Tiruchirappalli
valar1030@yahoo.com

R.Gayana
Student – M.E - CSE
Department of CSE
University College of Engineering,
BIT Campus, Anna University,
Tiruchirappalli
22.gayana@gmail.com

***Abstract*— Cloud computing is a computing service which offers several services to the users based on their demands. Nowadays enormous user accessing the clouds which lead to over utilization or underutilization of cloud resource. Live migration is a one of the technique used to avoid either overutilization or underutilization of resources and is a process of moving a virtual machine from the source to destination host without detaching the client or application. Live migration effectuates energy efficiency, load balancing and efficient resource allocation and live migration of virtual machine may bombard to various security menace over integrity, anonymity, authentication and authorization in data plane, control plane and migration plane. Various security methods have been proposed by researchers in the past for enforcing integrity, anonymity, authentication and authorization. This paper scrutinizes the various threats and mechanisms to alleviate bombard during live migration of virtual machine in cloud environment.**

***Keywords*—** Cloud computing, Live Migration, Virtual Machine, Energy efficiency, Integrity.

I. INTRODUCTION

Cloud computing is the firmest emerging technology that revolutionizing IT industry. In recent years cloud computing has attracted significant attention from various fields like trade and academe [1] and it involves hiring different types of services such as software as a service (SAAS), infrastructure as a service (IAAS) and platform as a Service (PAAS) etc. Cloud computing is mainly emanated from the virtualization technology where Virtualization is a process of developing the virtual version of storage, memory, software, network and data. In order to satisfy the demand of cloud, a greater number of virtual machines are hosted on a physical machine. Virtualization permits the sharing of same physical resources among many users which helps to make utilization of resources efficiently and effectively [2].

Virtual machine migration is a major concern of Virtualization. In the fast-growing world, every user wants to get their requested service in less time. Therefore, the load balancing performs a major role in cloud environment [3]. Cloud computing afford service to the huge users with less time using load balancing. Load balancing decreases the imbalance of resources from over all physical machines i.e., it distributes the resources in virtual machines to eliminate the situation of overloading or under loading. In VM migration the VMware moved from one physical host to other host. Similarly, the data of VMs are also gets dispatched from one host to other.VM migration consumes energy both on the machine from which it is being migrated and the machine to which it is being migrated.

During migration of data there is a possibility of risk factors both in terms of qualitative and quantitative factors. The research lies on secure data transfer at the time of migration. Data security predominant research work in cloud computing. Integrity, Authorization, Authentication, Confidentiality and Auditability are the major fundamental priorities which must be controlled during data transmission.

II. REQUIRMENTS OF SECURE VM MIGRATION

Virtual machine migration is a process of migrating VM from source host to destination host without any menace [3].

2.1 INTERGRITY: At the time of migration, source and destination host must be integrated in order to identify and verify the correct destination host. It checks the quality of secure migration. Also, it ensures a trust establishment between source and destination host.

2.2 AUTHENTICATION: During VM migration many attacks and security threats may occur. In order to perform secure VM migration (protecting from attacks and threat) source and destination must have mutual authentication.

2.3 AUTHORIZATION: Appropriate access control policies must be provided to protect live migration. Unauthorized activities, unauthorized user/role and unauthorized migration operation are controlled by access control list (ACL).

2.4 CONFIDENTIALITY: While VM migration the intruders may eavesdrop the data that are being conveyed. To avoid this data should be encrypted before the VM migration.

2.5 REPLAY RESISTANCE: An invader can capture traffic and replay it later to get authenticated in VM migration process. Therefore, live VM migration process should be replay resistant. Nothing can be used to prevent replay attack in migration.

2.6 SOURCE NON-REPUDIATION: Source host cannot deny the VM migration operation. This feature can be achieved by using public key certificates.

III. VM MIGRATION SECURITY ATTACKS

At the time of VM migration security attacks would take place in three different place they are (i) Control plane (ii) Data plane and (iii) Migration module [4].

3.1 CONTROL PLANE:

In control plane, communication mechanisms would take place at the time of VM migration. Live migration should function safely against robust attacks. Throughout Live VM migration, the VMM must be authenticated.

In control plane intruder may gain the control of live migration this may lead to DOS attack, unnecessary VM migration etc.

3.2 DATA PLANE:

In data plane, data communication occurs between VM migrations. In data plane, during live migration data are transmitted from one host to other. During migration of data from source to destination, intruders may have a chance of changing the data or collecting the information.

In data plane possible attacks are active attack, passive attack, Man-in-middle-attack and snooping.

3.3 MIGRATION PLANE:

Activation and monitoring are performed by the migration module.

