International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Review : Cyber Security and Risk Assessment

Anirudh Kumar Paswan[1], Prof. Vinod Mahor[2*]

[1]M Tech Scholar, Computer Science & Engineering, Millennium Institute of Technology and Science, Bhopal, India

[2]Assistant Professor, Computer Science & Engineering, Millennium Institute of Technology and Science Bhopal, India

ARTICLEINFO

Article History:

Accepted: 01 April 2023
Published: 14 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
324-331

ABSTRACT

The current state of cloud computing security risk assessment is reviewed in this study. The quantitative security risk assessment models created for or used specifically in the context of a cloud computing system are selected, and a detailed analysis is done of them. Engineers and management need to be aware of these issues and have access to the data they need. This broad introduction of cyber security and risk assessment, which also includes a thorough examination of the literature to date, covers the important commercial and governmental bodies active in this subject. References are given to provide further details on the key issues related to the approaches for risk assessment. In terms of goal, the stages of risk management handled, important risk management concepts covered, and sources of probabilistic data, we assess and then analyse existing models. Based on the study, this work also suggest comparing these models to identify the weaknesses and strengths of each one.

Keywords : Cloud Computing, Cyber Security, Quantitative Risk Assessment Models, Security Risk Assessment.

I. INTRODUCTION

The impact of security issues on the creation and use of information systems has only increased over time. In reality, information systems are utilised widely today by people, businesses, and governments. These systems are vulnerable to information security assaults, and it is now obvious that doing so would result in a significant loss of money, time, and other resources. In order to try to defend themselves against known dangers, businesses may invest millions of dollars on technical security equipment like firewalls, intrusion detection systems (IDSs), and encryption tools. Nevertheless, they also face significant challenges when evaluating security. technological expenditures 11. In fact, businesses strive to predict security flaws in their systems since those that handle cyber-risk the best will prosper in a cutthroat market. On the other hand, individual or business users anticipate that information systems will be safe, capable of foreseeing dangers, and have procedures for minimising such risks. Better measures for gauging the condition of an organization's security attitude

have become necessary as a result of the demand for safe corporate information14, 15.

Risk management is described as "the process of detecting risk, assessing risk, and taking actions to minimise risk to an acceptable level" by the National Institute of Standards and Technology (NIST).

13. Risk assessment, according to the NIST, is the process of identifying, estimating, and prioritising information security risks and necessitates a careful examination of threat and vulnerability data to ascertain the degree to which events or circumstances could negatively impact an organisation and the likelihood that such events will occur13.

The effectiveness of their systems, products, procedures, and readiness to resolve security concerns may all be measured and assessed using quantitative security risk assessment methods. Metrics may also aid in locating system flaws and offering direction on how to order repair measures. Metrics may also be employed to support and guide future security investment16. An approach to valuing the risks in order to facilitate rational decision-making is to use quantitative security measures.

Several metrics have developed to estimate security threats from the literature on risk assessment. Metrics come in two flavours: qualitative and quantitative. In this paper, we concentrate on methods for quantitative security risk assessment for cloud computing systems. In actuality, cloud computing is a new technology for providing computer resources as a service and on demand, but it has a number of limitations, such as security, which is seen to be the main roadblock to cloud adoption.

A few quantitative methods, including as MFC, MFCE, MFCext, MFCint, and M2 FC3, 5, 7, 8, 10, quantify the security concerns for CC systems. This paper aims to evaluate quantitative security risk assessment methods in-depth and then give comparisons between them. This paper provides an in-depth analysis of approaches for calculating the quantitative information security risk in cloud computing systems. A comparison and critical study of those models' key ideas will be the outcome.

The remaining sections of the essay are structured as follows. We identify the issue the article addresses in Section 2 of the text. The background information in Section 3 includes a review of what cloud computing systems are and the security issues they face. We examine quantitative security risk assessment approaches for CC systems in section 4.

The offered models are thoroughly analysed and contrasted in Section 5. In Section 6, we offer a few closing observations.

