IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 9, September 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

Cybersecurity Threats and Vulnerabilities in Cloud Computing: A Review

Shivansh Gupta[1]

Student, Delhi Public School, R.K. Puram, New Delhi, India[1]

ABSTRACT: Modern company operations have been revolutionised by the widespread use of cloud computing, which has brought about unmatched efficiency and flexibility. However, this development has also given rise to a complicated web of cybersecurity risks and weaknesses that could jeopardise data security, privacy, and general organisational security. This article carefully examines the panorama of prevalent threats, including data leaks, malware attacks, Denial of Service (DoS) incidents, insider threats, and vulnerabilities in cloud infrastructure. It also explores new issues like supply chain threats, risks associated with artificial intelligence, IoT integration, and the complexity of regulatory compliance. The study highlights the significance of encryption, access control, continuous monitoring, patch management, and employee training as proactive mitigation techniques, drawing on real-world examples and statistical insights. By thoroughly addressing these problems, businesses may successfully navigate the complex cloud security landscape, safeguard their digital assets, and guarantee the integrity and resilience of their operations in the increasingly linked digital world.

KEYWORDS: Cloud computing security, Cybersecurity threats, Cloud infrastructure vulnerabilities.

I. INTRODUCTION

As stated by Ganne (2022), cloud computing has become a cornerstone of contemporary company operations in a time of extraordinary scalability, flexibility, and cost-efficiency. As mentioned by Sokolov et al. (2019), concerns over cybersecurity risks and vulnerabilities have risen to the fore as businesses move more of their crucial data, applications, and services to cloud environments. Not only has the incorporation of cloud technologies revolutionised the business environment, but it has also created a number of security concerns that require close attention. The "2021 Cost of a Data Breach Report" from IBM Security and Ponemon Institute estimates that the average cost of a data breach has risen to an astounding $4.24 million per occurrence, with cloud-based attacks being among the most expensive (IBM, 2022).

Figure: Average cost of a data breach four segment in 2022
Source: (IBM, 2022)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

This emphasises the urgent requirement for a thorough grasp of the intricate security landscape around cloud computing. As a result of the shared nature of cloud infrastructures, the inescapable reliance on third-party service providers, and the dynamic interaction between organisations and Cloud Service Providers (CSPs), new attack vectors have been established. Aljumah & Ahanger (2020) mentioned that even though cloud technology has many advantages, it has also created a number of security flaws, including unreliable application programming interfaces (APIs), poor identity and access management, and the potential for supply chain intrusions. Nafea & Almaiah (2021) stated that understanding the dangers and best practises for protecting cloud environments is not only a choice; it is a strategic need in a digital ecosystem where data breaches are becoming more expensive.

II. RATIONALE AND OBJECTIVE

Even with the rapid growth of cloud computing, there is still a substantial knowledge gap about the complex environment of "Cybersecurity Threats and Vulnerabilities in Cloud Computing." Although the existing literature recognises the significance of cloud security, thorough assessments covering the wide range of threats, vulnerabilities, and emerging difficulties are very rare (Vinoth et al., 2022).

This research paper was motivated by the need to quickly close this gap by providing a comprehensive analysis of the many different cybersecurity issues that exist in cloud systems (Mughal, 2021). The potential consequences of security breaches cannot be understated as businesses depend more and more on cloud infrastructure. In order to improve risk management procedures, protect sensitive data, and guarantee smooth business operations, it is imperative to have a complete grasp of the most common threats and vulnerabilities (Alexei & Alexei, 2021).

The primary objective of this research paper is

1. To conduct a comprehensive analysis of cybersecurity threats and vulnerabilities in cloud computing environments.
2. To identify and categorize common attack vectors and weaknesses in cloud infrastructure through literature review and case study analysis.
3. To propose practical mitigation strategies and best practices to enhance cloud security for informed decision-making and risk management.

