World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Analysis on addressing the threats to cloud computing on the basis of security safeguards for sap cloud services

Vedaprada Raghunath *

IT Director, IMR soft LLC, USA.

World Journal of Advanced Research and Reviews, 2024, 23(03), 2539–2548

Publication history: Received on 14 August 2024; revised on 24 September 2024; accepted on 26 September 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.3.2912

Abstract

Cloud computing has become an integral part of combination/multi-cloud infrastructures due to its many benefits, including quick deployment, flexibility, cheap costs, and scalability, which have attracted businesses of all sizes. New possibilities and threats in terms of security flaws are cropping up in this field, even if cloud storage provides substantial advantages and inexpensive choices for IT administration and growth. When we talk about safeguarding cloud infrastructure systems, we're referring to a set of rules, regulations, and systematic procedures. This is also known as cloud computing security. The purpose of implementing these security measures is to safeguard cloud-based data, facilitate the enforcement of legislation, ensure the privacy of consumer information, and set standards for encryption in specific devices and applications. Modern cloud computing and security concerns throughout the cloud's many layers are addressed in this study. Within this context, the current study would make a substantial contribution to lowering the frequency of security breaches in cloud computing, paving the way for the continued provision of safe and reliable services. Storage of databases on the cloud is expanding rapidly in the IT industry, including SAP networks. Because enterprises are ultimately responsible for the security of their data, migrating databases to cloud computing environments brings with it a plethora of security risks. To guarantee data integrity, availability, and secrecy, appropriate security measures should be put in place before a company migrates its sensitive data to the cloud. When data is at rest, it is most vulnerable to unauthorized access; when it is in transit, it must be subject to strict supervision.

Keywords: Cloud computing; Cloud security; Cloud security issues; Security attacks; Intrusion

1. Introduction

In today's world, it is both difficult and expensive to keep up with the traditional computing technology. In today's environment, it is becoming increasingly difficult to transmit information in any location at any time using traditional computing. This is particularly relevant since that peripheral storage configuration is a must-have for any data storage involving sensitive personal information [1-5]. Increasing numbers of internet operators on sharing portals, social networking, digital broadcasting, and related themes are putting a strain on outdated computing. As the number of people using the Internet, the number of resources being used, and the convenience of accessing them continue to rise at an exponential rate, a new paradigm in cloud computing services is necessary. The concept of cloud computing has recently received a lot of interest within the field of ICT.

Most commonly, cloud computing is related with the transfer of facilities and data processing to a location-transparent service or provider, whether that service or provider is located within or externally [6-8]. The use of cloud computing has made a significant impact on every organization in the globe, regardless of the location or the sector in which it operates. The cloud-based system is currently being utilized for the entirety of the enterprise system, which includes everything from fundamental development tools to big databases and software designed for enterprise use. Cloud

[*] Corresponding author: Vedaprada Raghunath

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

computing security is an essential precondition in this setting, as cloud computing is genuinely a pivotal component of numerous IT discussions [9-11]. Most discussions revolve on the usual suspects: the pros and cons, the ease and security, and the details.

Despite this, even the most widely used protection mechanisms are not always sufficient to keep the data from being damaged, accessed in an unauthorized manner, having its integrity compromised, and other similar threats. [12-13]. There are a great number of additional critical and significant aspects of any information technology architecture that ought to be enforced in a manner that is significantly more effective. The cloud-based infrastructure is one example of such a system [14]. Cloud computing's scalability, enhanced mobility, and flexibility in application development, as well as its decreased storage costs, make this prediction seem obvious. Regardless, the cloud's hyper-connected nature raises serious concerns about the safety of the cloud computing infrastructure. Figure 1 shows the current state of affairs in terms of the accessibility of various computer platforms and resources.