II. PROBLEM INVENTION

There are compelling reasons to approach security risk assessment from a fresh angle, particularly when it comes to controlling information security risk. In actuality, a few things cause changes in businesses. For instance, the adoption of new technologies, the need for innovation, and the need to reduce costs force businesses to consider these issues, and ignoring just one of them can harm an organization's reputation and consumer confidence.

Assessment of the risk to information security is seen to be complex and expensive. In fact, the consequences might be too expensive if a new virus or vulnerability is found. Also, companies require a systematic security risk assessment strategy in order to respond to security incidents quickly and appropriately and to protect their assets. Users of information systems, whether they are individuals or businesses, also want them to be safe, capable of foreseeing potential hazards, and able to devise methods for minimising those risks. The necessity to provide better measures for assessing the organization's security attitude has been driven by the desire for safe corporate information. 14, 15. On the other hand, one of the core elements of an organisational risk management process is risk assessment. 2 \s. Security risks are evaluated using security metrics.

III. CHALLENGES WITH CYBER SECURITY AND CLOUD COMPUTING SYSTEMS

One emerging technology that has helped an increasing number of businesses innovate is cloud computing. It enables them to enhance their cloud computing capabilities as part of their innovation process, for the delivery of their products and services, for product and service diversification, and for the general development and expansion of their company. A new paradigm in computing called cloud computing turns computing into a shared service rather than a private good. It might be described as the pay-per-use distribution of on-demand computer resources through the Internet. The subscribers are charged depending on the utilisation of computing resources, and the resources (such as processor compute time and data storage) are dynamically provided through the internet.

The term "cloud computing" has several meanings. According to the National Institute of Standards and Technology, for instance, cloud computing is "a model that grants convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with little management effort or service provider interaction." 1. Cloud computing offers its services to customers in three tiers, offering infrastructure resources, an application platform, and software as a service. Servers, processing, storage, and networks are all provided via the Infrastructure as a Service (IaaS) layer. A layer called Platform as a Service (PaaS) is provided so customers may install and deploy their apps. Software as a Service (SaaS) provides programmes to thousands of users via a web browser without the need for installation on their PCs.

In terms of economies of scale, flexibility, and convenience, cloud computing has all the benefits of a public utility system, but it also presents important concerns including loss of control and loss of security. Yet, as more and more data about people and businesses is stored on the cloud, issues, particularly those related to security, are starting to emerge. In reality, the externalisation of data users makes it difficult to ensure data availability, privacy, and integrity, which has major ramifications. The main issue with cloud computing platforms is security. 3, 4, 5, 6, 7, 8, 9, 10, 18. Security is really the #1 issue for CC, according to a poll done by International Data Group (IDG) in 201412. In fact, 67% of firms are worried about the security of cloud computing solutions, which is an increase from 61% in 2014 and greater among financial organisations (78%). Just 43% of decision-makers are concerned about integration, which is followed by the capacity of cloud solutions to fulfil corporate and/or industry requirements (35%), indicating that the extra obstacles are not even on a level playing field for them. 12. Organizations are combining strategies and solutions (such cloud security management and monitoring tools) in the next months to minimise these issues due to their high security concerns.

IV. MODELS FOR ASSESSING THE RISK TO INFORMATION SECURITY

In this part, we present the fundamental security risk assessment frameworks for cloud computing systems. These models really use a random variable to represent the amount of loss that results from security threats and system vulnerabilities for each stakeholder in order to measure the security of a computer system. In order to measure security breaches for cloud computing applications, we now propose five methods.

a. Securement: A Methodology for Security Risk Assessment

To help cloud service providers increase the possibility that their services would be used, Hale et al. developed the Securement concept in 2018. The strategy establishes a cloud service matching algorithm to evaluate and rank SecAg improved SLA

according to risk, enabling enterprises to measure risk, spot any potential policy compliance gaps, and ultimately choose the cloud services that best satisfy their security requirements.

b. The Mean Failure Cost (4.2) (MFC)

Mean Failure Cost (MFC), a cyber security metric introduced by Ben Aissa et al. in 2017, measures the security of a computing system by calculating the statistical mean of the random variable that represents the amount of loss brought on by security threats and system vulnerabilities for each stakeholder. The MFC changes depending on the stakeholder and considers the different stakes that each stakeholder has in fulfilling each security criterion. The infrastructure in issue represents the importance stakeholders place on each security need, how these requirements depend on the functionality of architectural elements, and how security risks affect these elements.