In migration module integrity related problems would take place.

IV. CATEGORIES OF ATTACKS

The vulnerability of cloud can be categorized based on three different participants such as Cloud, User and Service [5-6]. Based on the participants the attacks are categories into six types. They are listed in the Table.1.

Table1. Categories of Attacks

Categories	Attacks	Data Plane	Control Plane	Migration Plane
Service-to-User	In databases • Sql injection • Buffer overflow etc.,	✓	X	X
User-to-Service	Client based application • web browsers • API communication Common vulnerabilities • SSL certificates • cache poisoning	X	✓	X
Cloud-to-Service	• Denial of service	X	✓	X
Service-to-Cloud	• Data tampering • Privacy • Eavesdropping	✓	✓	✓
Cloud-to-User	• No direct contact point to users	X	✓	✓
User-to-Cloud	• Phishing • Scams triggering • Manipulating the user to provision unwanted cloud resources • Incorrect billing details	✓	✓	✓

V. RELATED WORKS

The related works with their algorithms and their metrics are explained below.

Osama Alkadiet.al., explains about various security threats on VM migration[5-6]. This paper explains about the collaborative anomaly detection system. Two different algorithms are used for identifying the attacks and unusual patterns. The Mixture Localization-based Outliers algorithm is used for identifying inside and outside attackers and the Gaussian-mixture models is used to identify unusual patterns in network traffic data. This paper provides integrity and confidentiality.

Dr. Subarna Shakya et.al, illustrates about the data migration. This paper explains about the overview of data security and solution for the Data Migration Privacy Framework. For secure data transmission a Secure Socket Layer (SSL) [7] protocol is established between source and destination nodes. Temporary session key, random key, symmetric encryption and migration tickets are the security parameters are majorly used and it is concerned for authentication with minimum privilege. Migration tickets are mutually transmitted between the channels. In addition, the encryption of data is made by prediction-based encryption (PBE). Prediction based encryption is the combination of Identity Based Encryption (IBE) and Attribute Based Encryption (ABE). Application taken in this paper is healthcare systems and e-commerce networks. Sensitive and non-sensitive information strictly differentiated and sensitive data are encrypted.

D.suneetha et. al, in this paper describes about the data security. Data security is most challenging issue in cloud computing. In order to secure data, the data are encrypted using the artificial neural network [8] and the sensitive data are identified using dynamic fragments model. The main objective of this paper is to store the data in secure manner.

Prashant Sahatiya et.al, illustrates about the secure data migration. Advanced Encryption Standard (AES) is used for data encryption and Elliptic Bend Diffie-Hellmann Plan [9] is being used for generating the shared key between the hosts for verifying the authentication and authorization. After verifying the security, the VM is migrated securely.

Gokul Geetha Narayanan et al., demonstrates about the various attacks and method to overcome the attacks at the time live VM migration. At the time of VM migration data are transmitted from one host to another, intruders may eavesdrop, data tamper would take place. To enhance secure VM migration IP Sec protocol and onion routing algorithm [10] is used.

Anitha H Met.al., exemplifies software defined networks (SDN) is used for secure VM migration. SDN controller will contain the detailed information about the resource utilization of host. Capability based Access control list (CACL) is maintained in the SDN controller [11]. CACL is used to build collaboration framework between hypervisor and SDN controller in order to provide secure VM migration. Integrity and confidentiality are the security parameters used.

Masahiro Hijiet.al., represents block chain technique is most conventional technique. The policy management technique using block chain [12] method has been familiarized to overcome the problem occurs during VM migration. Data can be migrated without inspecting the information about the server running on the VM.

Tengchao Ma et al., explains about the resource scheduling problem. This problem may influence on energy consumption and the resource utilization of active physical and virtual machine security. Security enhanced particle swarm optimization algorithm [13] is used for secure VM migration and number of VM migration is reduced by enhancing security. Roulette wheel goal is to achieve long term optimization. The overall energy consumption, resource usage, SLA violation rate and secure VM migration efficiency of SE-PSO is good on compared with standard PSO.

Devi Radha Ranet.al., describes about the secure data transmission and detection. The B-tree Huffman Encoding (BHE) algorithm are used for data packets compression, the Modified Elliptic curve cryptography (MECC) algorithm is proposed which encrypts the data packets and transmits it to a receiver. Deep learning Modified Neural Network (DLMNN) classifier, which assess the received data packet IP-address [14].

Pengcheng Wei et.al., depicts the idea of block chain integrity protection mechanism. This method helps to overcome the data tampering problem. 'Block-and-response'' [15] mode is used to construct a blockchain-based cloud data integrity verification scheme.