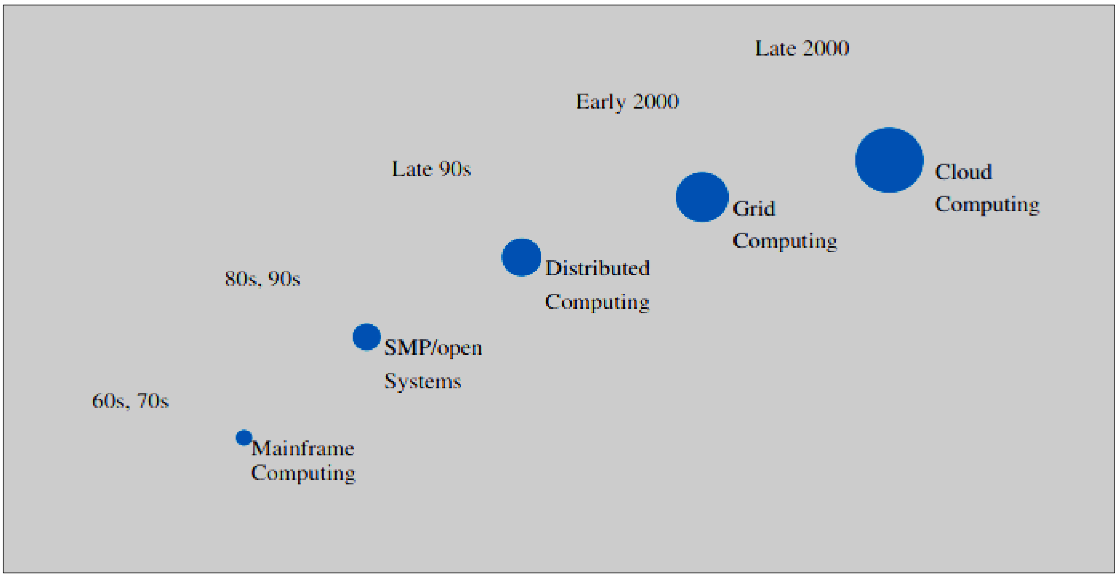

Figure 1 The evolution of computing architecture.

Cloud computing, an ever-expanding Internet-based programme that integrates several applications, services, and infrastructure, is characterised by on-demand and pay-as-you-go computing.

A comparable technology was utilized by telecommunications companies in the year 1960 in order to supply point-to-point data lines. This was the beginning of the principle that underpins this modern invention. This practice was carried out until the year 1990, when it was successfully replaced by the implementation of virtual private networks. Conversely, the cloud has been integrated into both server and structure in an effort to lessen network traffic and enhance communication efficiency.

Through the development of new data centers, Amazon has played a significant part in the process of building cloud computing. It was applied in 2007 by Google, IBM, and a number of other organisations and businesses that are considered to be exceptional [15].

2. Literature review

The research paper [16-23] adds to the current body of knowledge by presenting a thorough comparison of cloud security frameworks and standards. This is a great resource for academics and practitioners looking to weigh the pros and cons of different security frameworks and make educated decisions on cloud security adoption.

According to Gartner, four of the most significant challenges associated with cloud computing include governance, the selection of cloud environments, and security and privacy concerns. For the purpose of minimizing risk, regulating expenses, and producing profit, the board of directors ought to be in charge of guiding cloud investments. The growing popularity of cloud computing has recently caused a shift in how businesses handle and retain their data. The cloud offers numerous advantages, such as scalability, cost-effectiveness, and flexibility, among many others. However, due to the increasing dependence on cloud services, it is crucial to establish adequate security protocols. By utilising cloud security frameworks, organisations can develop and implement security rules tailored to their particular cloud environments [24-25]. Among the many security-related subjects covered by these documents are risk assessment, security solution selection and implementation, security monitoring, incident response planning, and continuous security improvement. You may see all the many kinds of frameworks that are currently available in Table 1.

Table 1 Introduction to Frameworks

Frameworks	**Description**
COBIT 5 for Cloud Computing	Specialised issues related to cloud computing are addressed by extending the COBIT framework.
NIST	Addresses privacy and security concerns in the cloud by outlining recommended methods and standards
ISO 27017	Information security best practices for cloud services according to ISO/IEC 27001
FedRAMP	A standardised approach for evaluating and authorising cloud security is provided by a federal programme in the US.
AWS Well-Architected Framework	The article lays out the best ways to build and manage secure and efficient cloud infrastructures.
CSA STAR	Data stored in a database that describes how various cloud providers adhere to the Cloud Control Matrix developed by the Cloud Security Alliance (CSA).
ENISA Cloud Security Guide	Covers a range of security issues and offers guidance on how to assess and mitigate risks in cloud environments.

Table 2 Cloud security issues: a comparative study

Threats	**Affected Cloud Services**	**Effects**	**Solutions**
Abuse of cloud computing	PaaS and IaaS	Validation Loss, Service Froud, Strong attacks due to unidentified sign-up	Network analysis, Robust registration and multifactor authentication
Insecure API	PaaS and IaaS	Improper authentication and authorization, the wrong transmission of Content	Data Encryption, Strong access control and multi-factor authentication
Malicious Insider	Paas, SaaS and IaaS	Asset damage productivity loss and confidentiality break	Duty Segregation, IAM policies
Data Loss	Paas, SaaS and IaaS	Removal, modification and stealing of confidential and personal data	Disaster, backup and recovery management
Service and Account hijacking	Paas, SaaS and IaaS	Breaching into critical areas of cloud and server, access of root account	Adoption of strong authentication, and security policies.

Cloud computing offers numerous benefits, such as accessibility from anywhere at any time, better geographic coverage, less infrastructure investment, and many more. Nevertheless, cloud computing is associated with a number of potential security complications. The security of data, applications, and infrastructure that are kept in the cloud may be compromised as a result of these vulnerabilities. Managing these risks is critical for ensuring the availability, integrity, and confidentiality of cloud resources, especially as more and more companies are depending on cloud services. The following graphic shows a few of the most typical worries about cloud security. A given that Figure 2 illustrates some of the most common cloud security issues [26-32], and Table 2 details the effects on cloud services and the cloud and cloud services that are affected.