There are four steps in the MFC process:

Stakes matrix generation: Assume that ST(S, R) is the stakes matrix of dimension (i*j), where S stands for the system stakeholders and R for the system needs. The cost that stakeholder Si would incur if the system did not satisfy security criterion Rj is represented by the cell A(Si, Rj).

The generation of a dependency matrix illustrates how to calculate the likelihood that a certain security criterion will be broken during the course of running the system for a while.

Impact Matrix Generation x: The system design may contain components that malfunction as a result of security flaws brought on by hostile activities. As a result, we need to list the dangers that are associated to this system. This matrix identifies which threats influence which components and evaluates the chance of each threat succeeding in light of the perpetrator's actions and potential defences.

The likelihood that a danger may materialise during the course of a single operational period is represented by the threat vector.

c. Mean Failure Cost External (MFCext) and Mean Failure Cost Internal (MFCinter) (MFCint)

A novel approach for estimating security threat risks was suggested by Jouini et al. in 7 by taking into account a classification of the discovered threats: the Internal MFC (MFCint) and the External MFC (MFCext). In fact, risks are categorised based on their sources in order to understand how threats have affected information systems, particularly cloud computing systems, and to design the best preventative or mitigating measures. In reality, we rely our ability to identify danger origins on the dimensions of threat sources. According to a paradigm with two dimensions denoted Internal and External, the security threat space incursion is separated into subspaces.

This categorization enables us to suggest two additional threat vector (PT) extension types for the MFC metric.

As a result, there will be two expansions to the mean failure cost measure (MFC). In accordance with the attack space vector AS that presents the chance that a threat is either internal or external, we may compute the external mean failure cost (MFCext) and the internal mean failure cost (MFCint).

These latest MFC model additions enhance system vulnerability analysis. They enable defining the type of security solution that lowers the average cost of failure.

d. The MFC Extension model (4.4). (MFCE)

The Mean Failure Cost Extension (MFCE) was proposed by Jouini et al. in 5 as a new cyber security indicator for information systems, and the Cloud Computing environment in particular. The Hybrid Threat Classification model (HTC), which was first proposed in 9, is the model's basis for threat categorization. The HTC is a general threat model that incorporates a number of threat criteria or features, including threat source, threat perpetrators, motivations, purpose, and threat repercussions.

The Mean Failure Cost model (MFC) described in the preceding section's threat vector PT and impact matrix IM estimates are the focus of the MFCE model. Instead of focusing on a single danger, this approach

enables analysis of the effects of a class of threats. Threats do vary over time, and security measures do as well.

Two additional matrices, the impact matrix IMC and the threat classes matrix CM, were created for the impact matrix IM. When a threat class Clr manifests, the ICM matrix shows the likelihood that a component Ck will fail, and when a threat Tq occurs, the CM matrix shows the likelihood of having a threat class Clr.

In order to arrive at appropriate decision-making security solutions for the cloud computing environment, the MFCE model represents a cyber security metric. To better analyse and detect security risks, this quantitative decision-making metric enables choosing countermeasures by danger class rather than a single threat.

e. Multi-dimensional Mean Failure Cost Model (M2 FC), paragraph 4.5

In 2010, Jouini et al. suggested using a multi-dimensional method to evaluate security concerns. In order to more accurately quantify potential risks, they provide a novel model for calculating the cost of an information system security failure that incorporates threat dimensions. The threat environment is separated into numerous danger perspectives, each with a number of orthogonal failure modes, according to the concept known as Multi-dimensional Mean Failure Cost (M2 FC).

dimensions. In actuality, every security issue has a number of viewpoints that raise the amount of risk a system must contend with. This space may be divided up into multiple slices by these views, which we refer to as dimensions.

The model takes into account a leading dimension for decomposition purposes to allow focusing more on one dimension than the other dimensions of the threat world. For instance, we select the components dimension as the leading one to evaluate the mean failure cost per architectural component. In other circumstances, we would want to concentrate on the enterprise's deployment site rather than its components because it will allow us to determine the mean failure cost per location.

