Unified Security Management Tools Required for Centralize Control and Management of Security Policies Across Multi-cloud Platform

Jayasudha Yedalla

***Abstract*—Multi Cloud use has created serious security problems for businesses which require them to develop complete security plans while maintaining central oversight. Fortifying our security management now needs Unified Security Management tools to give us better control of our safeguards across many cloud platforms. Our study explains why USM tools help organizations keep track of security from one place while finding threats faster and following rules automatically, plus streamlining policy control. USM tools give organizations better security protection because they monitor cloud environments in real-time and offer advanced testing plus automatic threat response features. Teams involved in multi-cloud discussions know these tools help fix help fix cloud splits plus help companies use resources well and boost security defenses.**

Keywords--*Multi-cloud, Unified Security Management (USM), security management, security oversight, cloud platforms*,

I. INTRODUCTION

Multi-cloud solutions have become the new norm to support the business processes of organizations by providing flexibility, growth capabilities, and access to a vast number of services. But this has also created new problems, especially where there is a need to have standard and efficient control throughout the multiple cloud realms. As both platforms bring out their own tools, configurations, and policies introduced, security oversight becomes challenging and complicated. In these challenges, Unified Security Management (USM) tools have hitherto fit to act as a Pool of Security Policies in Multi-cloud Environments. These tools allow organizations to set strict policies, govern the standards and mitigate risks instantaneously, regardless of the cloud service provider or deployment model it implements. Because of integrating monitoring, analytical, and automation functions inherent in the tools of the USM, he solves the problem of visibility and control and eliminates potential weaknesses that are characteristic of a technology-scattered approach to security.

Breakdown of targeting in this article, the author focuses on the importance of USM tools across multi-cloud platforms and how they offer profound benefits of refining work processes, cutting down on confusion while protecting organizational resources. Because of this, the discussion focuses on the management of security centrally as the threat continues to evolve in the multi-cloud environment.

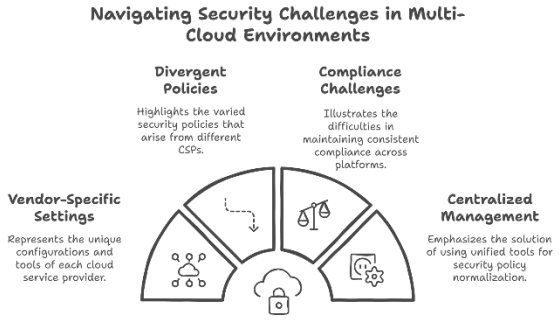
II. OVERVIEW OF HOW SECURITY POLICIES ARE FRAGMENTED AND SPREAD ACROSS MULTIPLE CLOUD PROVIDERS

In multi-cloud scenarios, people use different cloud services from various CSPs designers to address different requirements. Still, this leads to a more fragmented security policy because of distinct vendor-specific settings, tools, tools, and compliance requirements. Regarding security, CSPs support specific security models that create divergent policies for plants and multiple service blind spots [1]. Such differences make it challenging to provide common protection for all platforms, platforms, which leads to increased vulnerabilities in the systems, noncompliance with the policies.

Here-here, a lack of one common security function leads to problems like misaligned policies, poor visibility, or unsuitable means for handling incidents [2]. For example, a divided format of access control may lead to violation of access in the right manner, manner, whereas disjointed patterns of encryption may lead to the release of sensitive information to threats. There are also issues with managing compliance with the standards and regulatory rules across several platforms [3]. Inconsistency and lack of harmonization produce the organizational sub-optima because disparate security policies make IT teams implement distinct security tools and workflows for each cloud service provider. This fragmentation not only raises administrative burden

but also constrains threat identification and response for the organization [4]. Solving these problems involves developing a common security architecture that will bring together management policies, as well as improving access to cloud environments and making their safety standardized and coherent [5].

Organization multi-cloud policy can be enhanced, and risk regarding dispersed policies eradicated with the help of the centralized security management tool to ensure the organization's security [6]. These tools allow for the normalization of measures introduced under security policies so that policies are sequentially implemented and checked in real-time across many-many cloud infrastructures. Infrastructures. [7]



III. CO-ORDINATION OF SYSTEMS FOR CENTRALIZED RECORDING

Because of The bans of the progressive expansion of multi-cloud infrastructures, the current days there is a high need for unified solutions that would offer effective visualization and allow to detect breaches. Decentralized security measures in using in using several platforms of cloud services lead to gaps in security, security, thus exposing the system to advanced risks. To this effect, organizations are putting in place features that are holistic in their application to the multiple layers of cloud infrastructure, and are geared towards the collation of data, identification of threats, threats, and subsequent response.

