Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
December 2022 10(12), 55–68

IT PROJECT RISK MANAGEMENT FOR CLOUD ENVIRONMENT LEVERAGING ARTIFICIAL INTELLIGENCE

Remya Nair [1], Dr. J. Meenakumari [2]

[1] Research Scholar, Registered with University of Mysore, International School of Management Excellence (ISME), Bangalore, India
[2] Research Supervisor, International School of Management Excellence (ISME), Bangalore, India

Received 12 November 2022
Accepted 14 December 2022
Published 31 December 2022

Corresponding Author

Remya Nair,
remya.sanju.nair@gmail.com

DOI 10.29121/granthaalayah.v10.i12.2022.4940

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Cloud security contributes to multiple risk parameters like multitenancy, Insecure interfaces/APIs, Malicious Insiders, Malware injections, the lack of information on location of storage of data, the unavailability of details on type of data saved in the same server, hacking. AI or Artificial Intelligence works on pre-collected data and scenarios fed into the computers thereby predicting in advance the possibilities of risk, warning if there is any unusual occurrence in the cloud and proposing the Risk Mitigation plans based on various scenarios. Proactive risk prediction will have a huge impact on risk mitigation, cost saving as well as customer satisfaction. A pilot study has been conducted to ascertain the impact of various risk factors identified by circulating the questionnaire among practitioners from the relevant domains. The questionnaire is circulated among the current industry practitioners and experts in this area and facilitates to conduct the pilot survey on the significance of various risk parameter. The impact of each risk factor is identified and is subjected to analysis. With the help of prediction algorithms, the possibility of occurrence of risk, the impact, and consequences of that particular event, as well as the mitigation strategies could be foretold. This objective of this paper is to propose management perspective of a framework of AI, that can contribute to proactive risk management in cloud. This paper deals only with the management overview of implementation of AI in risk mitigation strategies and not the technical aspects of AI. The futuristic scope of this paper would be a management overview on automation of risk mitigation strategies in cloud platform using AI.

Keywords: Artificial Intelligence, Cloud Security, Risk Management, Risk Mitigation Strategies, Proactive Risk Prediction

1. INTRODUCTION

Cloud Computing consist of a large integrated array of components provided by a cloud service provide which includes tools and applications, primarily all the resources that deals with networking, software, data storage, databases, and servers. Cloud is of 4 main types of namely private cloud, public cloud, hybrid cloud and multi clouds. The three main types of cloud computing services are Iaas: Infrastructure as a Service, Paas: Platform as a service and Saas: Software as a Service. The major advantages of cloud are increased productivity, cost savings speed, performance, security, and efficiency.

2. ADVANTAGES OF CLOUD COMPUTING

Cost Savings: Cost saving Chandra and Borah (2012) is one of the major benefits of Cloud Computing. Application of Cloud Computing overburdens the handling of complex IT Infrastructure management and maintenance activities. However, this also results in considerable cost savings. The service provider efficiently performs the purchase and maintenance of hardware equipment.

Strategic edge: A competitive edge is offered over the competitors by the application of cloud computing Weinman (2017) In terms of underlying economic and financial implications Internet of Things is very relevant to a variety of companies as an evolving technology. It also acts as an enabler of strategic business in terms of its fundamental economics and financial repercussions.

High Speed: In cloud computing the demand is highly fluctuating resulting in periods of underutilization or overloading. InfiniBand, is in a high performance cloud computing environment. Cost savings and flexibility is promised by a cloud-based Infrastructure-as-a- Service (IaaS) approach for high performance computing applications Mauch et al. (2013).

Restoration of data & Data backup: The recovery and backup of the data stored in cloud platform is easier Compared to the on premise data recovery. Mao et al. (2012) Eventhough the drastic growth of digital content causes massive strains on the storage systems in the cloud environment, the data replication technology has been established to be effective in reducing the backup window, thereby minimizing the network bandwidth and storage space in cloud servers

Automatic Software Integration: Automatic software integration is one of the specific features of the cloud computing. No additional effort is required to customize and integrate applications to the cloud platform. This integrated feature of the cloud platform helps in saving a lot of time and money.

Reliability: One of the primary advantages of cloud computing is reliability. The cloud computing network is always reliable as the performance can be very consistent and accurate

Mobility: The primary advantage of cloud computing is the mobility aspect of it where the network could be access from anywhere irrespective of the location. The cloud computing us totally location independent and the primary requirement to access a cloud data is just an Internet connectivity. The location independence feature of cloud makes it more suitable for digital transformation in the modern era.

Unlimited storage capacity: One of the primary advantages of cloud computing Is that there is no constraint for the storage limits. Based on the requirement of the storage capacity, the storage limit in the cloud could be either added on or decreased with very less financial implications.

Collaboration: The cloud computing platform ensures collaboration of multi geography and location independent employees in an extremely efficient, convenient, and secured manner.