III.METHODOLOGY

The present investigation utilises a secondary research methodology to thoroughly investigate the topic of "Cybersecurity Threats and Vulnerabilities in Cloud Computing." In secondary research, facts and insights are gathered by methodically analysing previously published books, reports, case studies, and reliable web sources (Ruggiano & Perry, 2019).

Identification, selection, and analysis are the three steps that make up the approach. Selecting reliable sources, such as academic journals, industry reports, and the publications of reputable organisations, is necessary for the first identification process (Sileyew, 2019). These resources offer an excellent basis for comprehending different facets of cloud security risks and vulnerabilities. Sources are then narrowed down through a careful selection process based on their applicability, reliability, and recentness.

During the analysis phase, the information that has been acquired is synthesised and organised into thematic categories, allowing for the detection of common risks new difficulties, and mitigation tactics (Sileyew, 2019). The paper's depth and practical application are further enhanced by a comparative study of real-world case studies.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

IV. LITERATURE REVIEW

Introduction to Cloud Computing and Its Importance in Modern Business

As stated by Kamal et al. (2020), modern company landscapes are being reshaped by the revolutionary power of cloud computing. Businesses are increasingly implementing cloud solutions due to the rapid expansion of digital data and the requirement for dynamic scalability. The fact that 92% of businesses have a multi-cloud strategy shows how widely this technology has been accepted, according to the Flexera 2021 State of the Cloud Report (Flexera, 2021). As mentioned by Mukherjee (2019), cloud computing has never-before-seen benefits. For illustration, the seamless access to data is demonstrated by Dropbox, a cloud-based file-sharing service. Without regard to their physical locations, users can easily collaborate on documents in real-time. The scalability of the cloud is further demonstrated by Netflix's reliance on Amazon Web Services (AWS). In order to handle higher demand during peak hours, AWS automatically scales capacity, guaranteeing a flawless streaming experience (AWS, 2022). As commented by Podeschi & DeBo (2022), along with increasing productivity, cloud computing gives companies the ability to spend less on capital equipment. In order to save $15 million over the course of a year, Airbnb switched from using its own infrastructure to Amazon Web Services (Amazon Web Services, 2022).

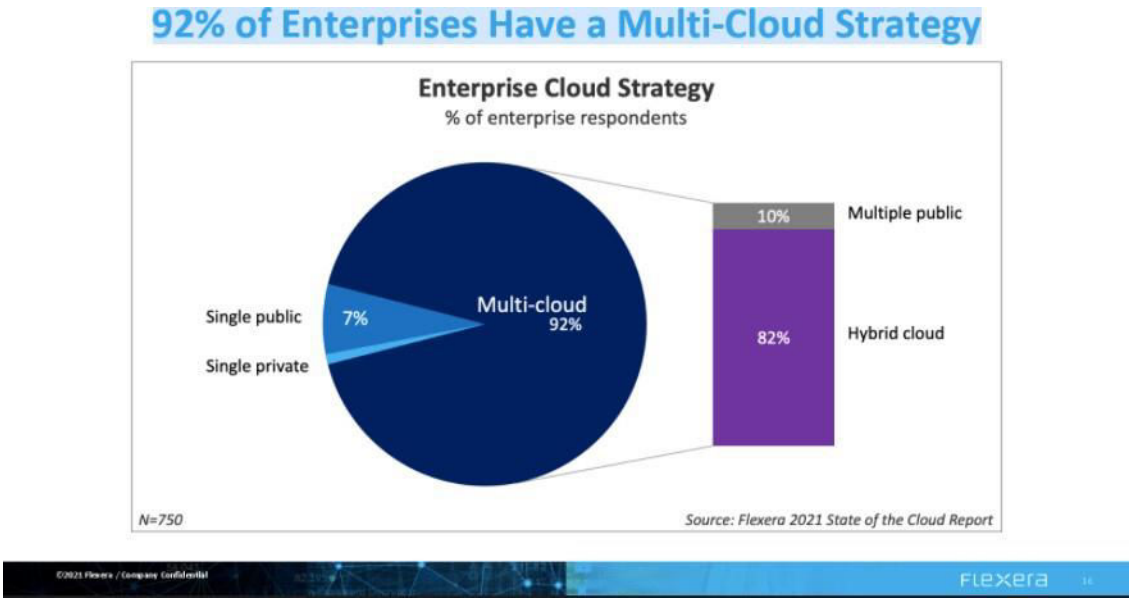

Figure: % of Enterprise adopting Multi- cloud Strategy
Source: (Flexera, 2021)