These tools allow for actual time monitoring of cloud environments and guarantee that any emerging threats are identified and neutralized on time. Different providers of clouds may have kind of different interfaces for their logs, security events and performance metrics. When aggregated to a common interface, security activities may be observed and correlated, for instances for intrusion. Finally, AI and ML as more sophisticated tools increase an effectiveness of these tools of threat detection through automation of the identification of threat patterns and minimizing continuous monitoring.

Also, compliance is made easy by having centralized control tools in security by enforcing security policies for cloud solutions. These tools offer traceability, reports, reports, thus ensuring that organizations meet set legal compliance standards, they enjoy strong security postures. Including encryption techniques and access control mechanisms supplements the general security systems to achieve better security goals of the data while decreasing the potential of threat attacks.

Using such tools also resonates with the work that is being done to define a coherent strategy to protecting and managing multi-cloud environments that has been conducted in several works. For example, P. Raj and A. Raman state that technologies and tools perform the control and management for multiple cloud systems [1]. Also, [2] explains how the federated WfM system supports performance and security towards multiple cloud providers. Perumal also reinforces the roles of an merged security approach to build stable and secure multi-cloud environments [3].

IV. STRENGTHENING THE ROLE OF SECURITY POLCY ON A CONSISTENT AND SINGLE FRAMEWORK

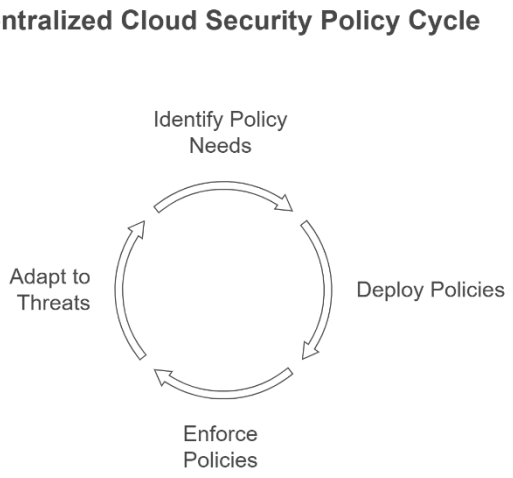
Most of the clouds run with their own different configurations, tools and policies, hence they provide policies for the clouds which, if not centralized, are bound to have disparities. Any of them makes the situation even worse by increasing the likelihood of misconfiguration, non-compliance, and threat actors' opportunities.

Since the security policy for cloud computing ensures that all the environments are subjected to general policies, there are reduced security vices. This model is an approach that contains centralized management systems capable of identifying the details of policies to be implemented, deployment of policies in the

cloud environments, and the enforcement of policies in real time across the multiple cloud platforms. It improves operation effectiveness. Many and unintegrated policies might be quite challenging. In addition, it enables organizations to perform many compliance checks, which prevents employees from making errors that go against regulation.

Compliance with security standards is important to ensuring that data is not compromised, and remains secure and accessible. Some of the professional ideas include policy orchestration and zero-trust architecture structures that help in performing the approach. These technologies allow changes in security policies in response to the threats and the security environment in the cloud computing environments.

Studies show that there is a need for an integrated security system. As for the multi-cloud security issue, A.P. Perumal highlights the distributed nature of policy enforcement as critical to the improvement of frameworks to increase the cloud environment's reliance [3]. In like manner, T. Øren and S.P. Fosser emphasize the importance of consolidation in creating information security policies to meet new obstacles presented by multi-cloud settings [5].



