An Analysis of Using Augmented Security Techniques to Shield Virtualized Resources in Cloud Computing

Sujata[1], Dr. Brij Mohan Goel[2]
[1]*Assistant Professor, Department of Computer Science, Pt. NRS Government College, Rohtak)*
[2]*Professor, Department of Computer Science & Engineering, Baba Mastnath University, Asthal Bohar, Rohtak*

Abstract- This study describes how a mobile network that relies on inter-node cooperation to enhance communication is known as an intermittently connected network (ICN). Here this collaboration involves nodes delivering messages from other nodes to specified locations. There is no need for ICN infrastructure and nodes do not store routing data. Although this environment can facilitate message dissemination, it introduces routing issues. This environment may facilitate the dissemination of the message, but it raises questions of routing. Ensuring good delivery performance is particularly difficult in the absence of accurate routing information or network infrastructure. This study extends the potential of context-aware approaches to delivery in information-centric networks (ICNs). This analyzed context-aware strategies incorporate personal, historical, and environmental factors, which are different from the initial and widely used ICN routing algorithms. Extensive simulation results show a 15 percent increase in delivery probability when context-aware ICN routing techniques are used.

Keywords- Cloud Computing, Information-Centric Network (ICN), Network Security, Security Technique, Virtualized resources, Legacy Web Applications.

I. INTRODUCTION

The dissemination and attainability of data have been totally changed by the emergence of information-centric networking (ICN), but routing problems still exist. Guaranteeing best delivery performance is particularly hard without network infrastructure or routing data. This study utilizes context-aware methodologies to enhance transfer likelihood in an Information-Centric Network (ICN). Considerable simulation results indicate a 15 per cent enhancement in delivery probability when employing context-aware ICN routing methodologies. The findings firmly suggest that incorporating context-awareness into ICN routing algorithms can remarkably enhance the overall delivery success rate. Taking into account a range of contextual aspects such as environmental conditions, historical data, and individual preferences allows for more precise customization of routing decisions to meet the network's specific requirements. Hence, the efficiency and effectiveness of information distribution in ICNs can be remarkably improved, resulting in a more trust worth and responsive network infrastructure. This research make possible future research and development in utilize context-aware techniques to improve routing strategies in ICNs.

Cloud Computing and Virtualized Resources:
Cloud computing defines the provision of computing services via the Internet, enabling exposure to and storage of data and programs on distant servers rather than local equipment. Virtualized resources demand the generation of virtual presentations of hardware, storage, and networking elements etc., enabling users to evaluate and allot resources as desired without physical limitations. Organizations can get upgraded flexibility, scalability, and cost-efficiency in managing their IT infrastructure by incorporating these technologies.

Significance of Security in Cloud Environment:
Security is very important in cloud computing, as organizations are consigning their sensitive data and applications to external service providers. In today's era, it is very difficult to protect the confidentiality, integrity and availability of data and protect it from various security threats. Implementing strong security measures, like encryption, digital signature, login id & passwords, and monitoring tools, can decrease risks and protect critical information on the cloud. To enhance the security measure, several organizations are also make use of advanced security techniques likes threat intelligence, multi-factor authentication etc. Investing in enhanced

security measures is very difficult for businesses aiming to save their cloud environments and uphold the faith of their stakeholders.

Objectives and Methodology of the Study:

The primary objective of this study is to evaluate various cloud security systems in preventing and mitigating cyber threats. And for this, an in-depth study of the current literature on cloud security will have to be done. The researcher conducted interviews with industry professionals to understand best practices and upcoming challenges in this study. The research took an in-depth look at organizations that have effectively deployed sophisticated security measures in their cloud settings. It aims to provide valuable insights and advice to organizations looking to improve their cloud security posture.

Operation Models in Cloud Environment:

Different operating models pose different security challenges, so organizations must carefully analyze and implement security measures for their cloud data and apps. These operational models are discussed below;

i) Public Cloud: In Public cloud availability of computing services are provided by third-party vendors. Although its provide convenience and cost efficient services, businesses should impose caution when sharing authenticated and sensitive data on these platforms due to excess security threats. Businesses should impose robust cryptography techniques and access limitations to safeguard the confidentiality, integrity and authenticity of their data in this cloud.

ii) Community Cloud: These services are utilized collectively by different businesses having common interests. These businesses participate to handle a secure and private cloud resources customize to their personal requirements. Businesses make use of this kind of cloud must implement explicit protocols for accessing data and sharing among members to uphold data privacy, security and authenticity.

iii) Hybrid Cloud: These clouds combine components of both public and private clouds, enabling businesses to fit their distinct requirements. This adaptability allows businesses to credit the scalability and cost-efficiency of public cloud services. Businesses can improve their cloud environment by using the benefits of both public and private.

iv) Private Cloud: In a Private cloud environment all computing resources are dedicated to a single user. Private cloud model provides enhance security, privacy and authenticity as all resources are used delicately by the businesses. These clouds are best for organisations with sensitive information that should not be disclosed on a public cloud.

