**Cloud Computing and Enhanced Security Protocols**

**Team members:**

**Noor Elghouti 225379**

**Shahd Mohamad 225393**

**Reem Ramadan 224683**

**Mariam Hamdy 224085**

**Abstract**

This abstract examines how security and cloud computing interact, discussing the difficulties and solutions associated with protecting infrastructure and data in cloud settings. The article highlights the essential requirements for strong security measures while outlining the main traits and deployment models of cloud computing. The abstract explores common security problems like identity management, network security, and encryption as crucial remedies for problems like data breaches and compliance problems O. Rebollo et al (2015). It also covers new developments like AI-driven threat detection and the significance of risk management frameworks. In the end, it emphasizes how teamwork is necessary to strengthen cloud security and guarantee a robustbecosystem.   
  
**Introduction**

Information technology has evolved, and cloud computing is now a popular business model for providing IT resources. Individuals and businesses can obtain on-demand network access to a shared pool of managed and scalable IT resources, including servers, storage, and apps, through cloud computing. Lately, cloud computing has received a lot of attention from both practitioners and academic Ahmed M, Litchfield AT (2018). In our daily lives, we use cloud services extensively for things like data storage, document writing, business management, and online gaming. In addition, cloud computing offers the infrastructure that has enabled major digital trends like big data, artificial intelligence, mobile computing, and the Internet of Things, which has accelerated industry dynamics, upended preexisting business models, and fueled the digital transformation. Cloud Computing Architecture (2019). On a pay-per-use basis, cloud users can access various services and/or resources from any location at any time. As a result, a lot of businesses, organizations, and individual users are switching to cloud computing and exchanging massive amounts of data there. But the largest obstacle to cloud computing's widespread adoption is security concerns. Infrastructure, data and storage, and access control in cloud environments are among the areas where security concerns are present. Even though there are already a lot of surveys about cloud security, there is still a gap in how these problems are properly mapped to the solutions that address them Z Kazi (2017). One survey addresses access control mechanism, while others focus on virtualization problems and solutions. However, there is a lack of a unified framework that would both broadly define cloud security and thoroughly examine its needs. This paper examines the importance of cloud security, the idea of how cloud security works and provides a brief overview of security risks. There is also discussion of the various ways to prevent or lessen security problems in cloud environments.

**Research Question:** How can cloud security evolve to protect data integrity, confidentiality, and accessibility amidst evolving threats?

