**Cloud Computing Security and Privacy Issues**

**Name- Ramandeep Bura**

**Student ID- S20241661**

**Unit Code & Name- (ICT501) Foundation of IT**

**Instructor’s Name- Neda Azizi**

**Introduction**

The cloud computing has revolutionized the way organizations have been managing information and data by providing more efficient and elastic models. Outsourcing of business processes makes organizations to reduce expenses on equipment and software, enhance integration and accessibility of resources. However, this movement suggests pretty huge security and privacy concerns, which has to be fixed to meet new data security and regulatory demands. The cloud structure is especially dangerous since data is located on servers in other regions and is copied to the Internet. These are; Data protection, Data access, Data identification and Data breaches.

More explicitly, the hybrid risks model associated to shared responsibility model of cloud computing mean that specifically CSPs and customers must work together to protect the cloud environment. Thus, CSPs are expected to manage and safeguard infrastructure and ensure that they offer reliable security measures; it is the customer who has to do the same for the data and the application. Privacy concerns are also paramount important as clouds mostly involve transfer and storage of data belonging to an individual or an Organization. Ensuring data protection laws as discussed under GDPR or HIPAA are observed is very crucial. It is crucial that all companies proactively follow these regulations when it comes to cloud practices in order to avoid penalties as well as negatively impacting their reputation with customers (M. Armbrust et al., 2009). This shows that there is requirement of good and specific measures to be taken when using cloud services to enhance the security of the services being used while at the same time ensuring all service comply with the set standards.

**Technological Analysis**

**Chosen Technology: Data Encryption in Cloud Computing:**

**Relevance to Modern Industry:-**

Data encryption has become quite a phenomenon for fulfilling the need of information security requirements in the sphere of cloud computing. As the use of the cloud system increases, most of the significant data, as well as business-critical applications are stored in the cloud system. It is paramount to protect such data from external influences and risks. In relation to these problems, it is crucial to ensure that data encryption becomes a core requirement especially for the organizations which deal with the transmission of highly sensitive data as seen with the finance sectors, healthcare department, any e-commerce sectors in compliance and data security.

**Key Features and Capabilities:**

1. In-Transit Encryption:

* TLS/SSL Protocols: Encrypts the connectivity between the client machines and the cloud servers thus safeguarding the data in the process. This alert means that there is no eavesdropping or man-in-the-middle attack taking place.
* VPN Integration: Connects private network to a public network while seamlessly providing the confidentiality to the data being transferred through the two networks.

1. At-Rest Encryption:

* AES Encryption: AES is fast and secure because of the way it works, thus it is commonly used. It encrypts data that is stored on cloud servers, such that, even if the physical security aspect has been penetrated, data cannot be retrieved.
* Key Management Services (KMS): Safely generates, stores, and manages access keys, so that encryption keys are protected and used improperly.

1. Full Disk Encryption (FDE):

* Device-Level Security: Encrypts all data on cloud storage device, no need re-configure file format or databases for maximum security protection.

.

**Comparison with Alternative Technologies:**

Tokenization:

* Pros: As a result, a substitute sensitive value with non-sensitive substitutes that can be utilized in systems to avoid exposure of the actual data. Higher order security useful for payment card data and identification information.
* Cons: Once again tokens need to be correlated with the source data and thus the concept of Token vault needs to be safe and efficient. A weaker application as compared to encryption to control the flexible complexity data process and analysis.

Access Controls (IAM):

* Pros: Ensures that only the user that is permissible by the filters that have been set in the D-acct can access the data and or resources that have been protected. Incorporates efficient security measures which include the role-based or attribute-based access control.
* Cons: Does not safeguard data; concerns itself with who would be able to view information rather than determining who is able to intercept data in motion or information at rest.

Data Masking:

* Pros: This tool camouflages important data to any person who is not allowed to access such information while making it retrievable by the authorized testers and developers. Effective for non-production environments.
* Cons: Does not offer premeded protection infrastructure as encryption does in safeguarding data in production systems. Despite the use of the mask, the contents of the signal can become known at some point in time.

**Recent Developments and Trends**

**Technological Advancements:**

1. Zero Trust Security Model:

* Concept: The main concept behind from this is “Hype, trust but always authenticate”. To this hype, sits the reality meaning threats may be in and out of the network heightening the need for authenticating each person or device seeking access to resources.
* Advancements: This paper establishes that permanent protection, micro-segmentation, and continued monitoring are the best practices. Presently it is employed by vendors like Microsoft Company and Google using the Zero Trust frameworks.

1. Confidential Computing:

* Concept: here concept is Safeguards information in active employ by storing it in data resulting from computation within an SE, which in turn is an abstract concept designating a secure processing environment at the hardware level.
* Advancements: The prominent manufacturers in this case are Intel, AMD, and ARM, which are developing security processors that incorporate TEEs. Since the beginning of this year, major cloud service vendors such as Microsoft Azure and Google Cloud services have begun integrating confidential computing.