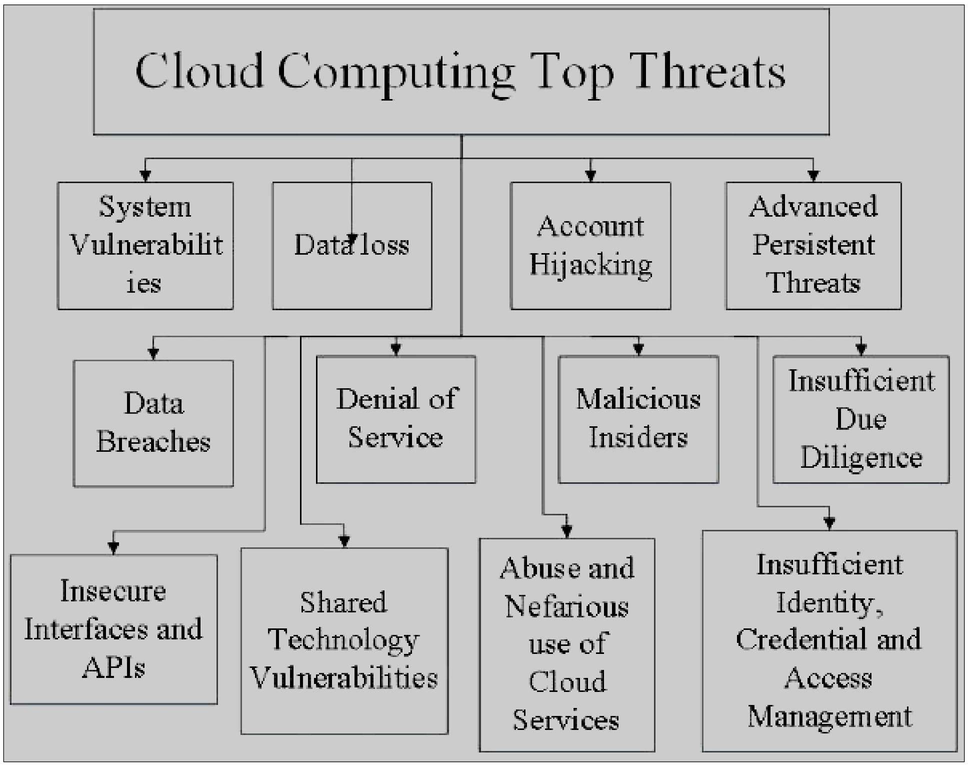
Cloud Computing Top Threats
System Vulnerabilit ies
Data loss
Account Hijacking
Advanced Persistent Threats
Data Breaches
Denial of Service
Malicious Insiders
Insufficient Due Diligence
Insecure Interfaces and APIs
Shared Technology Vulnerabilities
Abuse and Nefarious use of Cloud Services
Insufficient Identity, Credential and Access Management

Figure 2 Top Cloud Security threats

3. Security safeguards for sap cloud services: addressing the threats to cloud computing

Cloud services are quickly gaining popularity among businesses of all sorts, from startups to well-established multinationals, and corporate businesses are quickly embracing them as part of their digital transformation initiatives. Businesses can reap several benefits from using these platforms, such as reduced costs, improved operational efficiency, scalability, flexibility, and agility in business change. It is necessary for businesses to safeguard their vital information and assets by evaluating risks, threats, and migrating processes to the cloud. The Cloud Security Alliance (CSA) publishes a study called "Top Threats to Cloud Computing" once a year.

If your company uses or is thinking about using cloud computing, you should read the Pandemic Eleven study. A thorough analysis of the most pressing risks to cloud security is presented, along with suggestions for reducing such risks. In response to Cloud Security Alliance's "Top Threats to Cloud Computing Pandemic Eleven" report from June 2022, we take a look at the improved security features offered by SAP Cloud Services in this blog post.

3.1. SAP Holistic Approach to Cloud Security

Before we go into the security features offered by SAP cloud services to ward off the top cloud computing threats identified in the CSA Pandemic 11 report, let's take a brief look at SAP's all-encompassing cloud security strategy. When it comes to cloud security, SAP is quite serious. The problem has permeated all levels of the firm, from strategic planning to operational procedures. In order to ensure that its cloud services are secure from a wide range of attacks, SAP follows industry best practices and regularly tests its security measures.