**Review of Literature**

1. **Mechanisms and Strategies of Cloud Security**

Every cloud security measure works to accomplish one or more of the following: enable data recovery in case of data loss and Protect storage and networks against malicious data theft. First data backup and disaster recovery in the cloud are of paramount importance for Data Protection and Availability: Data is a critical asset for businesses, and its loss or unavailability can have severe consequences. Cloud backup ensures that data is securely stored off-site, protecting it from physical damage, theft, or on-premises disasters. In the event of data loss, cloud-based disaster recovery enables organizations to quickly restore data and resume operations, minimizing downtime and maintaining business continuity Mitigation of Risks: Organizations face various risks, including hardware failures, cyber-attacks, human errors, and natural disasters. Cloud backup and disaster recovery provide a safety net against these risks. By regularly backing up data to the cloud, organizations reduce the risk of permanent data loss and can recover quickly in the face of unexpected events Scalability and Flexibility: Cloud-based solutions offer scalability and flexibility, allowing organizations to easily adjust their backup and recovery capabilities according to their evolving needs. Cloud service providers can accommodate increased data volumes and provide storage resources on-demand, ensuring that backups are comprehensive and that recovery processes can handle growing data requirements Geographic Redundancy: Cloud service providers typically operate data centers in multiple geographic locations, ensuring redundancy and data replication. This geographic redundancy enhances data availability and resilience, as backups are stored in multiple locations, reducing the risk of data loss due to localized disasters or outages. Automated Backups: Cloud backup solutions often offer automated backup processes. Organizations can set up scheduled backups, ensuring that data is regularly and consistently backed up without manual intervention. This automation reduces the risk of human error and ensures that critical data is always protected. There are many types of cloud backup full back up: A full backup involves creating a complete copy of all data and files in the organization's environment. This initial backup captures all data, including files, databases, applications, and system configurations. Subsequent backup operations focus on capturing changes or updates made since the last full backup. Full backups provide comprehensive data protection but can be time-consuming and require significant storage resources. Second, SECURING CLOUD WITH FOG Cloud computing is a technique which provides services to clients over the network; user can use any type of services (SaaS, PaaS, IaaS). Cloud storage is the model of network enterprise storage where huge amounts of data are stored. Cloud computing provides storage space services for the users, user can store his data and information in the cloud, and he can access to information as store it forms any computer connected to the internet. The main thing is that the user doesn’t know where and how data is stored. And who can see the data? The problem of user when he stores sensitive information in the cloud the user requires security of the cloud computing to assurance nobody can right to use and view his data and business-related information that his store in cloud, to avoid this problem used encryption method. But encryption method unsuccessful in preventing data theft attacks. By applying encryption technique to the information, we can’t realize total protection to confidential data. In Existing system as per the Literature survey done it is observed that decoy file creation is done whenever new file is being upload to the cloud was suggested but, in such case, require huge amount of storage space in the cloud. A. Disadvantages: It’s not identified when the attack is happening, it’s very complex to identify which user is attack and we can’t detect the file which was hacked.

**2. Importance of Cyber security**

Cloud security is an essential aspect of modern business operations, encompassing various measures to safeguard cloud-based infrastructure, applications, and data. With the increasing adoption of cloud computing, organizations are recognizing the importance of maintaining a robust security posture to protect against potential threats and ensure regulatory compliance. The benefits of cloud computing, such as lower upfront costs, reduced operational expenses, scalability, and enhanced flexibility, are driving its widespread adoption. However, concerns about security, governance, and compliance persist among IT professionals, especially regarding the protection of sensitive business information and intellectual property. Cloud security addresses these concerns by providing measures to guard against security breaches, manage remote work environments securely, ensure disaster recovery preparedness, comply with data protection regulations, and eliminate weak links in access control. For instance, cloud security systems enforce strict access controls to prevent unauthorized access to sensitive data and mitigate the risk of data leaks. Compliance with regulations like HIPAA and GDPR is essential for maintaining the integrity of business operations and protecting customer data. Moreover, cloud security plays a crucial role in enabling organizations to leverage the benefits of cloud computing fully. It supports next-level customer service, remote working capabilities, and fast scalability, while mitigating risks associated with misconfiguration and cyber threats. In today's digital landscape, where the threat of cyber-attacks is ever-present, ensuring the security of cloud environments is paramount. By implementing robust cloud security measures, organizations can protect their digital assets, maintain customer trust, and avoid potential financial losses resulting from avoidable breaches. Cloud security is an evolving field that constantly adapts to emerging threats and technological advancements. As organizations increasingly rely on cloud-based solutions for their operations, the need for robust security measures becomes even more critical. One of the key challenges in cloud security is the shared responsibility model, where both the cloud service provider and the customer are responsible for different aspects of security. While cloud providers offer security measures at the infrastructure level, customers are responsible for securing their data and applications within the cloud environment. This necessitates a comprehensive understanding of security best practices and the implementation of appropriate controls to mitigate risks effectively. Furthermore, the dynamic nature of cloud environments, characterized by frequent changes in infrastructure and configurations, introduces additional complexities for security management. Continuous monitoring and automation are essential to detect and respond to security threats promptly. Collaboration between IT professionals, security experts, and cloud service providers is crucial for developing effective cloud security strategies. By staying informed about the latest security trends and leveraging advanced technologies such as artificial intelligence and machine learning, organizations can enhance their defense mechanisms against evolving cyber threats.