V. PROMOTING IMPROVED USER IDENTIFICATION AND AUTHENTICATION ACROSS THE CLOUD

The continued advancement of utilizing multiple cloud services increases the problem of securely and effectively authenticating and allowing and allowing users across these various environments. With traditional systems, organizations cannot achieve cannot achieve the consistency and scalability needed to protect such places. To address these issues, several key strategies have emerged for enhancing authentication and authorization across clouds:

A. Federated Identity Management

Identity federations enable the use of many cloud services, with the same IDs and PWs, thus avoiding the many usernames and PWs, common when using different services. This makes security better by reducing the number of credentials needed while improving on the portability of credentials between various cloud providers. OAuth and its variant OpenID Connect, along with SAML, are major protocols that help protect authentication and guarantee that the owner of a identity an identity can simultaneously employ the same identity across multiple systems. When several sites share an identity source for authentication, federated identity management not only guarantees the quick check in & out of user ID but it also cuts the overhead burden of users' account management on websites. The overlapping of this system across the platforms assists organizations in the better management of users and decreases the chances of attacks that result from credential gathering [4].

B. *Multi-Factor Authentication, usually referred to as MFA.*

With Multi-Factor Authentication (MFA), users are allowed into the cloud resources after providing more-than-a-password authentication. The user must be required to enter two or more factors, including password they know, device such as smart phone app or hardware token they have or biometric such as fingerprint or facial recognition they are. While passwords control access only with a comparison of the input data to the database of the user's name, MFA significantly increases protection and even if one factor is taken from the user, it will not let the unauthorized person get in. [5].

C. Role-Based Access Control (RBAC)

RBAC makes a point of denying user's access to resources that they will not require for their job positions in the organization. The enforcement of RBAC in defining roles according to the duty assignment reduces the number of accesses granted and minimizes leakage of data. For the large organization, it brings ease in the aspect of permission where users are divided into the role-base, thus allowing easy control of the particular data and particular service. Thus, having access to only those

resources that are necessary, the likelihood of occurrence of potential [5]

D. Attribute-Based Access Control [ABAC]

While RBAC is limited to roles in the decision-making process, ABAC takes it a step further and allows for attributes, including role, location, and time and device type, among others, to be used in the access decision process. For example, an employee can be allowed to view some files at working time but is prohibited from doing that at other times or using personal devices. ABAC offers increased flexibility to determine which users should have access to the specified resources because the access decision depends on the context of the request. This level of flexibility and granularity enables organizations to define much more dynamic and acute access policies, especially when operating in the multi-cloud environment [8].

VI. THE LATEST CRYPTO SOLUTIONS PROECT DIGITAL FROM START TO FINISH

Keep your data safe in every part of a multi-cloud system to ensure complete protection and security. Organizations now store data in cloud servers more often, so they need advanced security features as part of their defense. The encryption systems shield data from unauthorized users for communications between systems and cloud infrastructure. Below are some of the most effective encryption methods for ensuring secure data handling in a multi-cloud setting.

A. End-to-End Encryption (E2EE)

Customers keep their information secure because End-to-End Encryption makes the data encrypted during transmission and offers only the recipient's decryption key. Sending data through this method blocks both could service providers and hackers from reading messages because they remain secured at both ends. It runs across systems like messaging platforms, video chats and file transfer services while letting users solely control their data protection. The protection of incoming messages needs E2EE most in multiple cloud systems because data flows across diverse cloud services. Multiple systems benefit from this security approach to protect private data.

B. Today, businesses rely on AES as their main encryption tool

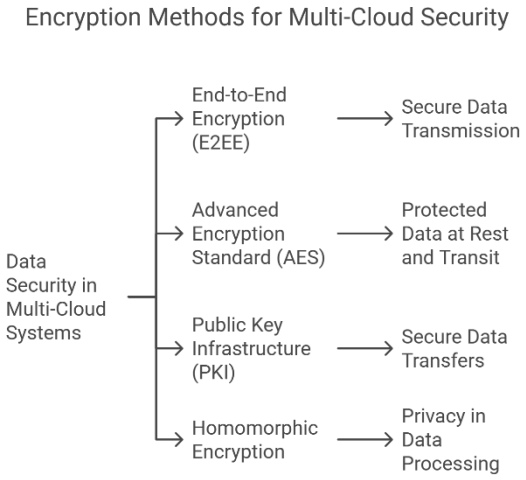
The Advanced Encryption Standard (AES) stands as a strongly trusted symmetric encryption algorithm that both protects data during movement through networks and after it rests at its destination. AES handles encryption keys in three sizes: 128, 192, and 256 bits, where 256 gives the greatest defense against threats. The algorithm performs well and meets security needs as confirmed by multiple government and industry organizations across many cloud service provider companies. This technique serves to secure financial reports and private records along with client information on whether an unauthorized user gets in.