SAP has a strong security posture because it has implemented multiple layers of protection and has a strategy that does not assume any inherent trust. That way, the business will be safe from any dangers that may arise. There are already established comprehensive strategies like zero-trust and defense-in-depth. The Cyber Fusion Centre (CFC) is SAP's all-encompassing plan for handling cyber threat intelligence, security operations, and incident response. This synergy facilitates preemptive measures, making it easier to safeguard critical technological and data resources. With the help of the Cyber Fusion Centre, SAP is prepared to deal with the ever-changing landscape of cybersecurity threats was shown in figure 3.

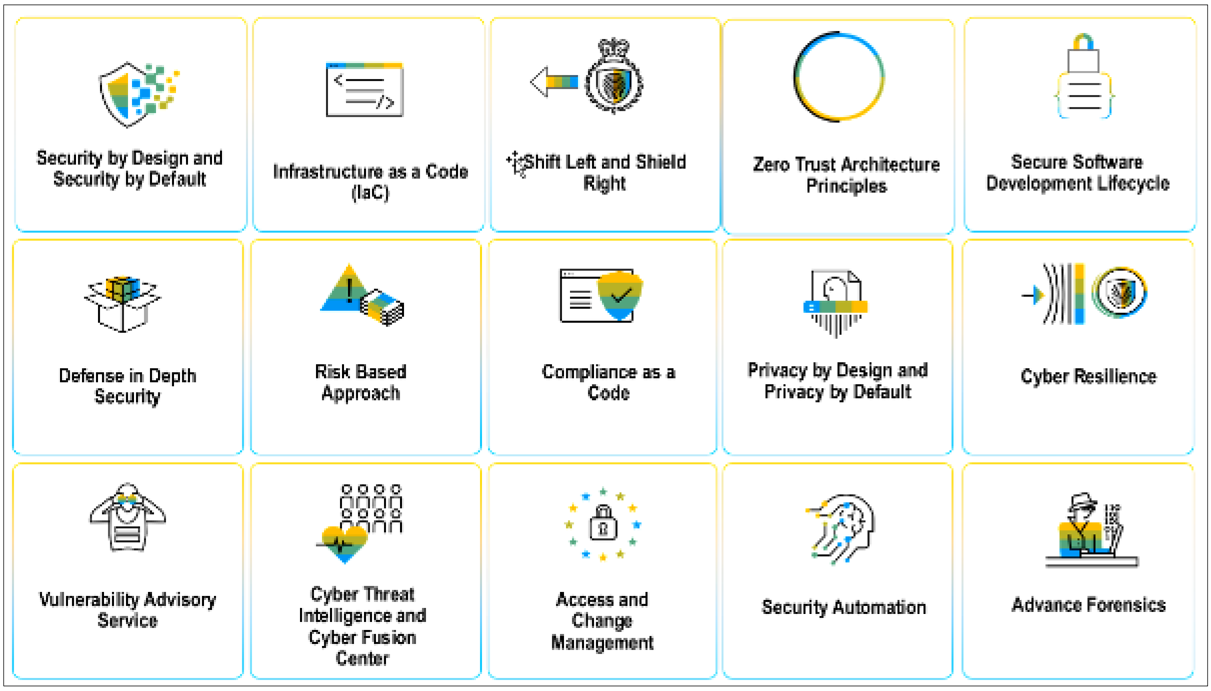
Security by Design and Security by Default
Infrastructure as a Code (IaC)
Shift Left and Shield Right
Zero Trust Architecture Principles
Secure Software Development Lifecycle
Defense in Depth Security
Risk Based Approach
Compliance as a Code
Privacy by Design and Privacy by Default
Cyber Resilience
Vulnerability Advisory Service
Cyber Threat Intelligence and Cyber Fusion Center
Access and Change Management
Security Automation
Advance Forensics

Figure 3 SAP's Comprehensive Strategy for Countering Cyber Threats

In order to find any cyber risks and come up with ways to reduce them, SAP performs comprehensive "Threat Modelling" exercises throughout the Secure Software Development Lifecycle (SSDLC).

"Shift left" and "shield right" refer to the practice of incorporating security testing and prevention into the development and deployment process at earlier stages. This helps find security concerns early on and prevent them from happening.

By anticipating and fixing possible security flaws before they escalate, SAP is able to make their software more resistant to cyber assaults. The zero-trust model, a strategy based on risk, and multiple layers of security are all part of these ideas. By firmly owning and securely managing the cloud accounts of hyperscale providers, SAP protects the environment and ensures that public cloud services are not vulnerable to security misconfigurations. This blog, along with several others by jay.thodenvanvelzen on the same subject, does a great job of explaining SAP's methods for managing cloud infrastructure.

4. Threats to cloud computing pandemic eleven

In order to develop robust security measures, organizations must first comprehend the risks associated with cloud computing. Automation, analytics, business intelligence, software development, integration, extensions, and business applications are just a few of the many uses for cloud computing. Although there are numerous advantages to migrating to the cloud, there are also many risks that must be carefully considered. Companies may protect their data and adhere to best practices in cybersecurity by learning about these threats and developing strategies to deal with them. The "Top Threats to Cloud Computing Pandemic Eleven" report from the Cloud Security Alliance (CSA) summarises the eleven most significant risks to cloud computing.