Quick Deployment: Quick deployment is one of the major advantages of cloud computing. Rapid deployment is possible in cloud computing and the entire system can be functional in a short span of time. the rapid deployment is directly proportional to the kind of technologies that are utilised or implemented in the particular business as well as the complexity of the system.

Other Important Benefits of Cloud Computing: Other relevant and significant Cloud Computing advantages are: Demand based Self-service, Multi-

tenancy, Resilient Computing, Faster and effective virtualization, Low-cost software, Advanced online security, Location and Device Independence, availability, and scales automatically to adapt to the surge in demand, pay-per-use , Web-based control & interfaces, API Access .

3. MAJOR DISADVANTAGES OF CLOUD COMPUTING

The following are the disadvantages of the cloud computing. The various factors that could be accounted as the disadvantages also contribute to the risk factor of cloud. A detailed analysis of the disadvantages of cloud computing are listed below.

Inconsistent Performance: When multiple applications share the same server and run simultaneously any DDOS, or malicious intrusion might result in inconsistent performance of the shared resource. Since the location of data storage of the data is not known a security attack on any of the one client data might affect the whole system security.

Technical Issues: Despite maintaining a high security and maintenance standard, cloud technology is always prone to technical issues and outages. Even the most reliable and efficient cloud security provide a may face this issue despite using the most innovative expensive and latest technologies.

Security Threat in the Cloud: Security risk is one of the major drawback that we have to deal with while working on a cloud computing environment. The sensitive information od the company is shared with a 3rd party cloud computing service provider as a result of which the hackers might have easy access of this information if there are any leakages in the security systems formulated by the cloud service provider.

Downtime: The cloud service provider may face with certain downtime issues such as power failures, Internet connectivity issues, maintenance contact issues of the service etc. One of the primary disadvantages that should be considered while working with a cloud computing environment is the downtime issue.

Internet Connectivity: One of the primary requirements for a stable cloud network is the uninterrupted Internet connectivity. The Internet connection should be stable uninterrupted as well as intrusion free from malicious hackers. In short, a secured and uninterrupted Internet connectivity is the basic requirement for a good cloud platform.

Lower Bandwidth: The cloud service provider has many mechanisms implemented to limit the bandwidth usage of the respective users. If the agreed upon allowances are surpassed by the organization then the additional charges could be significantly higher.

Lacks of Support: The technical knowledge shared by the cloud computing companies so as to provide online support to the customer is very minimal. As a result of which a non technical person might find the troubleshooting of issues related to cloud a very tedious and hectic process.

4. ARTIFICIAL INTELLIGENCE

AI or Artificial Intelligence is one among the recent and innovative technology that has transformed numerous realms. Artificial Intelligence (AI) can be described as the development of computer systems that can perform assignments that require human intelligence Russell (2016). The major areas that utilize AI are empirical searches, character detection, the concept of mobile robotics, sophisticated systems for facial recognition and the natural language processing. During early 1980s,

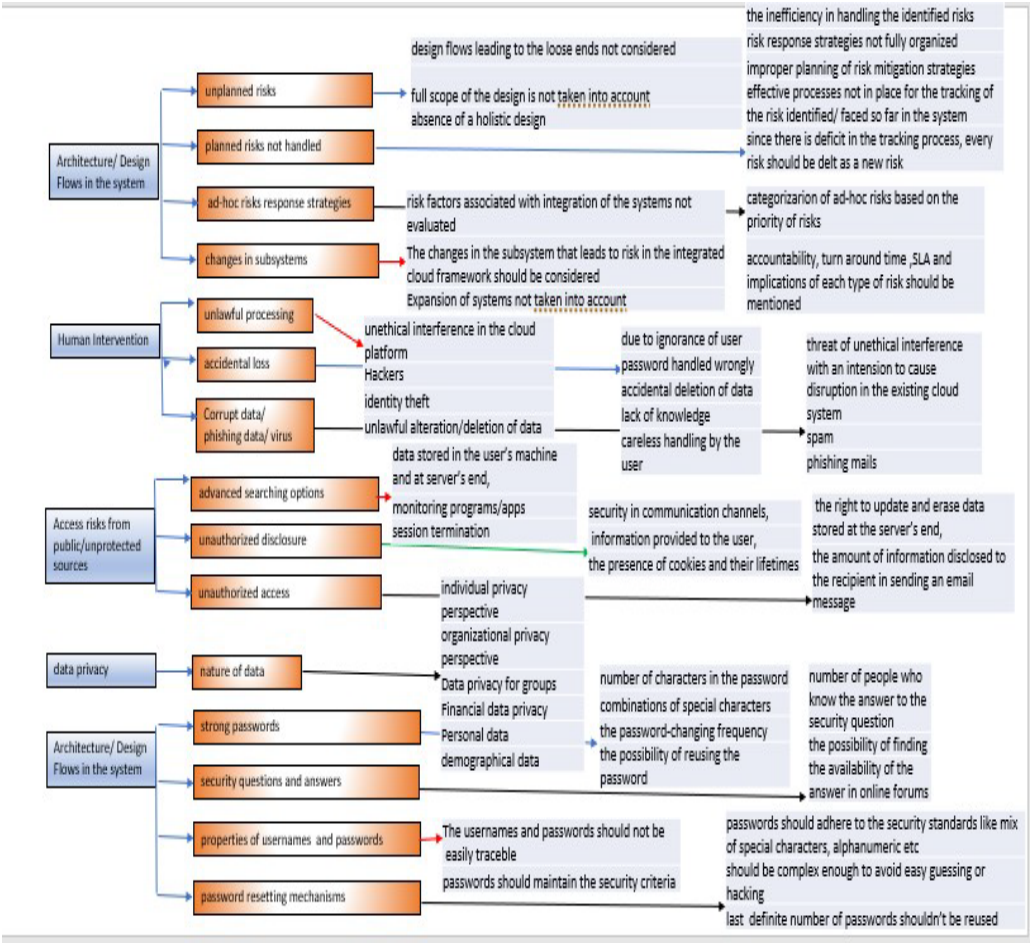
significant conceptual progress was made in the technology-driven field, and there was a significant increase in its application Issa et al. (2016). By the beginning of 1990s, Artificial Intelligence attained significant growth because this advanced and innovative of technologies permitted engineers to utilize large volumes of data, design robots in an effective manner, and work with advanced computing powers. AI concepts have progressed and altered the realm of technology.