Key Concepts in Cloud Security

As stated by Tabrizchi & Rafsanjani (2020), the fundamental ideas that support the protection of digital assets in virtualized settings serve as the basis for cloud security. With 90% of organisations expressing concerns about cloud security, the 2021 Cloud Security Report by Cybersecurity Insiders highlights the pervasive worry (Fortinet, 2021). The Shared Responsibility Model, in which cloud service providers (CSPs) and clients jointly manage security, is a fundamental principle. For instance, AWS is a good example of this approach, where clients are in charge of security inside the cloud while CSPs manage security for the cloud infrastructure (AWS, 2019). IAM, or identity and access management, is yet another crucial component. IAM procedures are crucial for controlling resource access. For example, Google Cloud Identity and Access Management make it easier to manage user permissions precisely (Google Cloud, 2022). Data confidentiality is ensured via encryption, a pillar of cloud security. For protection against unauthorised access, Microsoft Azure's Transparent Data Encryption (TDE) encrypts stored data.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

An additional security measure is Multi-Factor Authentication (MFA). The best example of this idea is provided by Okta's Adaptive MFA, which modifies authentication based on user behaviour (Butt et al., 2020). These ideas are essential for creating thorough cloud security plans, guaranteeing data integrity, privacy, and effective risk management, as well as providing a strong framework for contemporary corporate operations.

Common Cybersecurity Threats in Cloud Computing

As stated by Ageron, Bentahar & Gunasekaran (2020). modern corporate operations are moving more and more towards the cloud, which opens up a new frontier of cybersecurity dangers that require attention and preventative actions. The "2021 Cost of a Data Breach Report" published by IBM Security and the Ponemon Institute reveals that the average cost of a data breach has risen to an astounding $4.24 million per occurrence, highlighting the significant financial ramifications of these risks (IBM, 2022).

In the cloud environment, data breaches are particularly concerning. High-profile events, like the iCloud breach in 2014, revealed weaknesses in data stored in the cloud (Kaloudi & Li, 2020). The incident, which revealed private celebrity images, underscores the dangers of insufficient security measures. An additional threatening problem is malware and ransomware attacks. Considering that 27% of breaches involve malware, the 2021 Verizon Data Breach Investigations Report highlights their relevance (Verizon, 2023). These attacks use phishing emails as entry points to infect cloud infrastructures. Once installed, ransomware has the ability to hold cloud-stored data hostage and demand high ransoms in exchange for its release (Offner et al., 2021).