For businesses seeking to strengthen their cloud security measures, the CSA Pandemic Eleven report is an invaluable resource and was shown in figure 4. This research delves into the most recent cloud security risks and offers advice on how to deal with them. According to the Cloud Security Alliance, these eleven risks pose the greatest danger to cloud computing:

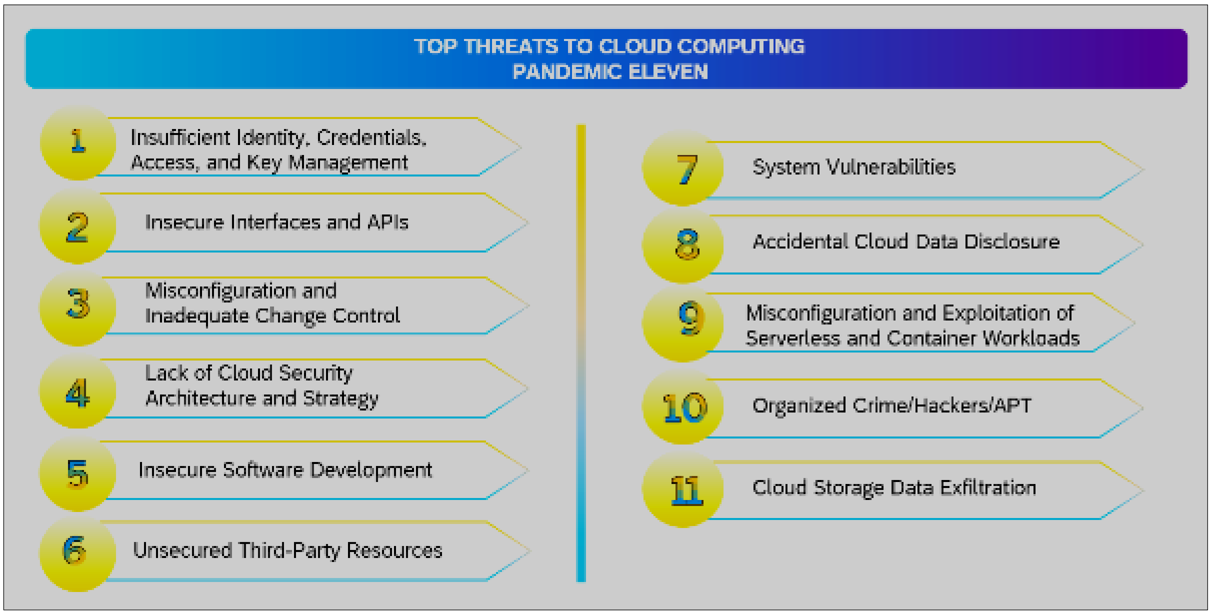
TOP THREATS TO CLOUD COMPUTING
PANDEMIC ELEVEN
1 Insufficient Identity, Credentials, Access, and Key Management
2 Insecure Interfaces and APIs
3 Misconfiguration and Inadequate Change Control
4 Lack of Cloud Security Architecture and Strategy
5 Insecure Software Development
6 Unsecured Third-Party Resources
7 System Vulnerabilities
8 Accidental Cloud Data Disclosure
9 Misconfiguration and Exploitation of Serverless and Container Workloads
10 Organized Crime/Hackers/APT
11 Cloud Storage Data Exfiltration

Figure 4 Pandemic Eleven Leading Dangers to Cloud Computing

4.1. Security Safeguards in SAP Cloud Services to Address Cloud Computing Threats

Several SAP cloud services provide security tools or services, which will be examined in the sections that follow. Customers or SAP's operational security might use these resources to lessen the impact of the typical cloud computing threats highlighted by Pandemic 11.

4.2. Threat 1: Insufficient Identity, Credentials, Access, and Key ManagementSecurity Safeguards Available with SAP Cloud Services:

To assist avoid this problem, identity access management, multi-factor authentication, and role-based access restriction should be put into place. Only authorised people should be able to access the data. This is where role-based access control (RBAC) comes in handy for managing various jobs.

The ability to securely keep encrypted customer data is essential, as is the ability to encrypt the data while it is in transit. Data breaches can be prevented by auditing every user activity and taking action when questionable conduct is detected. Integrating SAP Identity Provisioning Services (IPS) and SAP Identity Authentication Service (IAS) is standard practice for most SAP cloud products. All of these services are now part of SAP Cloud Identity Services, which is a standard feature in SAP BTP. The IAS can take on the role of an identity provider or serve as an intermediary to transfer authentication to a customer-owned identity provider platform (IDP) that is already integrated with an existing SSO system.