**3. Cloud Computing Risks**

Therefore, the types of Cloud Security Risks are a lot and here are some of them. First, Data Breaches, One of the most significant concerns in cloud computing is the risk of unauthorized access to sensitive data (Alomari & Jie, 2021). Data breaches can occur due to misconfigured security settings, insider threats, or sophisticated cyber-attacks targeting cloud infrastructure or applications. In addition, Compliance and Regulatory Violations: Organizations operating in regulated industries must adhere to strict compliance requirements regarding data privacy, such as GDPR, HIPAA, or PCI DSS (Goyal et al., 2020). Failure to comply with these regulations can result in legal penalties, fines, or reputational damage. Also, Denial of Service (DoS) Attacks: Cloud-based services are susceptible to DoS attacks, where malicious actors overwhelm the system with a flood of requests, causing service disruptions and downtime (Aljawarneh, 2020). These attacks can impact the availability of critical resources and disrupt business operations. Account Hijacking: Weak authentication mechanisms or compromised credentials can lead to unauthorized access to user accounts or administrative privileges (Goyal et al., 2020). Account hijacking can result in data theft, unauthorized modifications, or unauthorized use of cloud resources. The consequences of cloud security risks can be far-reaching and detrimental to organizations, affecting their reputation, financial stability, and regulatory compliance. Some potential implications include financial Losses: Data breaches or service disruptions can incur significant financial losses due to remediation costs, legal fees, regulatory fines, and loss of revenue (Goyal et al., 2020). Reputational Damage: Publicized security incidents can tarnish an organization's reputation and erode customer trust, leading to customer churn and diminished market competitiveness (Aljawarneh, 2020). Cloud computing offers unprecedented opportunities for organizations to innovate, scale, and optimize their operations (Aljawarneh, 2020). However, the adoption of cloud services comes with inherent security risks that must be addressed to ensure the confidentiality, integrity, and availability of data and applications. By understanding the various types of cloud security risks, their implications, and effective mitigation strategies, organizations can strengthen their security posture and navigate the cloud landscape with confidence. Ultimately, proactive risk management and continuous vigilance are essential to safeguarding sensitive assets and maintaining trust in the cloud environment.

Problems and Solutions: This section identifies common challenges in cloud computing, such as data security and privacy, performance issues, password security, and lack of expertise. It proposes solutions to mitigate these challenges, including software updates, network configuration, cyber security solutions, real-time monitoring, password management, multi-factor authentication, and employee training programs.

**Problems & Solutions**

|  |  |  |
| --- | --- | --- |
|  | Problem | Solution |
| Data security and privacy | When working with Cloud environments, data security is a major concern as users have to take responsibility for their data, and not all Cloud providers can assure 100% data privacy. No identity access management, lack of visibility and control tools, data misuse, and cloud misconfiguration are the common reasons behind cloud privacy leaks. There are also concerns about malicious insiders, insecure APIs, and neglect or oversights in cloud data management. | Install and implement the latest software updates, as well as configure network hardware to prevent security vulnerabilities. Using antivirus and firewalls, increasing bandwidth for Cloud data availability, and [implementing cyber security solutions](https://sprinto.com/blog/cyber-security-compliance/) are some ways to prevent data security risks. |
| Performance challenges | The performance and security of [cloud computing solutions](https://sprinto.com/blog/cloud-compliance-guide/) depend on the vendors, and keep in mind that if a Cloud vendor goes down, you may lose your data too. | Cloud Service Providers should have real-time SaaS monitoring policies.  (SaaS monitoring helps ensure a seamless user experience by offering real-time data directly from the user's browser, improving visibility, awareness, and the ability to troubleshoot issues without relying on a service provider's help desk.) |
| Password security | Account managers manage all their cloud accounts using the same passwords. Password management poses a critical problem, and it is often found that users resort to using weak and reused passwords. | Secure all your accounts by using a strong password management solution. To further improve security, in addition to a password manager, use Multifactor Authentication (MFA). Cloud-based password managers should alert users of security risks and leaks.  (Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint.) |
| Lack of expertise | Cloud computing is a highly competitive field, and there are many professionals who lack the required knowledge and skills to be employed in the industry. There is also a huge gap in supply and demand for certified individuals and many job vacancies. | Companies should help existing IT staff in up skilling their careers and skills by investing in Cloud training programs. |