By the 21st century, Artificial Intelligence is at its prime, and has a deep influence on individuals and organizations to a considerable extent. Artificial Intelligence technology is applied in digital transformation in various industries and not only the IT and ITES Sector Nagaraj (2019), (2020). AI applications include autonomous vehicles, navigation systems, advanced chatbots, robotic nurses, games etc Russell (2016). The start-ups that use Artificial Intelligence for businesses across multiple industries, can generate a revenue of almost $1.2 trillion in a single year compared to their less-informed competitors by 2020 McCormick et al. (2016).

The major industries where Artificial Intelligence can be implemented are the healthcare and life sciences, banking, energy, manufacturing industry, automotive industry, media, entertainment insurance, telecommunications, financial services, travel tourism and hospitality. AI's trajectory is growing in a rapid pace in large number of businesses across the world. The relevance, acceptance and application of AI technology are expanding in the industrial setting as it enhances the level of innovation and minimizes the manual intervention. AI is incorporated in various organizations such as marketing, sales, finance, customer service, etc in various industries.

5. RISK MANAGEMENT

The Risk Management Process has many critical steps. Out of that the six major steps include1.Assess the Risk -The risk parameters are identified and the impact of each of these risks is assessed. 2.Prioritize the risk-The identified risk parameters have to be prioritized based on the impact and significance of each of the risk parameters.3. Create the Risk Profile-The risk profile for each risk type of risk is formulated. A risk register has to be maintained which contains all the risk profiles defined.4.Choose the risk strategies The strategies to be followed in each of the risk scenarios have to be drafted.5Execute Risk Strategies-Risk strategies that are identified should have a proper execution plan and should be executed properly.6.Measure Residual Risk-After the risks are identified, rectified and managed, the next important step is to measure the residual risk associated with each process. The risk parameters with three level of subconstructs are identified in the paper Nair and Meenakumari (2021)



6. LITERATURE REVIEW

Although Turing (1950) claim that machines—especially digital computers—can "think". The following are the labels suggested by Turing to the objections that he considers: Theological, "Heads in the Sand", Mathematical, Lady Lovelace's Objection as well as the arguments from Consciousness, Various Disabilities, Continuity of the Nervous System, Informality of Behaviour, Extra-Sensory Perception

In 1961, the evolved idea of AI was explained based on heuristic programming problems of making computers solve difficult problems. The five areas identified were Search, Pattern- Recognition, Learning, Planning, and Induction. A computer can only perform what it is told to do. The efficiency could be improved by utilizing pattern-Recognition techniques thereby restricting the application of the machine's methods to apt problems. Pattern-Recognition along with adequate Learning, can be used to reduce search by exploiting generalizations based on accumulated experience. To handle extensive problem management, machines are required to construct models of their environments, applying some specific scheme for Induction. Minsky (1961)

In the wake of liberalization and globalization, women entrepreneurship ventures are gaining significance. Women entrepreneurship is the route to women empowerment. Mishra and Kiran (2014) The women entrepreneurship is a topic of wide interest Grisna Anggadwita (2021). The role of women's financial

independence and the subsequent social and economic development of the society is studied in detail. Wojcieszak (2019). The prototypical homemaker with her innate managerial skill, knowledge and adaptability in the difficult social background made them eager to take up business ventures and often have transformed them into success stories. Arvind (2011)