Sambit Kumar Mishra et al., discuss about the learning automata algorithm is to optimize the make span of the cloud system and improve the resource utilization that provides a secure resource allocation. Finite set of tasks is allocated to ALOLA [16] to determine the make span of the cloud system. System performance is to compare with learning and without learning automata.

Virendra Singh Kushwah et.al narrates about the data tampering at the time of VM migration. In recent years cloud user has been increased to certain extern, since the user increase still worry about the security provided by the cloud service providers. In order provide security the data stored is being encrypted. In this paper prediction-based encryption [17] is used for encrypting the data. So, this would help to overcome the data tampering problem this would provide integrity and confidentiality.

Sebastian Biedermannet.al., explains about the secure data migration [18]. This uses Live Migration Defense Framework (LMDF) which is used to detect delay for a live migration and to take security related tasks in additionally gained time. LMDF would provide high integrity and confidentiality

Xin Wanet. Al., demonstrates the trusted VM migration. This paper proposes the improved secure virtual trusted platform module (vTPM) migration protocol [19]. A trusted channel and property-based attestation of destination platform is used to assure the security requirements of the vTPM migration.

Wei Wanget.al explains about method [20] to improve security in virtual machine live migration. Policy controlled secure live migration that is based on Intel vPro hardware platform for protecting the virtual machine migration. Policy controlled secure live migration framework has been proposed to verify the level security to reach the destination and to provide security for hypervisor and Virtual machine running on it.

The comparison of security algorithms with their performance metrics are tabulated in Table 2.

COMPARISON OF SECURITY ALGORITHMS WITH ITS PARAMETER METRICS

Topic	Algorithm Used	Integrity	Confidentiality	Availability	Authentication	Authorization	Replay resistance	Non repudiation
Mixture Localization-Based Outliers Models for securing Data Migration in Cloud Centers (2019)	Mixture Localization-based Outliers (MLO) and Gaussian-mixture	Yes	Yes	No	No	No	No	No
An Efficient Security Framework for Data Migration in A Cloud Computing Environment (2019)	Secure Socket Layer (SSL) and Prediction Based Encryption (PBE)	Yes	Yes	Yes	Yes	Yes	No	No
Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment (2019)	Artificial Neural Network and The Dynamic fragments model	No	Yes	No	No	No	No	No
Secure Live Virtual Machine Migration in Cloud Computing (2019)	AES, SHA-256 ECDH	Yes	Yes	No	Yes	Yes	No	No
Securing VM migration through IPsec tunnelling and onion routing algorithm (2018)	IPsec tunnelling and onion routing algorithm	Yes	Yes	No	Yes	Yes	No	No
SDN Based Secure Virtual Machine Migration in Cloud Environment (2018)	SDN	Yes	Yes	No	No	No	No	No
Policy Management Technique Using Block chain for Cloud VM Migration (2019)	Block chain	No	Yes	No	Yes	Yes	No	No
SE-PSO: Resource Scheduling Strategy for Multimedia Cloud Platform Based on Security Enhanced Virtual Migration (2019)	Particle Swarm Optimization and roulette wheel	No	Yes	Yes	No	No	No	No
Secure Data Transmission and Detection of Anti- forensic attacks in Cloud Environment using MECC and DLMNN (2019)	B-tree Huffman Encoding (BHE) algorithm, Modified Elliptic curve cryptography (MECC), Deep learning Modified Neural Network (DLMNN) classifier	Yes	Yes	Yes	Yes	Yes	No	No
Block chain data-based cloud data integrity protection mechanism (2019)	Block chain	yes	No	No	No	No	No	No
A Secure VM Consolidation in Cloud Using Learning Automata (2019)	ALOLA: Algorithm for Optimal Allocation using Learning Automate	No	Yes	No	No	No	No	No
A Security approach for Data Migration in Cloud Computing	prediction-based encryption	Yes	Yes	No	No	No	No	No
Improving Security of Virtual Machines during Live Migrations (2013)	live migration defence framework	No	Yes	No	Yes	No	No	No
An Improved vTPM Migration Protocol Based Trusted Channel (2012)	improved secure vTPM migration protocol	Yes	No	No	Yes	Yes	Yes	Yes
Secured and Reliable VM Migration in Personal Cloud (2010)	hypervisor based fault tolerance technology (HBFT),	No	Yes	No	Yes	No	No	No

Table 2. COMPARISON OF SECURITY ALGORITHMS WITH ITS PARAMETER METRICS

VI.CONCLUSION

In this paper, several security requirements, different types of security attacks and various categories of attacks classes are discussed. And the comprehensive analysis is performed for the secure live VM migration based on the various security measures (requirements).