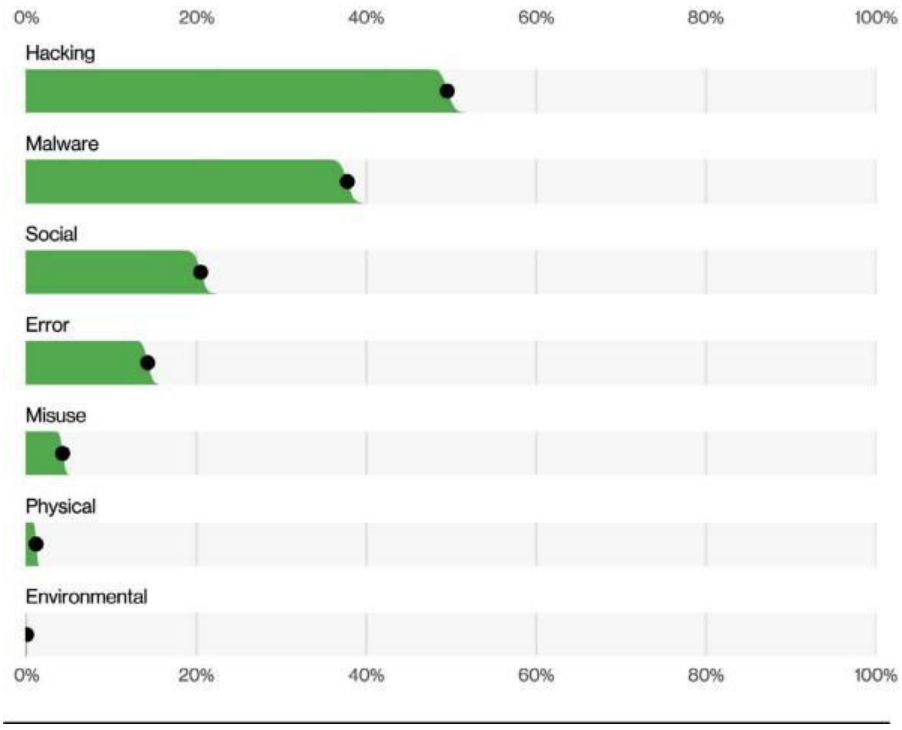

Figure: Actions in breaches
Source: (Verizon, 2023)

Attacks using denial of service (DoS) pose a serious risk. These assaults interfere with cloud services, leading to significant downtime and monetary losses. The 2020 Amazon Web Services (AWS) outage serves as an illustration of the possible repercussions of DoS attacks by having an impact on widely used online services and illuminating the susceptibility of cloud infrastructure to such attacks (Amazon, 2017). Another risk is posed by insider threats, which involve dishonest or careless insiders with access to cloud resources. The seriousness of these dangers is shown by high-profile incidents like the 2019 Capital One hack (Khan et al., 2022). The exposure of more than 100

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

million customer records was caused by improperly configured web application firewalls in the cloud environment. The significance of strong access restrictions and employee awareness is demonstrated by this incident.

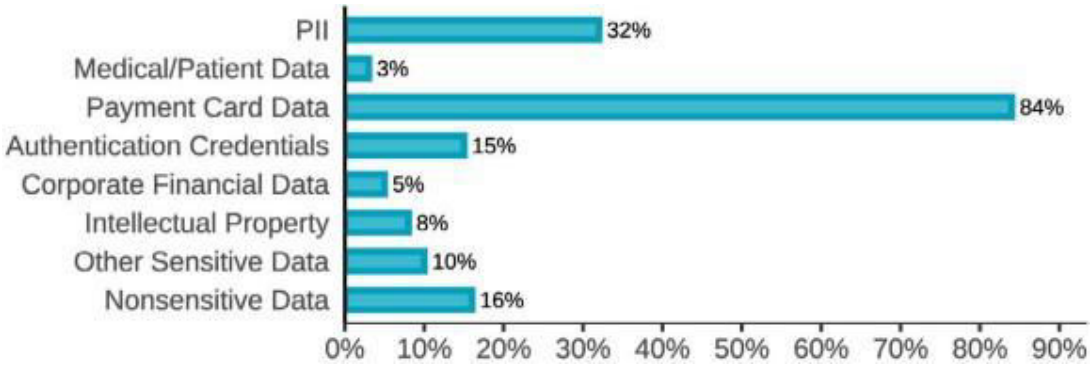

Figure: Percent of breaches in caseload
Source: (Verizon, 2023)

Furthermore, application programming interface (API) vulnerabilities are an important issue. Exploiting API flaws could result in unauthorised access to cloud services, which could endanger systems and expose data. These hazards are more than just hypothetical situations in the dynamic world of cloud computing; they pose actual risks with real repercussions. Therefore, thorough security measures, continual monitoring, and ongoing personnel training are essential to preserve cloud environments and safeguard sensitive data from these many risks.