1. AI and Machine Learning for Security:

* Concept: AI and ML as a means to identify anomalous behaviours of the system, threat assessment and preventive auto control actions.
* Advancements: In this case, there is an enhancement of the threat intelligence and a real analysis of the threats. The sophisticated solutions that can be purchased at such providers as Darktrace and CrowdStrike are already witnessing the growing interest because they provide real-time and smart approaches to security (Xiao, L et al., 2018).

**Market trends:**

1. Increased range of Adoption of Multi-Cloud Strategies:

* Trend: Enterprises today are using more than one cloud service from multiple service providers to avoid being locked-in to one vendor, to reduce the cost and to have business continuity for a longer time.
* Impact: Desiring high level of security systems that can operate in various clouds. Some players like HashiCorp, VMware are already trying to solve the multi-cloud security problem and they solve to some extent.

1. Development in Cloud-Native Security Solutions:

* Trend: This means that cloud-native security is becoming important since organizations are developing and launching new solutions in the cloud directly.
* Impact: This is achieved by improving on the aspects of container security, Kubernetes security, and serverless security. Firms like Aqua Security and Sysdig are examples of companies that are presently aiming at these modern cloud arrangements.

1. Regulatory Compliance and Data Sovereignty:

* Trend: This is because governments threaten to intensify and change the data protection laws (e. g. and instrumental laws forcing organizations to store data within the geographical location of the country like in same country.
* Impact: Compliance related services are being created and data locality solutions have been offered. To these regulations’ necessities, solutions are offered by means such as: Microsoft Azure data residency in the EU.

**Consumer Preferences:**

1. Prioritization of Data Privacy:

* Preference: The contemporary customers are even more conscious about their rights and information they share with a particular company basically they don’t want share any extra info.
* Impact: Firms are applying privacy protection technologies, organizational privacy solutions. There is an increase in the demand for data protection services where the consumers require guarantee that security measures and policies are reliable and less ambiguous.

1. User friendly security solutions:

* Preference: There is always the desire for simplified security solutions in terms of deployment and management to the provision of these solutions, without compromising on the degree of security (Wang, C., et al., 2012)
* Impact: Computerized security solutions wherein the plain paper is used and the components are integrated are pretty common now. When it comes to this requirement of having a central control of security management, there are tools available and these are AWS Security Hub and Google Cloud Security Command Center.

**Opportunities and Challenges:**

1. Improved data protection and privacy:

* Opportunity: The use and implementation of the encrypted solution for data protection have set their focus into achievement of protection against data leakage and unlawful access by aligning with higher standards of regulations such as GDPR, HIPAA & CCPA.
* Business Solutions: Today, the service providers are still able to provide the encryption services together with the compliance solutions that shall address the legal requirements. Among these services some can help the doctor in the activity of organizing the records of the patient in a secure manner.

1. Scalability and Flexibility:

* Opportunity: IT accumulation helps organizations to lease facilities by means of the IT accumulations, generously depending on the necessities of the demand and storage improvement.
* Business Solutions: Cloud services can also be of great help to the company where in the company is able to introduce new applications or even services faster because the capital investment in IT framework is not all that is required here. In this respect, it can be stated that, new products can be introduced in the market very conveniently and can be accepted in the market most effectively.

1. Cost Efficiency:

* Opportunity: Outsourcing with a cloud provider discourages the organizations from investing more on fixed asset like hardware and software rather, they opt for operating expenses.
* Business Solutions: From the name, one can make the observation that business organizations gets a boost in the aspect of cost management in which they only make expenditures which are strictly required in the provision of the IT services. For example, it allows young enterprises and SMBs to enter the sectors with new technologies in a comparatively less dangerous process.

**Challenges:**

* Security: One of the main risks in cloud is security. In today’s era, cloud is easy target for hackers like for data breach, cyberattack (Dillon, et al., 2010).
* Confusion in legal rules: This one is also the main challenge in cloud because different country have different rule which is headache for organization.
* Vendor lock-in: Sometime rely on one vendor also create problems because some time they stuck in flexibility and when it comes to pricing they can’t bargaining.
* Data privacy: This one is also the major issue for cloud organization when they store personal and sensitive data in their databases raises concerns for individuals (Kshetri, N. 2013).
* Performance and system down: Some time cloud services faces downtime which affects the overall performance for the user.