Cloud Computing Vulnerabilities:

It is essential to safeguard an extensive number of highly sensitive applications and systems from unknown and undiscovered vulnerabilities that hackers target.

i) Unpatchable Systems: Embedded medical devices, kiosks, point-of-sale systems, and other systems are frequently seen as unpatchable. Often, low-bandwidth networks for distant areas make the installation of substantial patches overly time-consuming or too expensive. Sometimes, regulations or agreements regarding reliability constraints may hinder system patching.

ii) Legacy Web Applications: SQL Injection attacks on web applications are the primary cause of the majority of broken records. Web applications are particularly vulnerable due to their inherent accessibility to attackers. Furthermore, the complexity of substance and utility is increasing, and developers are often inadequately trained in secure programming development practices. Edge security will not safeguard these networks, and it may be difficult to identify and provide the specialist resources for development essential to amend the coding.

iii) Enterprise Applications: Operating systems, databases, servers, and diverse applications frequently exhibit substantial basic programming flaws over time. Mitigating such vulnerabilities may be difficult, involving an update of systems and impacting administrative-level viewpoints. Resolving and implementing it effectively may need considerable time.

iv) Unsupported Operating Applications: Patches cannot be developed for obsolete operating systems and programmes that are close to the end of life, especially Solaris 8 and Oracle 10.1. The length of time and costs involved in migrating to a fresh layout are sometimes excessively expensive, causing organisations to pursue quick and affordable solutions. Despite the discontinuation of assistance with Windows 2000 in July 2010, virtual patches became the default inexpensive approach to

safeguard assurance for this and other unsupported platforms.

II. REVIEW OF LITERATURE

Lombardi and Di Pietro (2011) have underscored the risks associated with cloud computing and the unaddressed security issues therein. They proposed a unique design, the Advanced Cloud Protection System (ACPS), to augment the safeguarding of the integrity of guest virtual machines and cloud infrastructure components. ACPS may be utilised in many cloud systems, effectively managing guest and infrastructure components while ensuring transparency for virtual machines and users. It may locally address security breaches and notify the security management layer. A prototype of the ACPS idea has been developed on Eucalyptus and Open ECP and assessed against various workloads.

According to P. Jain (2012), the approach to cloud computing integrates the concepts of "software-as-a-service" and "utility computing" to deliver easy, upon request solutions to clients. There are many difficulties and challenges related to data security in cloud computing. The cloud service provider must ensure that the cloud service consumer's data is safe. In order to damage the whole network of cloud services and impact multiple clients using the exposed service, an attacker can enter the system by assuming to be a genuine user. This research initially highlights the characteristics that affect cloud security, and then examines the security challenges and issues faced by cloud service providers and consumers, including data security, privacy concerns, and compromised applications. It also discusses strategies to deal with these issues and challenges.

A. Patel, M. Taghvi, K. Bakhtiari, J.C. Jr. (2013) indicated that the decentralised and accessible characteristics of cloud computing and associated services make it a tempting focus for possible cyber assaults by adversaries. Intrusion Detection Prevention Systems (IDPS) are generally inadequate for conventional reconnaissance and deployment in cloud computing settings. The paper provides a comprehensive taxonomy by examining recent developments in intrusion detection and prevention systems (IDPS) and alert management strategies. It examines and rectifies violations inside the cloud computing environment. A compilation of pertinent needs has been assembled to satisfy the criteria of IDPS and cloud computing systems: autonomous computing self-management, ontology, risk management, and fuzzy theory.

The study by Qiu, Gai, Thuraisingam, and Tao (2018) highlights the challenge of safeguarding consumer privacy owing to evolving risks from internal as well as external service providers of emerging technologies in the financial sector. The research proposes a Proactive Dynamic Secure Data Scheme (P2DS) to safeguard the personal information of financial clients using Attribute-Based Access Control (ABAC) and data self-determination frameworks. This framework employs two primary algorithms: (i) the Attribute-based Semantic Access Control (A-SAC) algorithm and (ii) the Proactive Determinative Access (PDA) algorithm. This study emphasises the integration of a semantic methodology for enforcing data access, prioritising user-centric strategies to safeguard users' data against illicit cloud activities.