Vulnerabilities in Cloud Infrastructure

As stated by Kitchin & Dodge (2020), certain vulnerabilities present difficulties inside the complex web of cloud infrastructure, necessitating vigilant attention and effective responses. As reported by Parn & Edwards (2019), understanding these vulnerabilities is essential for establishing a resilient digital environment because they have the ability to threaten the basic foundation upon which cloud services depend. Concerns about insecure APIs and interfaces are quite important. Interfaces and APIs that are insecure or poorly designed expose businesses to a variety of hazards. This vulnerability was demonstrated by the well-known Adobe breach in 2013 (Krebsonsecurity, 2013). Attackers gained access to millions of consumers' personal data by taking advantage of a flaw in Adobe's web services API. This incident emphasises the importance of fortified interfaces and APIs to secure cloud services.

A further risk vector is deficient Identity and Access Management (IAM) procedures. Unauthorised access and data breaches might result from weak IAM measures (Ande et al., 2020). 61% of breaches, according to the Verizon 2021 Data Breach Investigations Report, involved credentials that were stolen (Verizon, 2023). This highlights the critical requirement for strict IAM protocols to safeguard cloud environments from unauthorised access and exfiltration. The shared resources and multitenancy features that define cloud environments bring new dangers. The "CloudPets" incident from 2017 is a prime example of the effects of data leakage because of weak access rules (Goswami, 2017). Voice recordings and personal information of over 2 million customers were made available due to a misconfigured database in a cloud-hosted service, underscoring the risks of inadequate multitenancy management.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

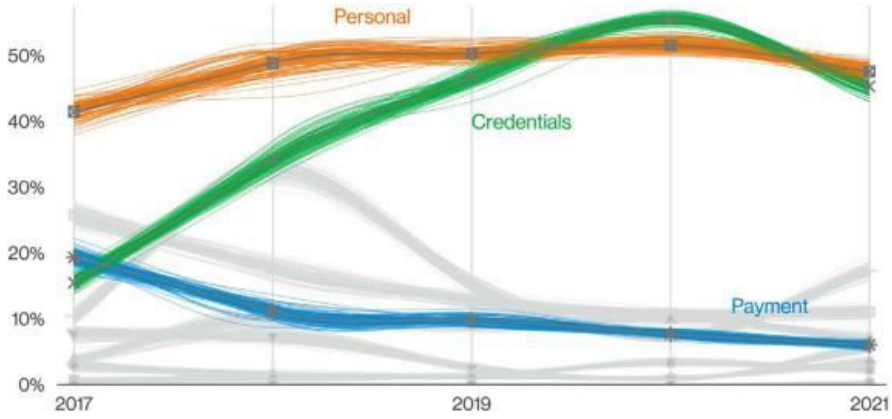

Figure: Top Confidentiality data varieties over time in breaches
Source: (Verizon, 2023)

As stated by Ageron, Bentahar & Gunasekaran (2020), the security environment is further complicated by virtualization issues. The flexibility and resource optimisation that virtualization technology provides come with certain potential concerns. The "Venom" vulnerability, which affected several virtualization technologies, was revealed in 2015 and showed how attackers may potentially escape from a virtual machine to access critical host data (Hassan et al., 2020). As stated by Gill et al. (2020), fortifying it against these vulnerabilities is crucial in a time when cloud infrastructure serves as the foundation of digital operations. In order to prevent potential attacks and guarantee the resilience of cloud environments, strict security measures must be included in interfaces, APIs, IAM practises, multitenancy management, and virtualization technologies (Paul et al., 2020). Strong security methods can turn these weaknesses into chances for proactive defence and all-encompassing protection against contemporary cyber threats.

Emerging Threats and Future Challenges in Cloud Security

As the digital environment changes, the field of cloud security encounters a constantly shifting panorama of new threats, requiring proactive solutions to protect critical data and activities (Abiodun et al., 2021). To ensure the stability of cloud infrastructures, these impending issues necessitate a proactive strategy.

The threat of zero-day exploits is significant. As demonstrated by the "Heartbleed" vulnerability in 2014, the growth of cloud computing multiplies the effects of zero-day vulnerabilities (Ali et al., 2022). Heartbleed, which took advantage of an OpenSSL flaw and might have compromised a large number of cloud services, highlights the need for organisations to improve their vulnerability management and response methods.