**Model 1:**

Model name: CERTAN

Dataset name: Network Traffic Android Malware

Comparison of the metrics between the Network Traffic Android Malware dataset and the other dataset.

|  |  |  |
| --- | --- | --- |
| Metric | Other Model | Our Model (Overall) |
| Accuracy | 98.09% | 81.77% (Test Data) |
| Balanced Accuracy | 97.72% |  |
| Precision | 99.34% |  |
| Recall | 95.87% |  |
| F1 Score | 97.58% |  |
| Macro Avg. Precision |  | 83% |
| Macro Avg. Recall |  | 79% |
| Macro Avg. F1 Score |  | 80% |
| Weighted Avg. Precision |  | 82% |
| Weighted Avg. Recall |  | 82% |
| Weighted Avg. F1 Score |  | 81% |

**Analysis**

1. Accuracy: The other model has a significantly higher accuracy (98.09%) compared to our model (81.77% on test data).
2. Precision: The other model's precision (99.34%), our model (not provided).
3. Recall: The other model's recall (95.87%), our model (not provided).
4. F1 Score: The other model has a higher F1 score (97.58%), our model (not provided).
5. Macro Avg. Precision, Recall, and F1 Score: These metrics are provided only for our model. They represent the average precision, recall, and F1 score across all classes without considering class imbalance. Our model achieves an average precision of 83%, average recall of 79%, and average F1 score of 80%.
6. Weighted Avg. Precision, Recall, and F1 Score: Similar to macro averages, these metrics are also provided only for our model. They represent the weighted average of precision, recall, and F1 score across all classes, considering class imbalance. Our model achieves a weighted average precision of 82%, weighted average recall of 82%, and weighted average F1 score of 81%.

**Which model is better?**

The other model is clearly the better-performing model across almost all metrics. Its higher accuracy, precision, recall, and F1 score suggest that it is more effective at correctly classifying the data.

**Model 2:**

Model name: Naïve Bayes

Dataset name: Network Traffic Android Malware

Comparison of the metrics between the Network Traffic Android Malware dataset and the other dataset.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Metric | |  | | --- | | **Our Model** |  |  | | --- | |  | | | **Second Model** | | --- |  |  | | --- | |  | |
| Accuracy | |  | | --- | | 0.43 | | 0.68 |
| Precision | 0.64 (Weighted Avg.) | 0.78 |
| Recall | |  | | --- | | 0.43 (Weighted Avg.) |  |  | | --- | |  | | 0.30 |
| |  | | --- | | **F1 Score** |  |  | | --- | |  | | |  | | --- | | 0.30 (Weighted Avg.) |  |  | | --- | |  | | 0.43 |
| |  | | --- | | **ROC AUC Score** | | N/A | 0.67 |

**Analysis**

1. Accuracy: The second model (0.68) is better than the Naive Bayes model (0.43).
2. Precision: The second model (0.78) has better precision compared to the Naive Bayes model's weighted average precision (0.64).
3. Recall: The Naive Bayes model has a higher weighted average recall (0.43) than the second model (0.30).
4. F1 Score: The second model (0.43) has a better F1 score than the Naive Bayes model (0.30).
5. ROC AUC Score: The second model has a moderate ROC AUC score (0.67), indicating its ability to distinguish between classes, which is not available for the Naive Bayes model.