In Cloud Platform the exact location of the data or the other sources of the data stored along with specific data will not be revealed to the user. The cloud data ranges from least security public source to extremely sensitive private data Kaufman (2009) Cloud Computing trends like Grid Computing, Utility Computing, Distributed Computing are rapidly advancing. The leading and dominant cloud service providers aid in developing applications in cloud environment and help users to access them from anywhere. A remote server stores the data in Cloud data, accessed with the help of services provided by cloud service providers. The data security is the major challenge as the confidentiality of the data transmitted to the remote server over internet has to be maintained. The priority is to address the security challenges before implementing Cloud Computing in an organization Rao, and Selvamani (2015), Choudhary et al. (2011). While considering the data security risks, multi tenancy is one of the major factors that should be taken into account. Aljahdali et al. (2014), Gheyas and Abdallah (2016).

Kaufman (2009)- identifies the fact that the vulnerability of a cloud service provider makes the particular cloud setup a highly visible target to the malicious intruders.

Aljahdali et al. (2014) this paper covers the Multi-tenancy in Cloud Computing due to carious cases like internet attacks, Attacks within cloud provider as well as multi-tenancy attacks. The scope of this paper includes the advantages of multi-tenancy as well as risks and partial attack model.

Rao and Selvamani (2015) in the paper "Data Security Challenges and Its Solutions in Cloud Computing "implies that in the Cloud environment data is stored and accessed from a remote server provided by cloud service providers.

Subashini and Kavitha (2011). "A survey on security issues in service delivery models of cloud computing explains all the risk factors Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication, and authorization, that are considered for Iaas, Paas and Saas.

Zissis and Lekkas (2012) and Dimitrios Lekkas, explain that Cloud environment is scrutinised in application level, virtual level, physical level. The first level of security threats in each of these identified requirements is explained.

In this paper by Chonka et al. (2011) Cloud Protector, a neural network is developed that was trained to detect and filter X-DoS attack in this paper in order to detect and filter X-DoS attack, a neural network, Cloud Protector, is developed.

In the paper by Jansen (2011) primary level risk factors are considered. However, what is not taken into account is the extensive risk analysis and weightage of each of these risks.

In the paper POWER, M. (2004), the detail study of the financial implications of the risk management is provided. Aven, Terje. (2015) the basics of risk management is analysed and explained. Realisation of unintented, negative consequences of an event is defined as risk. Risk management is the mitigation of negative consequences of an activity and associated uncertainties.

Three main goals of the paper Md. Tanzim Khorshed (2012) is to detect an attack when it happens, to inform relevant stake holders about the attack type and

take combating action, as well as to create information on the attack type by analysing the frequency and pattern of the attack.

7. RESEARCH GAP ANALYSIS – RELEVANCE OF THIS PAPER

There are many studies connecting AI, Risk management and Cloud. However, an in-depth study to leverage artificial intelligence to effectively formulate the risk management strategies in cloud is not extensively covered in any of the papers. There were papers which covered the use of risk management in cloud as well as AI in cloud. There were extensive papers in each of these three separate topics such as AI risk management and cloud. During the literature survey one extensive paper which analysis the leveraging of artificial intelligence for risk management in cloud platforms with the identified risk impact parameters was not available. The risk impact parameters in cloud data security are identified even to the level of sub factors. This paper tries to cover based on the impact parameters of each of the risk factors how AI could be leveraged to manage those risks.

8. METHODOLOGY

This research paper is based on quantitative analysis of primary data collected by means of a pilot study. The questionnaire containing the identified impact parameters was circulated among the practitioners in IT sector. The impact parameters are rated on a Likert scale of 1 to 5 ranging from high impact to significantly low impact. Various statistical tests are performed on these gathered data points. The tests conducted includes tee test chi square test and descriptive statistical analysis. Best on the status tickle analysis of all these values and taking the test as a reference the impact of all the identified risk parameters is investigated.