Machine learning (ML) and artificial intelligence (AI) present both potential and risks. Although AI and ML can improve security, they also give adversaries more advanced attack options (Alam, 2020). An example of AI-powered malware is DeepLocker, which shows how it may be used to mask malware and avoid detection. In order to defend against these AI-driven attacks, improved defence systems that comprehend and recognise changing assault strategies are required (Townsend, 2018).

The threat surface is expanded by IoT integration into cloud services. The vulnerability of interconnected IoT-cloud ecosystems was demonstrated by the Dyn DDoS assault in 2016, which affected important websites using a botnet of compromised IoT devices (Internet Society, 2017). To combat these new dangers, organisations need to improve the security of IoT devices, put in place strict access controls, and use intrusion detection systems.

Cloud infrastructure now comes under supply chain attacks. A number of organisations' cloud systems were compromised as a result of the 2020 "SolarWinds" hack, which targeted third-party software suppliers (Gupta,

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

2020). This incident serves as a reminder of the necessity of thorough supply chain risk assessments and increased inspection of third-party providers' security procedures. The difficulties with compliance and regulation are about to get worse (Nayyar, 2019). The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), two evolving data protection laws, add to the complexity of cloud security. In order to comply with regulatory requirements, businesses must negotiate a variety of compliance frameworks, put in place reliable data protection mechanisms, and develop incident response plans (IBM, 2022).

As stated by Torkura et al. (2020), organisations dependent on cloud environments must comprehend and anticipate these new dangers in a landscape rife with opportunities and difficulties. The importance of bolstering security measures, funding AI-enhanced defence systems, tackling IoT vulnerabilities, examining supply chains, and keeping up with changing compliance requirements cannot be overstated (Prasad et al., 2020). Organisations that adopt these techniques can successfully navigate the changing world of cloud security and protect their digital assets from unheard-of cyber threats.

Mitigation Strategies and Best Practices

As stated by Kaloudi & Li (2020), organisations should proactively protect their digital assets in the face of evolving cloud security risks by using strategic measures and best practises. A comprehensive strategy that includes encryption, access control, auditing, patch management, and employee education is needed to address the weaknesses mentioned above. Information saved in the cloud must be protected with encryption and data protection (Offner et al., 2021). Data must be encrypted both in transit and at rest. The importance of data encryption is highlighted by the fact that 53% of respondents to the 2021 Thales Data Threat Report view it as crucial to their cloud adoption strategy (Thales, 2021).

As mentioned by Kitchin & Dodge (2020), the combination of access control with identity and access management (IAM) provides a strong barrier against unauthorised access. Strong access controls based on the least privilege concept must be implemented immediately. According to the least privilege concept, users should only have the minimal access required to do their duties. The fine-grained permissions provided by Google Cloud IAM are an example of this strategy and improve security by reducing exposure (Google Cloud, 2022). Early threat detection depends on routine auditing and monitoring (Parn & Edwards, 2019). Continuous cloud environment monitoring and recurring audits make it possible to quickly spot suspicious activity. Organisations employing proactive monitoring might save up to $1.2 million annually, according to the Ponemon Institute's "2020 Cost of Insider Threats" report (CISA, 2020).

As mentioned by Ande et al. (2020), in terms of cloud security, patch management is a pillar. To fix known vulnerabilities, timely updates and patches are crucial. The 2020 "WannaCry" ransomware assault used vulnerable computers to cause devastation around the world (Gregory, 2021). This incident highlights how vitally important it is to immediately implement security updates to guard against potential breaches.

As commented by Aljumah & Ahanger (2020), risk reduction is considerably aided by employee training and awareness. A culture that values security is fostered by educating staff members about security best practises and the hazards associated with cloud computing. Employees were the weakest link in security chains, according to Proofpoint's 2020 "Human Factor Report," making training an essential investment (Proofpoint, 2020). These best practises work as foundations for strong security in a changing cloud environment (Nafea & Almaiah, 2021). Organisations can reduce threats and create a resilient security posture that protects their cloud infrastructure, data, and business operations by utilising encryption, putting into place strict access controls, conducting routine audits, vigilantly managing patches, and raising employee awareness.