- Single Sign-On (SSO)
- Multi-factor Authentication (MFA)
- Identity Federation: SAML 2.0. Open ID, OAuth 2.0. Authentication can be delegated to Corporate IDP
- Social Sign-On: SAP IAS can be integrated with social network identities like Google, Facebook, and LinkedIn.
- User Self-Service: Users can manage their account data and password themselves.

Risk Based Authentication is another security feature available in SAP IAS was given in figure 5. Administrators have the power to construct authentication rules based on different risk indicators. These rules can subsequently be used to apply actions such as Allow, Deny, and Two-Factor Authentication. One of SAP's offerings is SAP Identity Access Governance (IAG), a cloud-based solution that runs on SAP BTP.

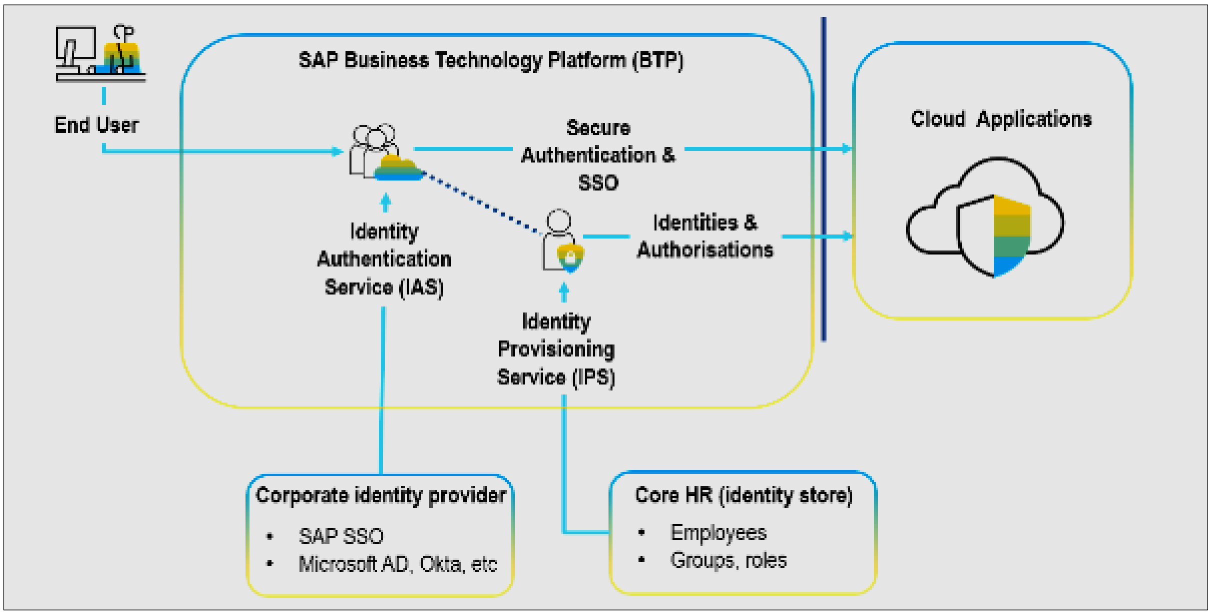
End User
SAP Business Technology Platform (BTP)
Secure Authentication & SSO
Identity Authentication Service (IAS)
Identities & Authorisations
Identity Provisioning Service (IPS)
Cloud Applications
Corporate identity provider
• SAP SSO
• Microsoft AD, Okta, etc
Core HR (identity store)
• Employees
• Groups, roles

Figure 5 SAP Cloud Identity Services

There is a vast array of features available with this service.

- By using access analysis, you can identify potential threats to vital access and segregation of tasks (SoD) and take steps to mitigate them.
- Establish and uphold business roles that are compliant with our Role Design Service.
- Business application and HR event-driven identity lifecycle self-service access request creation is the focus of the Access Request Service.
- Service for Verifying Access (assess and validate user access using auditable workflow).
- You can learn more about how people with special permissions are handling your company's data with the help of the Privileged Access Management Service, which keeps tabs on who has access to crucial and sensitive transactions.