9. DETAILS OF PILOT STUDY

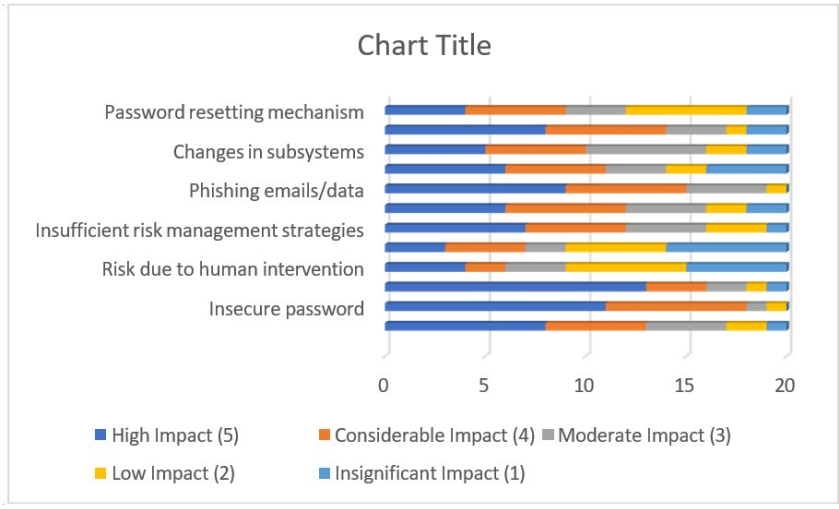
Questionnaire

On a scale of 1-5 how much would you rate impact of the following risk parameters

S. No.	Question	High Impact (5)	Considerable Impact (4)	Moderate Impact (3)	Low Impact (2)	Insignificant Impact (1)
1	Hackers/Identity theft	8	5	4	2	1
2	Insecure password	11	7	1	1	
3	Access the data from a public/unsafe network	13	3	2	1	1
4	Risk due to human intervention	4	2	3	6	5
5	Accidental loss	3	4	2	5	6
6	Insufficient risk management strategies	7	5	4	3	1
7	Lack of risk response plans for identified and known risks	6	6	4	2	2
8	Phishing emails/data	9	6	4	1	

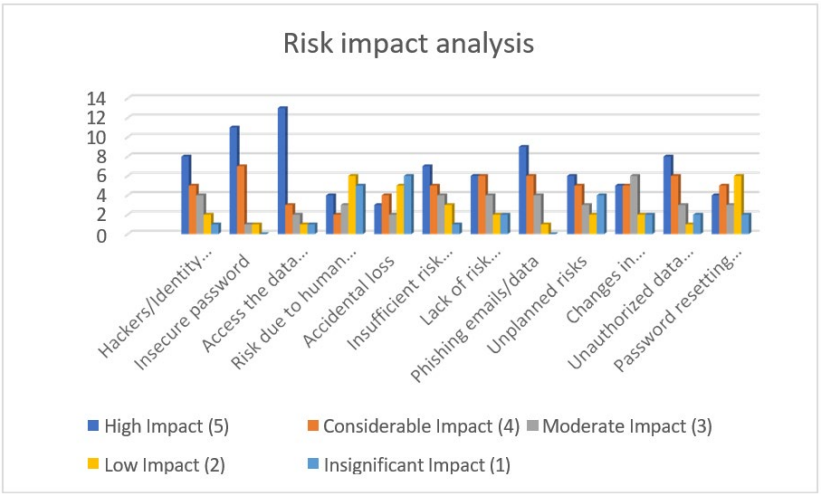
9	Unplanned risks	6	5	3	2	4
10	Changes in subsystems	5	5	6	2	2
11	Unauthorized data access	8	6	3	1	2
12	Password resetting mechanism	4	5	3	6	2

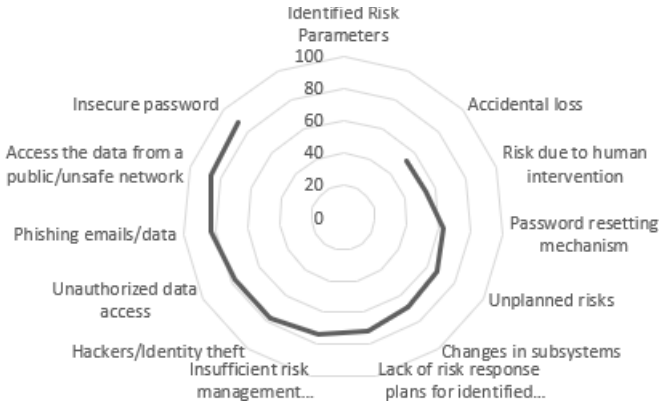
10. GRAPHICAL INTERPRETATIONS OF THE PILOT STUDY



11. INFERENCES FROM THE PILOT SURVEY

A questionnaire with the identified risk parameters is circulated among the various industry practitioners. Likert scale values of high impact to insignificant impact is chosen for each of the risk parameters by all the practitioners. Based on the Likert scale options a value of five to one is assigned to each of these options chosen. The values are then calculated with the weighted average method and the final values are interpreted in a graphical form. From the Likert scale values obtained the top 3 parameters that have high impact on the cloud platforms are insecure passwords, accessing the data from public unsecured network and the phishing emails and data theft.