V. CONCLUSION

In conclusion, a complex range of cybersecurity threats coexist with the transformational promise of cloud computing. It is crucial to recognise and deal with these difficulties because businesses are relying more and more on cloud infrastructure. Businesses may protect their digital assets from data breaches, malware attacks, DoS incidents, insider threats, and other developing risks by being aware of the vulnerabilities in cloud systems and implementing proactive mitigation techniques. A resilient cloud security posture must be established by

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

implementing encryption, strong access controls, ongoing monitoring, proactive patch management, and thorough employee training. Organisations will be able to take advantage of cloud computing while protecting their sensitive data and guaranteeing the continuity of their operations if they maintain an unwavering commitment to staying informed, adapting to new threats, and prioritising cybersecurity measures.

REFERENCES

[1] Abiodun, M. K., Awotunde, J. B., Ogundokun, R. O., Misra, S., Adeniyi, E. A., Arowolo, M. O., & Jaglan, V. (2021, February). Cloud and big data: a mutual benefit for organization development. In Journal of physics: conference series (Vol. 1767, No. 1, p. 012020). IOP Publishing.

[2] Ageron, B., Bentahar, O., & Gunasekaran, A. (2020, July). Digital supply chain: challenges and future directions. In Supply Chain Forum: An International Journal (Vol. 21, No. 3, pp. 133-138). Taylor & Francis.

[3] Ageron, B., Bentahar, O., & Gunasekaran, A. (2020, July). Digital supply chain: challenges and future directions. In Supply Chain Forum: An International Journal (Vol. 21, No. 3, pp. 133-138). Taylor & Francis.

[4] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.

[5] Alam, T. (2020). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.

[6] Alexei, L. A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research, (3), 128-133.

[7] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K.-I. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics, 11(23), 3934.
https://doi.org/10.3390/electronics11233934

[8] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications, 14(7), 1185-1191.

[9] Amazon Web Services. (2022). AWS Innovator: Airbnb | Case Studies, Videos and Customer Stories. Amazon Web Services, Inc. https://aws.amazon.com/solutions/case-studies/innovators/airbnb/

[10] Amazon. (2017). Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region.
Amazon Web Services, Inc. https://aws.amazon.com/message/41926/

[11] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.

[12] AWS. (2019). Shared Responsibility Model - Amazon Web Services (AWS). Amazon Web Services, Inc. https://aws.amazon.com/compliance/shared-responsibility-model/

[13] AWS. (2022). AWS Innovator: Netflix | Case Studies, Videos and Customer Stories. Amazon Web Services, Inc. https://aws.amazon.com/solutions/case-studies/innovators/netflix/

[14] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ...& Piran, M. J. (2020). A
review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.

[15] CISA. (2020). Insider Threat Mitigation Guide.
https://www.cisa.gov/sites/default/files/2022- 11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

[16] Flexera. (2021). Flexera Releases 2021 State of the Cloud Report Press Release. Www.flexera.com. https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report

[17] Fortinet. (2021). CLOUD SECURITY REPORT. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-cybersecurity-cloud-security-report-fortinet-2.5.pdf

[18] Ganne, A. (2022). Cloud Computing And Security Model-A Brief Survey. International Research Journal of Modernization in Engineering Technology, 4(11).

[19] Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A.,.....& Uhlig, S. (2022). AI for next
generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.