**Which model is better?**

The other model is generally better because it has higher accuracy, precision, and F1 score, despite having a lower recall. The ROC AUC score also indicates it has a reasonable ability to distinguish between the classes.

**Discussion**

Cloud security encompasses various facets, highlighting its complexity. Key measures include Identity and Access Management (IAM) for ensuring only authorized access, and Multi-Factor Authentication (MFA) to add an extra security layer. Data encryption at rest and in transit is crucial for safeguarding data, requiring robust encryption algorithms and secure key management. Network security, compliance with regulations like GDPR and HIPAA, and regular audits are essential. Monitoring and logging enable timely threat detection, while comprehensive incident response and disaster recovery plans ensure preparedness. Employee training on best practices and adopting a zero-trust architecture further strengthen security. Regular risk assessments and the use of AI/ML for threat detection enhance overall security effectiveness.

**Limitations**

Despite robust security measures, several limitations exist in cloud security practices. The shared responsibility model can lead to confusion and gaps in coverage if roles are not clearly defined. The dynamic nature of cloud environments adds complexity to managing security. Comprehensive data encryption can introduce performance overhead and key management challenges. Ensuring regulatory compliance across different jurisdictions is complex and resource-intensive. Monitoring and logging can generate vast data volumes, making threat detection difficult. Incident response and disaster recovery plans require regular updates and testing, which can be resource-intensive. Human errors and insider threats remain significant risks despite training programs.

**Conclusion**

In conclusion, the paper underscores the importance of robust security measures in cloud computing and emphasizes the need for continuous adaptation to emerging threats. It highlights the role of collaboration between stakeholders and the implementation of best practices to ensure the integrity, confidentiality, and accessibility of data within cloud environments.

References:

<https://www.sciencedirect.com/science/article/abs/pii/S0045790617320724>

<https://link.springer.com/chapter/10.1007/978-3-030-34957-8_7>

<https://ieeexplore.ieee.org/abstract/document/9032545/references#references>

<https://ieeexplore.ieee.org/abstract/document/8301700/references#references>

Gupta, M. V., & Assistant Professor. (n.d.). Benefits, challenges, importance of cloud security. Ijfans.org. Retrieved May 11, 2024, from <https://ijfans.org/uploads/paper/8cb332332e8562cc03e2965ad7d2cd27.pdf>

Mogos, Gabriela. (2019). Cloud Security. Critical analysis. International Journal of Computer Science and Information Security, 17. 51-54.

Aljawarneh, S. (2020). Cloud security: A comprehensive review. Journal of Computer Security, 1(1), 45-62.

Alomari, O. A., & Jie, W. (2021). Security issues in cloud computing: A systematic literature review. Journal of Cloud Computing: Advances, Systems and Applications, 10(1), 1-25.

Goyal, S., Jain, S., & Goyal, R. (2020). A survey on security issues in cloud computing. Journal of Information Systems Engineering & Management, 5(1), 18-28.

1-Kalla, D., Smith, N., Samaah, F., & Kuraku, S. (2023, April 13). Study and analysis of Chat GPT and its impact on different fields of study. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4402499

2- Mustyala, Anirudh. “Securing Cloud Infrastructure: Best Practices for

Protecting Data and Applications.” International Journal of Computer Trends

and Technology 71, no. 6 (June 30, 2023): 73–78.

<https://doi.org/10.14445/22312803/ijctt-v71i6p113>.

Ben-Salem M, Salvatore J. Stolfo, and Angelos D. Keromytis, “Fog Computing: Mitigating Insider Data Theft

Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW), 2012.

Ben-Salem M, Salvatore J. Stolfo, and Angelos D. Keromytis, “Fog Computing: Mitigating Insider Data Theft

Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW), 20123-

3- Ben-Salem Mnd

Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW), 2012.

3- Libraries, C. U. (1970, January 1). Fog computing: Mitigating insider data theft attacks in the cloud. Academic Commons. https://academiccommons.columbia.edu/doi/10.7916/D8T443GW