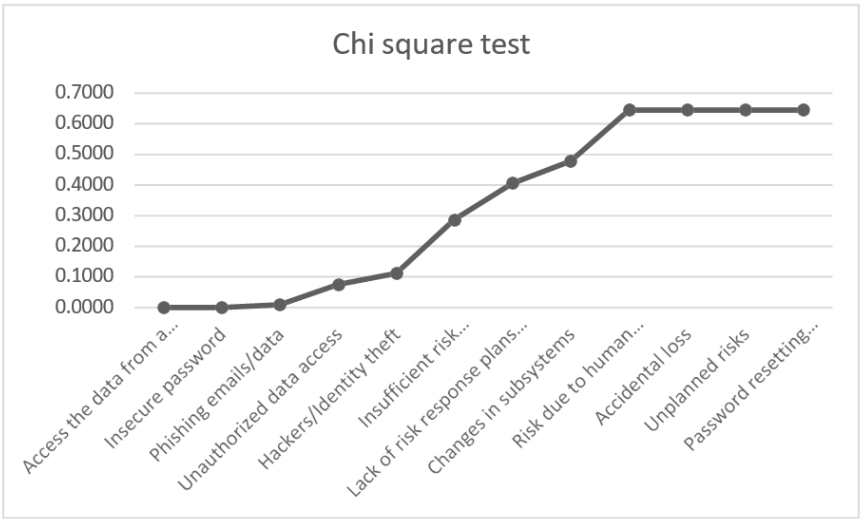
t-Test

t-Test: Two-Sample		
	Equal impact for all parameters	**impact analysis from pilot study**
Mean	60	71.9167
Variance	0	129.7197
Observations	12	12
df	11	
t Stat	-3.6245	
P(T<=t) one-tail	0.0020	
t Critical one-tail	1.7959	

Inference from the t-Test: A t-test is performed considering there is equal impact of all the risk parameters and the impact analysis from the pilot study. A p-value less than 0.05 is considered to be acceptable score to indicate the validity of the test. However as per this experiment the p- value for one tail test is 0.002 and the P value for two tailed test is 0.004 which indicates that these two tests are off very significant validity.

12. CHI SQUARE TEST ANALYSIS

Chi Square Test	
Identified Risk Parameters	**chi square test values**
Access the data from a public/unsafe network	0.0000
Insecure password	0.0001
Phishing emails/data	0.0091
Unauthorized data access	0.0749
Hackers/Identity theft	0.1117
Insufficient risk management strategies	0.2873
Lack of risk response plans for identified and known risks	0.406
Changes in subsystems	0.4779
Risk due to human intervention	0.6446
Accidental loss	0.6446
Unplanned risks	0.6446
Password resetting mechanism	0.6446



13. INFERENCE FROM THE CHI SQUARED TEST ANALYSIS

If chi-square calculated value is greater than the chi-square critical value, then null hypothesis is rejected. If the calculated chi-square value is less than the chi-square critical value, then the null hypothesis is "fail to reject". Si since the chi square value of the identified risk factors are critically low, the null hypothesis is failed to reject for those risk factors

14. DESCRIPTIVE STATISTICAL ANALYSIS OF THE DATA

Risk Parameters - Identified	Mean	Standard Error	Median	Standard Deviation	Sample Variance	Kurtosis	Skewness	Range	Confidence Level (95.0%)
Hackers/Identity theft	4	1.2247	4	2.7386	7.5	- 0.1333	0.6086	7	3.4004
Insecure password	4	2.1448	1	4.7958	23	- 1.1474	0.9519	11	5.9548
Access the data from a public/unsafe network	4	2.2804	2	5.0990	26	4.4630	2.0932	12	6.3313
Risk due to human intervention	4	0.7071	4	1.5811	2.5	- 1.2000	0.0000	4	1.9632
Accidental loss	4	0.7071	4	1.5811	2.5	1.2000	0.0000	4	1.9632
Insufficient risk management strategies	4	1.0000	4	2.2361	5	0.2000	0.0000	6	2.7764
Lack of risk response plans for identified and known risks	4	0.8944	4	2.0000	4	-3.0000	0.0000	4	2.4833

