Memorandum: Cloud Computing Security

TO: Prof. Becker

From: Robert Serembe

IS 390 Reading and Research

Date: 5/10/24

This Memorandum is just to share brief research of my topic cloud computing security.

I would like to begin with the early development of cloud computing, which traces back to the 1960s during the era of timesharing systems that allowed multiple users to share computing resources. The use of timesharing systems led to security issues, thus prompting the need for cloud security measures.

History of Cloud Computing: Past, Present, and Future (icorps.com)

Research Methodology, Limitations, and Results

I will collect data using different methods:

- Case Studies: Looking at specific examples of cloud security to understand what works well and what doesn't.
- Theoretical Analysis: Reading and reviewing existing research and theories about cloud security.
- Interviews: Talking with my group members and professor to get their insights and opinions.
- Surveys: Sending out surveys to gather data on how people use and view cloud security.
- Observations: Watching and noting how cloud security is applied in real situations.
- Library Research: Using the library to find books, articles, and other information related to cloud security.

Limitations- One main limitation I faced was changing my topic from cloud computing to cloud security. Cloud computing is a huge area, making it hard to cover everything. By focusing on cloud security, I can concentrate on a smaller, more specific part of cloud computing.

Results- Although I am still gathering results, I have made good progress in collecting data and focusing my research. Changing to cloud security has helped me dive deeper into specific issues and solutions. The information from interviews, surveys, and case studies will help me understand the current state and future of cloud security better.

1. Security threats in cloud security.

In this, I will talk about how many organizations, businesses and individuals have been affected.

Top Cloud Threats | CSA (cloudsecurityalliance.org)

2. Security Measures in Cloud Computing.

   Measures taken have helped many companies to stay in business and continue to secure their data with all means possible. This has resulted from previous experiences or seeing how other big companies go down due to not taking measures to secure themselves.

(PDF) Data Security and Privacy Issues in Cloud Computing: Challenges and Solutions Review (researchgate.net)

CSA Security Guidance for Cloud Computing | CSA (cloudsecurityalliance.org)

3. Challenges and limitations

Many organizations, businesses, and individuals face various challenges, including transparency and control issues, the shared responsibility model, and compliance issues. These challenges hinder their growth. To mitigate them, it is crucial to select the best cloud providers and ensure they evaluate their security issues before signing a contract with them.

4. Some Examples of Big Organizations affected by data breach are: -

When a data breach occurs, very sensitive information is stolen and may sometimes be sold on the dark web or third parties. Some of the biggest data breaches are: -

AT&T is the recent company where data was leaked online. Customers' information was published on the dark web. Others are Yahoo 2013-2016, Microsoft 2021, Facebook 2021, Linked in 2021, JPMorgan Chase 2012 and many more.

AT&T data breach: Millions of customers caught up in major dark web leak (bbc.com)

Biggest Data Breaches in US History (Updated 2024) | UpGuard

5. Best practices for cloud computing security.

- Employee training
- Continuous monitoring and compliance
- Implement security measures and controls early in cloud adoption process considering at each stage of cloud lifecycle.

6. Policy recommendations for improving cloud security on a global scale.

- International cybersecurity standards,
- cross board data protection laws,
- public and private collaboration,
- regulatory oversight, and enforcements