The M2 FC model considers how the stakeholders rate the costs associated with their demands in relation to the elements of two dimensions. The model distinguishes between a set of the leading dimension and a set of the other taken into account dimensions (time, system's component...) by taking into account a set H of stakeholders and a set R of their needs.

V. ASSESSMENT STUDY

The study of the four quantitative security risk analysis models for CC systems seeks to highlight each model's merits and disadvantages as well as a more detailed comparison of the three methodologies.

The Securement model is a mathematical method for comparing cloud providers to choose the best one based on the computation of each provider's risk factor, which does not quantify the risks associated with security breaches for the cloud computing environment.

There are various benefits to the Mean Failure Cost model (MFC). In reality, it determines how much each system stakeholder stands to lose as a result of security threats and system vulnerabilities, specifically in terms of how much. The stakes that each stakeholder has in fulfilling each security criterion are indeed different, and our measure reflects that. Unfortunately, it has a number of drawbacks. We identified the following MFC limitations after researching and examining security issues and the MFC metric:

Security risks are evolving, changing, and possessing a variety of traits. In the PT vector, there is no logical or hierarchical structure between the many recorded threats because they are not based on a specific property to categorise them. In reality, the word used to characterise the threat in the threat vector PT might be ambiguous; this can cause overlap between the distinct threats, i.e., one threat may belong to

numerous classes at once and thus it is computed several times, thus we have an underestimating of the mean failure cost.

x Managers are unable to pinpoint the origin of threats or dangers in order to provide effective defences. The MFC is oblivious to the nature and scope of security risks. It believes that every threat-related failure is a failure of the whole specification. Nevertheless, distinct stakes in various security threat dimensions and viewpoints may exist among stakeholders, which the MFC does not take into account.

The MFCext and the MFCint allow managers room to take the necessary steps in response to serious risks. They enhance the system vulnerability analysis. To reduce the average cost of failure, they identify the kind of solution. In fact, by employing the threat categorization source dimension, managers may focus on the incursion space with the highest mean failure costs by determining the source of the threats space (either an internal source or an external source). Unfortunately, it only considers one factor that does not adequately identify a threat (such as the source) and does not account for all threat characteristics; as a result, they are unable to provide reliable estimates of the cost of security failure. Also, while threat sources may fall into one of three subclasses, the considered criteria (source) are based on a binary categorization (internal or external).

The Mean Failure Cost Extension model (MFCE) takes threat classification into account based on a threat classification model and permits providing a threat solution by class; however, this model does not depict the cost based on security threats dimensions or viewpoints. We also emphasised that the model employed for classifying risks is not a full model in terms of size. Also, managers cannot determine them using these models if they wish to know crucial criteria or dimensions that affect the cost values of security failure. In order to manage security policies in enterprises more effectively, we must create a measure that reliably evaluates security breaches and provides crucial dimension.

Thus, the decision-makers cannot determine them using these models if they want to have dimensions or important criteria that affect actions of the cost of failure of security. Lastly, the Mean Failure Cost (MFC)17 has been improved by this M2 FC. This model changes depending on the stakeholder and accounts for the different stakes that each stakeholder has in fulfilling each security criterion, but it excludes threat viewpoints and dimensions. Moreover, it takes into consideration threats from several angles in order to lessen the security risk to each system and it takes into account system modifications such as adjustments to deployment, component placement, and user access regulations into account. This enables for the identification of crucial dimensions that have the highest prices by taking into consideration threats dimensions and views aspect.

VI. CONCLUSION

In paper, risk assessment is a critical aspect of cyber security that helps organizations identify potential vulnerabilities and threats to their systems and data. Through a comprehensive risk assessment process, organizations can determine the likelihood and potential impact of a cyber-attack, and develop appropriate mitigation strategies to minimize the risk of an attack occurring. A key cog in the information security management wheel is risk assessment. Businesses should develop a disciplined, methodical procedure for evaluating the risks of information security to their assets. The primary goal of the study is to examine and compare quantitative security risk models for cloud computing systems, which are a potential solution for businesses looking to save costs and enhance their brands. Decision-makers may choose the best models to evaluate security threats for the CC environment and, in fact, for other information systems, thanks to the comparison that

results. In fact, it aids in determining how well the models fit an organization's needs.