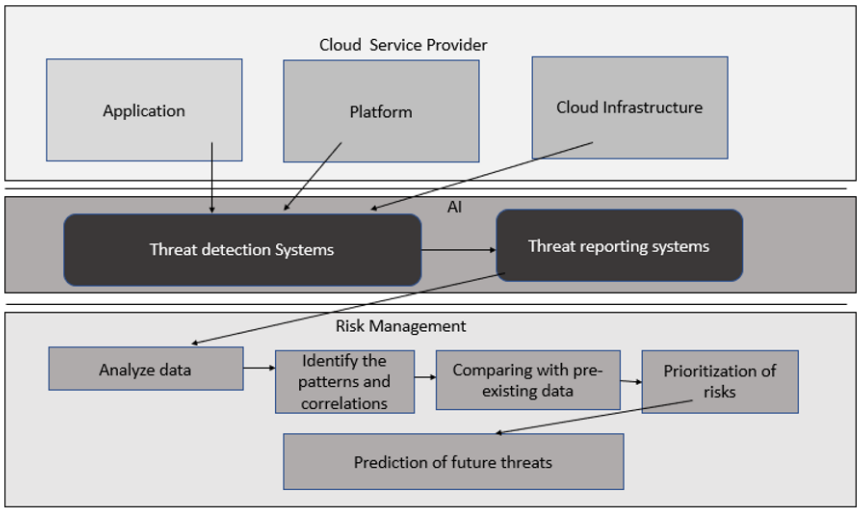
Phishing emails/data	4	1.6432	4	3.6742	13.5	-1.2922	0.3528	9	4.5622
Unplanned risks	4	0.7071	4	1.5811	2.5	-1.2000	0.0000	4	1.9632
Changes in subsystems	4	0.8367	5	1.8708	3.5	-2.8980	-0.3818	4	2.3229
Unauthorize d data access	4	1.3038	3	2.9155	8.5	-1.5986	0.6053	7	3.6200
Password resetting mechanism	4	0.7071	4	1.5811	2.5	-1.2000	0.0000	4	1.9632

15. INFERENCE FROM THE DESCRIPTIVE STATISTICS

Kurtosis- The three types of curves in kurtosis are mesokurtic, leptokurtic and platykurtic. Kurtosis values which are negative indicates a platykurtic distributive which reveals a flat and thin tail. Kurtosis values which are positive indicate leptokurtic distribution which has a higher peak and thick tails. As per the skewness analysis, although many values indicate that the distribution of largely symmetrical, there are values that indicate a few parameters are outside the allowable limit as well. The p-value of the confidence interval is also calculated. From the above descriptive analysis, the next action item is to perform the study with a large sample size for more accurate results.

16. RECOMMENDED MANAGEMENT MODEL FOR RISK MANAGEMENT IN CLOUD USING AI

Based on the three models of cloud application platform and infra structure an efficient threat detection system can be formulated. The identified risk parameters have been plotted into threat detection system and the impact of each of the risk identified has to be mapped in the system. With the help of the prediction algorithms the possibility of the risk could be foretold. The impact of these risks and their subsequent consequence should be identified prior and has to be fed into system. They identified mitigation strategies have to be verified against each of these risk parameters and the effectiveness of those should be validated. An effective threat reporting system has to be formulated.



The risk management strategies include the analysis of the data, the identification of the patterns and the correlations, comparing with the pre-existing data and prioritising the risk. The final step in the risk mitigation strategy is to predict the future risk as well as pre plan for the future impacts of the risks and identifying the critical risk that could unfold in the future.

17. CONCLUSION

As per the pilot study the major risk factors that have a very significant impact are access the data from a public/unsafe network, insecure passwords, phishing emails/data, unauthorized data access, hackers/Identity theft etc. Due to the sudden onset of the pandemic, digital transformation has gained a huge momentum. This specific paper is an attempt to integrate the AI, Risk management and cloud for an efficient risk mitigation. The futuristic scope of this paper is automation of the risk mitigation using AI with the implementation of advanced digital management technologies. Risk management strategies should be formulated in such a way for that the identified risk parameters can devised based on the impact factors. Risk management strategies should be predetermined for all the identified risk parameters. The RACI matrix should be prepared for all the risk management parameters so that the timely information and escalation of these parameters could be implemented.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Akinrolabu, O., Nurse, J. R. C., Martin, A., and New, S. (2019). Cyber Risk Assessment In Cloud Provider Environments: Current Models And Future Needs, Computers And Security, 87, 101600. https://doi.org/10.1016/j.cose.2019.101600.

Aljahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., and Xu, J. (2014). Multi-Tenancy in Cloud Computing 8th International Symposium on Service Oriented System Engineering, 2014. IEEE Publications. https://doi.org/10.1109/SOSE.2014.50.

Chandra, D. G., and Borah, M. D. (2012). Cost Benefit Analysis of Cloud Computing in Education International Conference on Computing, Communication and Applications, 2012, 1-6. https://doi.org/10.1109/ICCCA.2012.6179142.

Chonka, A., Xiang, Y., Zhou, W., and Bonti, A. (2011). Cloud Security Defence To Protect Cloud Computing Against HTTP-Dos and XML-Dos Attacks. Journal of Network and Computer Applications, 34(4), 1097-1107. https://doi.org/10.1016/j.jnca.2010.06.004.

Choudhary Kishor, N., and Rayalwar Arvind, P. (2011). Opportunities and Challenges for Rural Women Entrepreneurship in India. Variorum Multi-Disciplinary E-Research Journal, 01(III, February).

Gheyas, I. A., and Abdallah, A. E. (2016). Detection and Prediction of Insider Threats to Cyber Security : A Systematic Literature Review and Meta-Analysis. Big Data Analytics, 1(1), 6. https://doi.org/10.1186/s41044-016-0006-0.