III. RESEARCH GAP

Further evaluation is required to assess the expandability of ACPS in expansive cloud settings and to investigate its efficiency in real situations with multiple complexities. Moreover, ample testing is mandatory to verify the performance and security benefits of ACPS. Treating these research gaps will build up our understanding of ACPS's ability to enhance the security and integrity in cloud environment. Virtualization management in IaaS allows developers to increase control over security, but numerous safety issues remain in practice. As virtualisation proliferates within the information society, the imperative to maintain control over data intensifies. The security responsibilities of the provider and the client differ markedly between cloud service types. Amazon's Elastic Compute Cloud (EC2) infrastructure mandates vendor accountability for security up to the hypervisor, however Adrian et al. (2009) asserts that the customer has responsibility for security measures pertaining to the IT system, encompassing the operating system, applications, and data. To bolster security and foster consumer confidence in cloud computing services, all management and control interactions between cloud providers and clients must transpire through secure channels that provide authentication, authorisation, confidentiality, integrity, and accountability. Providers must provide robust mutual authentication mechanisms to fortify the security of consumer accounts. Providers

must guarantee that the chosen passwords are robust and sent exclusively over encrypted means. Enhanced access surveillance is advised to prevent unauthorised access. Ultimately, upholding responsibility and adherence to established security protocols necessitates the implementation of secure virtualisation management, restricting employee access to resources, and conducting frequent audits of all authorised access. They are described as follows:

1) Impact of Deployment Mode: The cloud deployment method IaaS uses for its delivery is susceptible to various levels of security vulnerabilities. The public cloud presents a significant risk, while the impact of the private cloud appears to be minimal. Physical security of infrastructure and disaster management is paramount in the event of any damage to infrastructure (whether natural or malicious). The infrastructure includes the equipment used for data processing and storage as well as the channels through which it is accessed.

2) Security rules: It is essential to establish, delineate, and execute security protocols in a machine-readable and uniform manner to facilitate access control, resource distribution, and other decision-making processes. The legislation pertaining to this matter should be sufficiently robust to enable automated enforcement of licenses and service level agreements (SLAs).

3) Service Automation: Security audits are made easier by an automated system that analyses and regulates the security and process control flow. This encompasses providing notification of any occurrence that contravenes security regulations or customer licence agreements.

IV. CONCLUSION

In conclusion, order for businesses to safeguard their data and resources, a detailed security architecture should be implemented. Enterprises can commit regulatory compliance and improve their security operations by adding advanced technologies for monitoring and improving security protocols. This strategy enhances security measures and refines overall efficiency in maintaining security issues. Enterprises must classify the establishment of thorough security measures to safeguard against major cyber threats. In addition, raising security awareness and providing continuous training to employees helps in mitigating any kind of risks and ensures that all employees of the firm are prepared to protect sensitive information. Developing adequate safety protocols is crucial in current digital landscape to preserve confidence among stakeholders and safeguard against cyber threats.

REFERENCES

[1] Hashizume Keiko, Rosado, David G., Fernández-Medina, Eduardo(2013), "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services, February 27, https://doi.org/10.1186/1869-0238-4-5

[2] Hussein, N. H., & Khalid, A. (2016). "A Survey of Cloud Computing Security Challenges and Solutions", International Journal of Computer Science and Information Security, Volume 14(1), Page No. 52.

[3] Jain, P. (2012), "Security Issues and their Solution in Cloud Computing", Journal of Computing & Business Research, pp. 2229-6166.

[4] Lombardi F, Roberto Di Pietro (2011), "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, Elsevier, July, Volume 34, Issue 4, pp. 1113-1122.

[5] M Qiu, K Gai, B Thuraisingham, L Tao (2018), "Proactive User-Centric Secure Data Scheme Using Attribute-based Semantic Access Controls for Mobile Clouds in Financial Industry", Future Generation Computer Systems, pp. 421-42.

[6] Nzanywayingoma Frederic, Yang Yang (2017), "A Literature Survey on Resource Management Techniques, Issues and Challenges in Cloud Computing", TELKOMNIKA, Volume 15, Issue 4, December, pp. 1918-1928.

[7] Patel A, Taghavi M, Bakhtiyari K, JúNior JC. (2013), "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review", Journal of Network and Computer Applications, January 31, Volume 36(1), pp. 25-41.

[8] So, K. (2011). "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks, Volume 3(5), pp. 247-55.

[9] Sugumaran, M., Murugan, B. B., & Kamalraj, D. (2014). "An Architecture for Data Security in Cloud Computing", In 2014 World Congress on Computing and Communication Technologies (WCCCT), IEEE, February, pp. 252-255.

[10] Zissis, D., & Lekkas, D. (2012). "Addressing Cloud Computing Security Issues", Future Generation computer systems, Volume 28(3), 583-592.