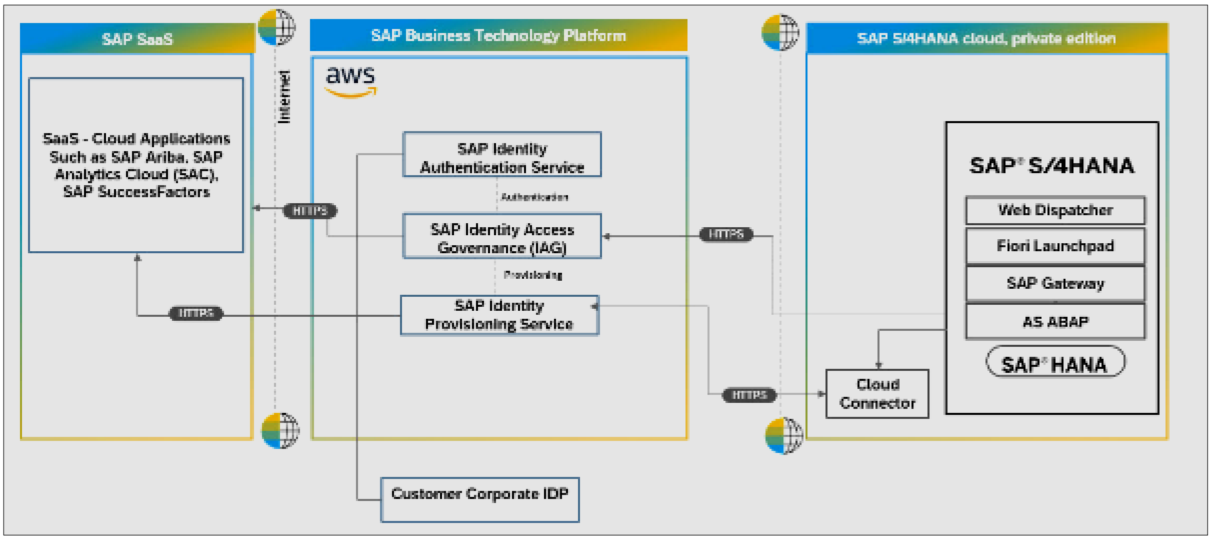
SAP SaaS
SaaS - Cloud Applications Such as SAP Ariba, SAP Analytics Cloud (SAC), SAP SuccessFactors
Internet
SAP Business Technology Platform
aws
SAP Identity Authentication Service
Authentication
SAP Identity Access Governance (IAG)
Provisioning
SAP Identity Provisioning Service
HTTPS
HTTPS
HTTPS
HTTPS
Customer Corporate IDP
SAP S/4HANA cloud, private edition
SAP S/4HANA
Web Dispatcher
Fiori Launchpad
SAP Gateway
AS ABAP
SAP HANA
Cloud Connector

Figure 6 SAP Cloud Identity Access Governance

4.3. Secure CCKMS/BYOK Key Management

Data held by SAP customers in the cloud is protected by strong encryption methods that are applied both during transmission and storage and was shown in figure 6. To further reduce the likelihood of illegal access to your data, SAP follows the Segregation of Duties (SoD) Principle by dividing up the tasks associated with managing encryption keys and data access. Customers have even more control over the security of their customer data with the help of BYOK/CCKMS, which is enabled by SAP Data Custodian Key Management Service (KMS). A small number of cloud solutions have this capability; these include SAP S/4HANA cloud, public edition and SAP S/4HANA cloud, private edition.

The "Bring Your Own Key" (BYOK) function gives users more agency by letting them use their own encryption keys. Further strengthening data security, this feature allows clients to maintain complete control over their encryption keys throughout their lifetime. Regarding the majority of their cloud services, SAP places a premium on preventing unauthorised access, modification, or theft of these encryption keys.

They maintain keys in a secure environment. Secure data centers are one example of physical security; secure key storage solutions and hardware security modules are examples of technological measures; and operational procedures such as frequent audits and restricted access protocols are examples of operational security. When it comes to safe key management in the cloud, SAP uses the segregation of duties principle to make sure no one person is in charge of everything.

5. Conclusion

The risk associated with cloud computing can be reduced in an easy and cost-effective manner. The security risks associated with any technology can be reduced to a minimum by the implementation of appropriate education and training programs, as well as an efficient risk mitigation strategy. It is possible for network administrators to considerably improve the incident reaction time and ensure the safety of the majority of cloud databases provided they develop and maintain a proactive knowledge with network activity. When it comes to these procedures, the development of security intelligence technologies can only be helpful if they are the sole supplement; they cannot take the place of monitoring and personal attention.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan et al., “Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records,” IEEE Access, vol. 8, no. 8, pp. 157959– 157973, 2020.

[2] D. Owens, “Securing elasticity in the cloud,” Communications of the ACM, vol. 53, no. 6, pp. 46–51, 2010.

[3] W. Y. Chang, H. A. Amara and J. F. Sanford, “Transforming enterprise cloud services,” Springer, 2010. [Online]. Available: https://www.springer.com/gp/book/9789048198450. Last Visit Nov 17, 2020.

[4] M. T. J. Ansari and D. Pandey, “Risks, security, and privacy for HIV/AIDS data: Big data perspective,” Big Data Analytics in HIV/AIDS Research, IGI Global, vol. 5, no. 6, pp. 117–139, 2018.

[5] M. Bilal, L. O. Oyedele, J. Qadir, K. Munir, S. O. Ajayi et al., “Big data in the construction industry: A review of present status, opportunities, and future trends,” Advanced Engineering Informatics, vol. 30, no. 3, pp. 500–521, 2016.