Hoyle, R. H. (Ed.). (1995). Structural Equation Modeling : Concepts, Issues, and Applications. Sage Publications, Inc.

Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing 44th Hawaii International Conference on System Sciences, 2011. https://doi.org/10.1109/HICSS.2011.103.

Kaufman, L. M. (2009). Data Security In the World of Cloud Computing. IEEE Security and Privacy Magazine, 7(4), 61-64. https://doi.org/10.1109/MSP.2009.87.

Khorshed, M. T., Ali, A. B. M. S., And Wasimi, S. A. (2012). A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing. Future Generation Computer Systems, 28(6), 833-851. https://doi.org/10.1016/j.future.2012.01.006.

Maccallum, R. C., and Austin, J. T. (2000). Applications of Structural Equation Modeling In Psychological Research. Annual Review of Psychology, 51, 201-226. https://doi.org/10.1146/annurev.psych.51.1.201.

Mao, B., Jiang, H., Wu, S., Fu, Y., and Tian, L. (2012). SAR : SSD Assisted Restore Optimization for Deduplication- Based Storage Systems in the Cloud IEEE Seventh International Conference on Networking, Architecture, and Storage, 2012, 328-337. https://doi.org/10.1109/NAS.2012.48.

Mauch, V., Kunze, M., and Hillenbrand, M. (2013). High Performance Cloud Computing. Future Generation Computer Systems, 29(6), 1408-1416, ISSN 0167-739X. https://doi.org/10.1016/j.future.2012.03.011.

Minsky, M. (1961). Steps Toward Artificial Intelligence. In Proceedings of The IRE, 49(1), 8-30. https://doi.org/10.1109/JRPROC.1961.287775.

Mishra, G., and Kiran, U. V. (2014). Rural Women Entrepreneurs : Concerns and Importance. International Journal of Science and Research (IJSR), 3, 93-98.

Mollah, M. B., Islam, K. R., and Islam, S. S. (2012). Next Generation of Computing Through Cloud Computing Technology. In 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), 1-6. https://doi.org/10.1109/CCECE.2012.6334973.

Nair, R., and Dr Meenakumari, J. (2021). Conceptual Model Depicting Risk Factors Influenzing Cloud Data Security. International Journal of Research - Granthaalayah, 9(8), 100-108. https://doi.org/10.29121/granthaalayah.v9.i8.2021.4160.

Priyadarshinee, P., Raut, R. D., Jha, M. K., and Gardas, B. B. (2017). Understanding and Predicting the Determinants of Cloud Computing Adoption : A Two Staged Hybrid SEM - Neural Networks Approach. Computers in Human Behavior, 76, 341-362. https://doi.org/10.1016/j.chb.2017.07.027.

Rao, R. V., and Selvamani, K. (2015). Data Security Challenges and its Solutions In Cloud Computing. Procedia Computer Science, 48, 204-209. https://doi.org/10.1016/j.procs.2015.04.171.

Rigdon, E. E. (1998). Structural Equation Modeling. In G. A. Marcoulides (Ed.), Modern Methods for Business Research, 251-294. Lawrence Erlbaum Associates Publishers.

Shucheng, Y., Wang, C., Ren, K., and Lou, W. (2010). Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing. In IN-FOCOM, 2010. Proceedings of The IEEE, 1-9. https://doi.org/10.1109/INFCOM.2010.5462174.

Subashini, S., and Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications, 34(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006.

Turing, A. M. (1950). I- Computing Machinery and Intelligence. Mind, LIX(236, October), 433-460. https://doi.org/10.1093/mind/LIX.236.433.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. (2008). A Break in the Clouds: Towards A Cloud Definition. In ACM Sigcomm Computer Communication Review, 39(1), 50-55. https://doi.org/10.1145/1496091.1496100.

Weinman, J. (2017). Fogonomics-The Strategic, Ecsonomic, and Financial Aspects of the Cloud 41st Annual Computer Software and Applications Conference (COMPSAC), 2017, 705-705. IEEE Publications. https://doi.org/10.1109/COMPSAC.2017.283.

Xu, G., Li, H., Ren, H., Yang, K., and Deng, R. H. (2019). Data Security Issues in Deep Learning : Attacks, Countermeasures, and Opportunities. In IEEE Communications Magazine, 57(11), 116-122. https://doi.org/10.1109/MCOM.001.1900091.

Zhang, X., Wuwong, N., Li, H., and Zhang, X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments 10th IEEE International Conference on Computer and Information Technology, 2010, 1328-1334. https://doi.org/10.1109/CIT.2010.501.

Zissis, D., and Lekkas, D. (2012). Addressing Cloud Computing Security Issues. Future Generation Computer Systems, 28(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006.