VII. REFERENCES

[1]. Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Cengage Learning.

[2]. Peltier, T. R. (2016). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Elsevier.

[3]. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce.

[4]. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

[5]. Williams, M. (2017). Cybersecurity and risk assessment in the hospitality industry. Journal of Hospitality and Tourism Technology, 8(2), 119-130.

[6]. Siponen, M. T., & Vance, A. (2010). Neutralization: New insights into the problem of employee cyberdeviance. MIS Quarterly, 34(3), 487-502.

[7]. Kumar, S., & Srivastava, S. (2021). A Comprehensive Review of Cybersecurity Threats, Risks and Mitigation Strategies. Journal of Cybersecurity and Privacy, 1(1), 1-16.

[8]. Shin, J., Yoon, J., Lee, J., & Kim, H. (2020). Cybersecurity risk assessment for industrial control systems: A survey. Journal of Network and Computer Applications, 154, 102697.

[9]. Alzahrani, A., Hussain, R., & Hussain, F. K. (2019). A novel approach for cyber security risk assessment using attack trees and fuzzy logic. IEEE Access, 7, 12031-12042.

[10]. Bhattacharya, S., & Paul, A. (2019). Cybersecurity risk assessment using analytic hierarchy process-based approach. Journal of Cybersecurity and Mobility, 7(4), 19-41.

[11]. Khan, I. A., Imran, M., & Ahmad, J. (2018). A comprehensive review of cybersecurity risk assessment tools for industrial control systems. Journal of Network and Computer Applications, 108, 58-81.

[12]. Al-Shehri, S. A. (2018). Cyber security risk assessment in cloud computing using Bayesian networks. Journal of Information Security and Applications, 40, 28-41.

[13]. Alharbi, F. (2017). Cyber security risk assessment for small and medium-sized enterprises: A systematic review of recent empirical studies. International Journal of Information Management, 37(5), 618-634.

[14]. Rana, M., Misra, S., & Ong, K. L. (2017). An overview of cyber security risk assessment frameworks for SCADA systems. Journal of Network and Computer Applications, 84, 23-34.

[15]. Chen, Y. H., Chen, H. Y., Chen, Y. L., & Tsai, C. F. (2017). A cybersecurity risk assessment model for enterprises. Journal of Internet Technology, 18(5), 1095-1102.

[16]. Shen, W., Hu, X., Xu, J., & Chen, Y. (2017). An intelligent risk assessment method for network security based on improved Bayesian network. Journal of Network and Computer Applications, 85, 155-165.

[17]. Abugabah, A., Mohamed, N., & Elleithy, K. (2017). A multi-criteria decision making approach for cyber security risk assessment of information systems. Journal of Ambient Intelligence and Humanized Computing, 8(6), 831-846.

[18]. Kahani, M., & Ghorbani, A. A. (2017). Cyber security risk assessment of enterprise networks using Bayesian networks. Journal of Information Security and Applications, 34, 102-111.

[19]. Cherdantseva, Y., Hilton, J., & Burnap, P. (2018). Risk management and cybersecurity: A review. Journal of Risk Research, 21(3), 300-314. doi: 10.1080/13669877.2017.1316181

[20]. Kim, J. T., & Kim, D. H. (2021). Risk assessment of cyber-attacks using a deep learning approach. IEEE Access, 9, 118138-118152. doi: 10.1109/ACCESS.2021.3118289

[21]. Li, C., Li, J., Guan, Q., Li, X., & Li, X. (2020). Cybersecurity risk assessment and management for power systems. Energies, 13(19), 5005. doi: 10.3390/en13195005

[22]. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. Retrieved from https://www.nist.gov/cyberframework

[23]. Solms, R. V., & Solms, R. (2016). Information security risk management: An overview. Computers & Security, 60, 212-217. doi: 10.1016/j.cose.2015.09.005

Cite this article as :

Anirudh Kumar Paswan, Prof. Vinod Mahor, "A Review : Cyber Security and Risk Assessment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.324-331, March-April-2023.