[6] K. Jamsa, “Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more,” Jones & Bartlett Publishers, 2012. [Online]. Available: https://books.google.co.in/books/about/Cloud_Computing.html? id=msFk8DPZ7noC&redir_esc=y. Last Visit Nov 17, 2020.

[7] M. T. J. Ansari and D. Pandey, “An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation,” International Journal of Advanced Research in Computer Science, vol. 8, no. 3, pp. 15–23, 2017.

[8] M. Almorsy, J. Grundy and I. Müller, “An analysis of the cloud computing security problem.” arXiv preprint arXiv: 1609.01107, 2016.

[9] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications, vol. 79, no. 5, pp. 88–115, 2017.

[10] R. Kalaiprasath, R. Elankaviand and D. R. Udayakumar, "Cloud security and compliance-A semantic approach in end to end security," International Journal of Mechanical Engineering and Technology, vol. 8, no. 5, pp. 987– 994, 2017.

[11] C. A. Ardagna, R. Asal, E. Damiani and Q. H. Vu, "From security to assurance in the cloud: A survey," ACM Computing Surveys, vol. 48, no. 1, pp. 1–50, 2015.

[12] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan et al., "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," Journal of Network and Computer Applications, vol. 74, no. 5, pp. 98–120, 2016.

[13] L. Coppolino, S. D'Antonio, G. Mazzeo and L. Romano, "Cloud security: Emerging threats and current solutions," Computers & Electrical Engineering, vol. 59, no. 6, pp. 126–140, 2017.

[14] H. Tabrizchi and Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," Journal of Supercomputing, vol. 5, no. 6, pp. 1–40, 2020.

[15] Patel, V. A framework for secure and decentralized sharing of medical imaging data. Health Inform. J. 2019, 25, 1398–1411.

[16] Park, S.-J.; Lee, Y.-J.; Park, W.-H. Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network. Commun. Secur. Soc.-Oriented Cyber Spaces 2021, 2021, 3686423.

[17] Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)

[18] R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama.

[19] GPB GRADXS, N RAO, Behaviour Based Credit Card Fraud Detection Design And Analysis By Using Deep Stacked Autoencoder Based Harris Grey Wolf (Hgw) Method, Scandinavian Journal of Information Systems 35 (1), 1-8.

[20] R Pulimamidi, GP Buddha, Applications of Artificial Intelligence Based Technologies in The Healthcare Industry, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4513-4519.

[21] R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.

[22] GP Buddha, SP Kumar, CMR Reddy, Electronic system for authorization and use of cross-linked resource instruments, US Patent App. 17/203,879.

[23] Nadella, G. S. (2023). Validating the Overall Impact of IS on Educators in U.S. High Schools Using IS-Impact Model – A Quantitative PLS-SEM Approach, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, ISBN 9798381388480, 189, 2023.

[24] Gonaygunta, Hari, Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, United States, ISBN 9798381387865, 142, 2023.

[25] Hari Gonaygunta (2023) Machine Learning Algorithms for Detection of Cyber Threats using Logistic Regression, 10.47893/ijssan.2023.1229.

[26] Hari Gonaygunta, Pawankumar Sharma, (2021) Role of AI in product management automation and effectiveness, https://doi.org/10.2139/ssrn.4637857.

[27] Sri Charan Yarlagadda, Role of Artificial Intelligence, Automation, and Machine Learning in Sustainable Plastics Packaging markets: Progress, Trends, and Directions, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 818–828, 2023.

[28] Sri Charan Yarlagadda, The Use of Artificial Intelligence and Machine Learning in Creating a Roadmap Towards a Circular Economy for Plastics, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 829-836, 2023.

[29] B. Nagaraj, A. Kalaivani, S. B. R, S. Akila, H. K. Sachdev, and S. K. N, "The Emerging Role of Artificial intelligence in STEM Higher Education: A Critical review," International Research Journal of Multidisciplinary Technovation, pp. 1–19, Aug. 2023, doi: 10.54392/irjmt2351.

[30] D. Sivabalaselvamani, K. Nanthini, Bharath Kumar Nagaraj, K. H. Gokul Kannan, K. Hariharan, M. Mallingeshwaran, Healthcare Monitoring and Analysis Using ThingSpeak IoT Platform: Capturing and Analyzing Sensor Data for Enhanced Patient Care, IGI Global eEditorial Discovery, Pages: 25, 2024. DOI: 10.4018/979-8-3693-1694-8.ch008.

[31] Amol Kulkarni, Amazon Athena Serverless Architecture and Troubleshooting, International Journal of Computer Trends and Technology, Vol, 71, issue, 5, pages 57-61, 2023.

[32] Amazon Redshift Performance Tuning and Optimization,International Journal of Computer Trends and Technology, vol, 71, issue, 2, pages, 40-44, 2023.