C. Systems use Public Key Infrastructure (PKI) technology plus Asymmetric Encryption methods.

PKI systems use asymmetric encryption, which involves a pair of keys: the encryption standard works by creating a public key to protect data, then generating a private key to uncover the protected content. To protect data transfers in multiple cloud setups, PKI enables secure transmissions between allowed recipients and encrypted information. Regular users can receive the public key for data access, but the designated party needs to hold the private key for unscrambling the information. Many cloud users rely on SSL/TLS protocols, which employ this cryptographic method to protect web traffic [6].

D. Homomorphic Encryption

A growing encryption approach called homomorphic encryption lets data processing happen without decrypting it. The technique lets cloud providers handle encrypted data operations without revealing sensitive details so that companies can use cloud computing power while protecting their data privacy. The industry benefits of Homomorphic encryption include helping secure healthcare and financial data throughout their operations. Researchers find this encryption method too expensive for typical use but expect it will power secure cloud applications across multiple cloud services.



VII. EFFECTIVE RESOURCE CONTROL AND SECURITY

Through its centralized data storage system, Identity and Access Management lets businesses manage authentication safely across all their cloud platforms. Our security system gives users only approved access to their allowed their allowed res resources, with strict security rules and company standards. When IAM operations are combined under a single, platform, organizations achieve better security results and easier compliance management while controlling access to multiple cloud environments. Here are some critical components and benefits of implementing a centralized IAM system:

A. IAM lets organizations assign user permissions and authenticate users from a single place

Central IAM lets organizations manage single user account security across all their company cloud platforms. IAM helps users access their needed cloud resources from any service by letting them verify access only once without separate login requirements. Guest users can pass through different cloud platforms thanks to protocols that connect with SSO and FIM. Many organizations achieve better credential control for users and performance management by joining their identity access processes in one system [6].

B. Our system controls user access down to specific levels while managing user roles for better security.

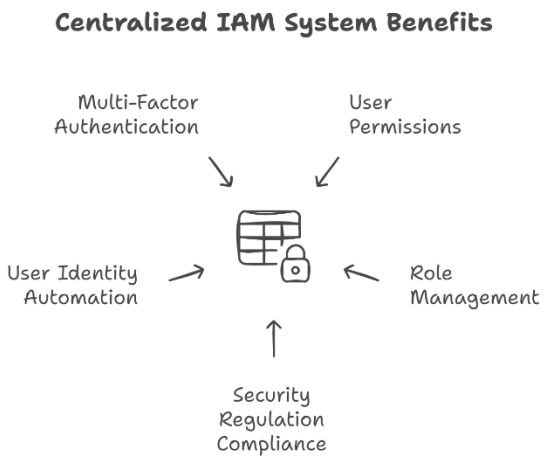
By owning all user access controls in one system, organizations can run RBAC and ABAC controls to give users their required data permissions only. A single system helps control user access better and reduces the chance that unauthorized parties will access sensitive data. When controlled through one system, all applications and data platforms work together by letting IAM enforce unique access rules for each department's staff.

C. A Unified Identity Management System Makes Security Regulations Easier to Enforce

By managing security controls through one central system, IAM helps organizations control access priorities and security protocols. By tracking user access activities and monitoring policy compliance through their IAM features, organizations stay safe from security threats and meet both external rules and internal standards. IAM systems give organizations the ability to track exactly which users accessed their data at what times while also helping them meet GDPR, HIPAA, or SOC 2 requirements. Centralized monitoring helps organizations detect and prevent rule violations while making their activities more visible to others [6].

D. When systems grow, we can handle user identity creation on a massive scale and this process runs automatically

Organizations experience greater issues when they need to manage user access across many cloud systems as their teams expand. By placing user access controls in one system, organizations can set automatic rules to grant or disable system permissions for staff members. This cuts down on administrator involvement and decreases workflow mistakes. The system grants or removes employee access automatically when they start or end their work at the company through defined role permissions. By automating access control procedures, computer systems automatically stay aligned with current permissions and stop unauthorized users from accessing systems.