[20] Google Cloud. (2022). Cloud Identity and Access Management | IAM. Google Cloud. https://cloud.google.com/iam

[21] Goswami, S. (2017). MeitY Requires Government Departments to Have a CISO. Www.bankinfosecurity.asia. https://www.bankinfosecurity.asia/meity-requires-government-departments-to-have-ciso-a-9945

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

[22] Gregory, J. (2021, September 1). What Has Changed Since the 2017 WannaCry Ransomware Attack? Security Intelligence. https://securityintelligence.com/articles/what-has-changed-since-wannacry-ransomware-attack/
[23] Gupta, S. (2020). Taxonomy of The Attack on SolarWinds and Its Supply Chain. https://www.cisa.gov/sites/default/files/ICSJWG-Archive/QNL_MAR_21/SolarWinds_Technical_Brief_2020%20v3_S508C.pdf
[24] Hassan, W., Chou, T. S., Tamer, O., Pickard, J., Appiah-Kubi, P., & Pagliari, L. (2020). Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science. International Journal of Informatics and Communication Technology (IJ-ICT), 9(2), 117-139.
[25] IBM. (2022). Cost of a Data Breach 2022. IBM; IBM. https://www.ibm.com/reports/data-breach
[26] Internet Society. (2017). IoT Security for Policymakers. Internet Society. https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/
[27] Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.
[28] Kamal, M. A., Raza, H. W., Alam, M. M., & Mohd, M. (2020). Highlight the features of AWS, GCP and Microsoft Azure that have an impact when choosing a cloud service provider. Int. J. Recent Technol. Eng, 8(5), 4124-4232.
[29] Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. ACM Transactions on Privacy and Security, 26(1). https://doi.org/10.1145/3546068
[30] Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart Cities and Innovative Urban Technologies (pp. 47-65). Routledge.
[31] Krebsonsecurity. (2013). Adobe To Announce Source Code, Customer Data Breach — Krebs on Security. https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/
[32] Mughal, A. A. (2021). Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment. International Journal of Intelligent Automation and Computing, 4(1), 35-48.
[33] Mukherjee, S. (2019). Benefits of AWS in modern cloud. arXiv preprint arXiv:1903.03219.
[34] Nayyar, A. (2019). Handbook of Cloud Computing: Basic to Advance research on the concepts and design of Cloud Computing. BPB Publications.
[35] Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2021). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Health Security Intelligence, 92-121.
[36] Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. Engineering, Construction and Architectural Management, 26(2), 245-266.
[37] Paul, P., Aithal, P. S., Saavedra M, R., Aremu, P. S. B., & Baby, P. (2020). Cloud Service Providers: An Analysis of Some Emerging Organizations and Industries. International Journal of Applied Engineering and Management Letters (IJAEML), 4(1), 172-183.
[38] Podeschi, R. J., & DeBo, J. (2022). Integrating AWS Cloud Practitioner Certification into a Systems Administration Course. Information Systems Education Journal, 20(5), 17-26.
[39] Prasad, C. S. S., Yadav, B. P., Mohmmad, S., Gopal, M., & Mahender, K. (2020, December). Study of threats associated with cloud infrastructure systems. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022055). IOP Publishing.
[40] Proofpoint. (2020, April 6). The Human Factor 2019 Report - Modern Cyber Attacks | Proofpoint. Proofpoint.com. https://www.proofpoint.com/us/resources/threat-reports/human-factor
[41] Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how?. Qualitative Social Work, 18(1), 81-97.
[42] Sileyew, K. J. (2019). Research design and methodology. Cyberspace, 1-12.
[43] Sokolov, S. A., Iliev, T. B., & Stoyanov, I. S. (2019, May). Analysis of cybersecurity threats in cloud applications using deep learning techniques. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 441-446). IEEE.
[44] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
[45] Thales. (2021). 2021 Thales Data Threat Report | Thales. Cpl.thalesgroup.com. https://cpl.thalesgroup.com/2021/data-threat-report#download-popup
[46] Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2020). Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure. IEEE Access, 8, 123044-123060.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209023 |

[47] Townsend, K. (2018, August 13). IBM Describes AI-powered Malware That Can Hide Inside Benign Applications. SecurityWeek. https://www.securityweek.com/ibm-describes-ai-powered-malware-can-hide-inside-benign-applications/#:~:text=In%20short%2C%20DeepLocker%20is%20a

[48] Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[49] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172- 2175.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details