In future we plan to propose a model which decreases the power consumption as well as enhance the security for VM migration by taking into account number of attacks which occur in data plane, control plane and migration module and it should meet all the performance requirements.

REFERENCES

[1] Princess, J.P., Paulraj, G.J.L. and Jebadurai, I.J., "Methods to mitigate attacks during live migration of virtual machines—a survey". Int. J. Pure Appl. Math, 118(20), pp.3663-3670 2018.

[2] Geeta and Shiva Prakash" Role of Virtualization Techniques in cloud Environment",Advance in Intelligent Systems and computing, PP 439-450, 2019

[3] Divyambika, R. and Umamakeswari, A., "Protection of virtual machines during live migration in cloud environment". Indian Journal of Science and Technology, 8(S9), pp.333-9 2015.

[4] Choudhary A, Govil, M.C., Singh, G., Awasthi, L.K. Pilli, E.S., & KapilD., "A Crititcal survey of live virtual machine migration techniques", Journal of Cloud Computing, Vol.6(1), Issue.23, 2017.

[5] N. Gruschka and M. Jensen, ''Attack surfaces: A taxonomy for attacks on cloud services,'' in Proc. IEEE 3rd Int. Conf. Cloud Comput., Jul. 2010, pp. 276–279

[6] AlKadi, O., Moustafa, N., Turnbull, B. and Choo, K.K.R., "Mixture Localization-Based Outliers Models for securing Data Migration in Cloud Centers"., pp.114607-114618 IEEE Access 2019

[7] Shakya, S., "An Efficient Security Framework for Data Migration in A Cloud Computing Environment". Journal of Artificial Intelligence, 1(01), pp.45-53 2019.

[8] D.suneetha, D.Rathnakumar, G.G.S.Pradeep, " Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment", International Journal of Recent Technology and Engineering, Vol. 8, Issue. 2, July 2019.

[9] Sahatiya, P. and Shah, H., "Secure Live Virtual Machine Migration In Cloud Computing", 6(1), pp.176-182 IJRAR-International Journal of Research and Analytical Reviews (IJRAR) 2019.

[10] Narayanan, G.G. and Saravanaguru, R.K., "Securing VM Migration Through IPsec Tunnelling and Onion Routing Algorithm". In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 364-370). IEEE 2018, June.

[11] Anitha, H.M. and Jayarekha, P., "SDN Based Secure Virtual Machine Migration in Cloud Environment". (pp. 2270-2275) In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE 2018 September.

[12] Uchibayashi, T., Apduhan, B.O., Shiratori, N., Suganuma, T. and Hiji, M., "Policy Management Technique Using Blockchain for Cloud VM Migration". In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 360-362). IEEE 2019, August.

[13] Ma, T., Xu, C., Zhou, Z., Kuang, X. and Zhong, L., "SE-PSO: Resource Scheduling Strategy for Multimedia Cloud Platform Based on Security Enhanced Virtual Migration", In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 650-655). IEEE 2019, June.

[14] Rani, D.R. and Geethakumari, G., "Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN", 150, pp.799-810, Computer Communications 2020.

[15] Wei, P., Wang, D., Zhao, Y., Tyagi, S.K.S. and Kumar, N., "Blockchain data-based cloud data integrity protection mechanism", 102, pp.902-911 Future Generation Computer Systems, 2020.

[16] Mishra, S.K., Sahoo, B. and Jena, S.K., "A Secure VM Consolidation in Cloud Using Learning Automata". In Recent Findings in Intelligent Computing Techniques (pp. 617-623), Springer, Singapore 2019.

[17] Kushwah, V.S. and Saxena, A., "A security approach for data migration in cloud computing". International Journal of Scientific and Research Publications, 3(5), pp.1-8 2013.

[18] Biedermann, S., Zittel, M. and Katzenbeisser, S., "Improving security of virtual machines during live migrations". In 2013 Eleventh Annual Conference on Privacy, Security and Trust (pp. 352-357).IEEE 2013, July.

[19] Wan, X., Zhang, X., Chen, L. and Zhu, J., "An improved vTPM migration protocol based trusted channel". In 2012 International Conference on Systems and Informatics (ICSAI2012) (pp. 870-875). IEEE 2012, May.

[20] Wang, W., Zhang, Y., Lin, B., Wu, X. and Miao, K., "Secured and reliable VM migration in personal cloud", In 2010 2nd International Conference on Computer Engineering and Technology (Vol. 1, pp. V1-705). IEEE 2010, April.