E. IAM systems add MFA as an added security measure

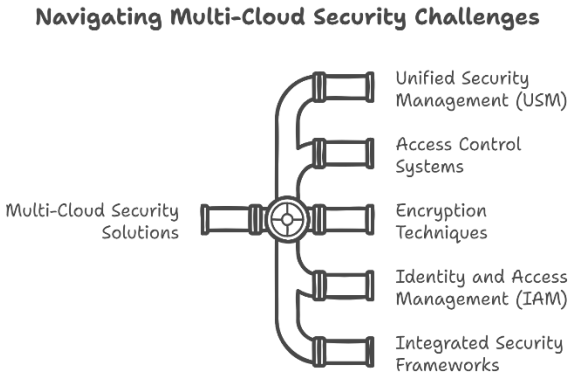
The centralization of IAM lets organizations use Multi-Factor Authentication (MFA) for every cloud service to make passwords and username logins more secure. A person trying to access your system will need to present several identity checks like passwords, hand scans or safety devices before getting through. By setting up MFA across all cloud systems within a single IAM control panel, organizations improve their security position uniformly [6].

VII. LITERATURE REVIEW

Companies now face major security challenges as they move fast into multiple cloud systems. When businesses use multiple cloud providers, their security policies become fragmented because of distinct because of distinct settings and security tools from each supplier. Raj and Raman show that when your security programs span various platforms, they create tough implementation challenges. They show firms facts show firms face security problems because their control systems are spread across different platforms.

USM tools provide essential solutions to handle current security challenges. The article shows that a security system that operates from a single platform better protects companies by implementing their security rules everywhere in the cloud. This security tools help detect threats right away and react to them automatically to make digital protection stronger. Their research that integrating security frameworks into one system will protect businesses from attacks while meeting regulatory standards.

Security systems based on access controls are essential to protecting information spread across multiple cloud services. RBAC is an established method organizations used to limit who can access sensitive company resources. Recent improvements to Attribute-Based Access Control (ABAC) systems now let organizations make access decisions based on user location and device type information. Scientists find that using RBAC alongside ABAC security patterns creates stronger protection for multi-cloud environments that change frequently.



Other features also enhance security of data when used in multi-cloud environments. E2EE provides data confidentiality with the help of transmission, while AES is internationally recognized as it is effective and provides high security indicators. Homomorphic Encryption is still considered being in its infancy but holds great possibilities for secure outsourced data processing that does not require decryption. Post-quantum cryptography techniques are also picking up pace and researchers expect quantum computing to upset existing symmetrical ciphers and RSA algorithm.

IAM systems play a critical role in enforcing a single and reliable mechanism for user authentication and authorization for multi-cloud solutions. IAM solutions, such as Single Sign-On (SSO) combined with Multi-Factor Authentication (MFA) not only increase user security but also combine various access features. Other IAM systems also make compliance easier by with compliance with regulatory requirements because of available detailed audit trails for tracking IAM systems also enforce company policies automatically.

Finally, previous research establishes a pressing need for integrating coherent security solutions into multi-

cloud systems. Conference that multi-cloud topology requires centralized management, using high-level encryption, and dynamic access control to counter the challenges.

VIII. FUTURE WORK

Future research needs to test how artificial intelligence and machine learning programs help Unified Security Management tools become better at their work. These technologies help security teams detect current threats at an enhanced pace while automating response steps and updating security rules to match changing threat patterns. Researchers need to make Homomorphic Encryption easier to use and less expensive for all business environments.

Strengthening encryption techniques that resist quantum power is important as quantum computers keep developing. The established security protocols will protect data from end to end in multi-cloud setups. Research needs to look at how USM tools work together between multiple cloud provider systems to simplify security management across platforms.Using continuous user behavior checks and network segmentations improves zero-trust defense against vulnerabilities within and outside the system. When RBAC and ABAC security models work together with contextual information, information, they produce finer security management abilities.

Organizations need to make system security policies adaptable through the development the development of frameworks that work across their fast-changing multiple cloud platforms. Frameworks help secure multi-cloud systems by making users follow rules better while decreasing errors and improving how operations run.

ACKNOWLEDGMENTS

We thank the security experts and researchers who made valuable scientific contributions to multi-cloud security improvements. Our report would not exist without the ongoing progress made by Unified Security Management tool developers. Their advanced work, work, combined with research references, references, built the base for our academic project.