**Ethical, Privacy and Governance Concerns:**

**Ethical Considerations:**

* Bias and Fairness: Can it give more preference to the certain group of people while discriminating the others? For instance, about facial recognition software, they can be racially biased. How can it be put in a way that will not discriminate the members of the society and the less privileged?
* Transparency and Explainability: Is it understandable for a user to grasp the logic behind a particular choice a cutting-edge technology makes? These algorithms create doubts regarding equality and responsibility, and clearly understandable ones are not always possible, so the use of opaque algorithms has drawbacks (Pearson, S. 2013).
* Human Control: Is such system beholden to the people, or will it go fully independent at some point? How do we define that degree and how can we make sure that human intervention will still be a focus?

**Privacy Concerns:**

* Data Collection and Use: There are some considerations that we need to answer like, What kind of data the technology will be able to access and how will it process the information. Some issues often raised include whether the user privacy will be protected and whether the user has the power of decision concerning the information about them (Dawson 2002).

* Data Security: As for how the collected data is to be protected, this will of course depend on the nature of the data collected as well as the particulars of the industry in which the database is to be applied (Takabi et al., 2010).

* Surveillance and Monitoring: Was the objective of the technology to act as spy or monitor the individuals or some organizations? The following are the ways through which one can ensure that adequate measures that will protect the rights to privacy are observed.

**Governance Concerns:**

* Regulation and Oversight: Can the existing laws protect against the apros and conherent risks with reference to the given technology? In institutions, business, or any organizations, is there any aspect in governance that is missing so that it could fit into a gap?

* Accountability and Liability: Thus, the following questions arise: It is appropriate to ask: Who therefore is to blame for the operation and the decision-making process implicate that the technology presupposes?

* Access and Equity: Who can have access to this technology and what we have to do for all the stakeholders to be able to get access to this new technology?

**Recommendations and Best Practices:**

**Recommendations:**

1. Encryption: Encrypt the data which is not being used or only being used temporarily and also the flow of the information through the channels. Encryption procedures should be performed with a high level of security and each key to the encryption methods should be protected (Xing Zhou, Xiaofei Tang 2011).

1. Access Controls: Thereby, the least privilege security model should be established. Make sure that restricted or limited access or permission level, or simply privilege level, contrived for a user corresponds to the job description or function the user is assigned to. This should be done to introduce a new level of security for the multi user environment through the process of Multi factor authentication.

1. Continuous Monitoring: This may include employing of security tools in the monitoring of the cloud activities in the lookout for any ab behaviors as well as security audits at regular intervals in order to assess the vulnerability points.

**Privacy Considerations:**

1. Data Minimization: But the single condition to be met here is that collected data should only encompass the data that would be of value to your business. This also means that all the other unjustified data collection procedures also need to be halted.

1. Data Governance: More effort should be directed into writing good policy regarding some of the following aspects that should clearly define how data should be managed, who can have access to information and the duration in which the data should be retained. This solution should also consider the guidelines in data privacy, among which are the GDPR and CCPA (Wang, C 2010).

1. User Transparency: In this case, the users should be informed in details how their personal data is being collected, used and processed for sharing. It is crucial to have clear policy concerning the use of the details that is personal and to ensure that the people who are under observation or who are being undertook in terms of data collection (Subashini, S., & Kavitha, V. 2011).

**Additional Best Practices:**

1. Employee Training: Promote and require the employees in the organisation to undergo training every calendar year for elevation of cybersecurity measures in addition to security consciousness concerning information protection and phishing (Halton, W. M., & Rahman, S. 2012).

1. Incident Response Plan: An agenda of the following process, which must be implemented in case of security breeches and data leaks, is also effective.

1. Multi-Cloud Strategy: In so far as is possible, multiple cloud systems should not be procured from the same vendor to prevent a single company having direct control over the information you entrust to it, and your security arrangements (Achar, S. 2022).

**References and Documentation**

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, et al., "Above the clouds: A Berkeley view of cloud computing" in , EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.
2. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.
3. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220-232. <https://doi.org/10.1109/TSC.2011.24>
4. Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications (pp. 27-33). IEEE. <https://doi.org/10.1109/AINA.2010.187\>
5. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386. <https://doi.org/10.1016/j.telpol.2012.04.011>
6. Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer, London. <https://doi.org/10.1007/978-1-4471-4186-7_1>
7. Dawson 2002, Maximizing sharing of protected information, vol.64-No.3, Journal of Computer and System Sciences.
8. Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31. <https://doi.org/10.1109/MSP.2010.186>
9. Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.
10. Wang, C., Wang, Q., Ren, K., Lou, W., & Li, J. (2010). Toward publicly auditable secure cloud data storage services. IEEE Network, 24(4), 19-24. <https://doi.org/10.1109/MNET.2010.5510914>
11. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. <https://doi.org/10.1016/j.jnca.2010.07.006>
12. Halton, W. M., & Rahman, S. (2012). The top ten cloud-security practices in next-generation networking. International Journal of Communication Networks and Distributed Systems, 8(1-2), 70-84.
13. Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering, 16(9), 379-384.