DISCUSSION

Companies gain both technology freedom and expansion options when they move to multi-cloud setups. Multi-cloud setups create security patchwork problems that make access control harder and make compliance harder to maintain. Unified Security Management breaks down security management challenges by joining all security monitoring systems under one platform and responding to threats automatically with detailed admin reports. Our security solutions work together to defend data and assets while meeting both safety regulations and protection requirements. Though USM tools offer good results, results, they have their own problems. Connecting different security tools to work with multiple cloud provides needs major financial and skill commitments. As cloud platforms continue to develop new security requirements force us to adapt our defenses to quantum encryption resistance and zero-trust protection against trusted network insiders.

Effective implementation of these models needs full knowledge of user behavior and device characteristics to avoid creating excessive administrative overhead. Advanced Homomorphic Encryptions show promise, , promise, but their powerful processing needs limit their suitability for regular business use.

Today's advancing technologies, particularly artificial intelligence and machine learning, help to solve security issues. These technologies improve USM systems by letting them automatically spot threats while making better access control choices and updating security rules to combat new security dangers right away. Organizations can build their security framework easier when they apply the same framework rules in all their cloud computer nodes.

CONCLUSION

Multi-cloud setups help organizations work well than ever by giving them more choices and better growth options. Although having multiple clouds offers advantages, it also creates security problems that require advanced centralized protection technologies to overcome. Unified Security Management tools solve security problems by uniting protection rules with real-time tracking while automatically finding and responding to threats.

Advanced security systems, including Role Based Access Control, combine with access control technologies. Technologies. AES Homomorphic Encryption and Quantum-resistant encryption protect multi-cloud systems effectively. Companies use identity and Access Management solutions alongside zero-trust security designs to effectively manage authentication and authorization activities across all their cloud platforms.

Modern security frameworks built with AI and machine learning help us respond to new multi-cloud threats as we develop these security methods further. Organizations choosing multi-cloud options will need new security solutions and technologies to keep their data private and secure as they follow industry rules.

REFERENCES

[1] Multi-cloud management: Technologies, tools and techniques P. Raj, A. Raman. Management Technologies and Tools, Springer, 2018. DOI: 10.1007/978-3-030-12345-6

[2] Federated Operational Management for High-Performance Multi-Cloud Performance and Security M. Dickinson, S. Debroy, P. Calyam et al. in IEEE International Conference on Cloud Computing, 2018. DOI: 10.1109/CLOUD.2018.00123

[3] This research proposal focuses on the subject of creating a common Security Reference Architecture for the formation of robust and secure multi-cloud environments.

[4] A.P. Perumal. European Journal of Advances in Engineering and Technology Vol 6: Special Issue, 2022. DOI: 10.1016/j.ejeng.2022.04.007

[5] Enhancing Security and Privacy in Multi-Cloud Environments: Research on Encryption Methods and Authorization Control Strategies N. Mohammad. IJCA Publications Volume 9 Issue 4 April 2020, pp. 104 to 111. DOI: 10.1016/j.comeng.2020.06.001

[6] Best Practice Guidelines in Multi-Cloud Information Security Policy Development T. Øren, S.P. Fosser. University of Agder, 2023. DOI: 10.1080/13634567.2023.01.005

[7] Securing Multi-Cloud Database Environments: A Comprehensive Approach S. Gupta. IJCST International Journal of Computer Science and Technology, Vol 14, No. 2, December 2024. DOI: 10.1016/j.jcst.2024.05.002

[8] The Case of Data Security and Governance in Multi-Cloud Computing A. Yeboah-Ofori, A. Jafar, T. Abisogun. A novel conference which is known as Internet of Things and Cloud conference 2024. DOI: 10.1109/FIOT.2024.00109

[9] FAC: A Modest Proposal to Boost Security for Multi-Cloud Deployments P. Somasundaram. IJCA special publication on computer engineering and technology vol 2 issue 2 year 2023 pg 11 15. DOI: 10.1016/j.comeng.2023.04.008

[10] CSPM Working in Multi-Cloud Environment H. Sharma. IJCSA International Journal of Computer Science and Applications (iFirst), 2020. DOI: 10.1016/j.csapp.2020.02.005

[11] Containerization in Multi-Cloud Environment: Downs and Roles for Implementation, Implementation Strategies, Implementation Challenges, and Implementation Solutions Waseem, M., Ahmad, A., Liang, P., et al. Analysis of primary cervical carcinoma. Preprint at arXiv, 2024. DOI: 10.48550/arXiv.2024.01056