Project Proposal

Written By
Michael Lawrence Ayodele

Email: BI51TW@student.sunderland.ac.uk

PROM02 - Computing Master''s Project (2023/4 - Sunderland - ASUND - NSSEM2)
2023/4

University of Sunderland

May 13, 2024

Topic: The Impact of Cyber Attacks on Cloud Security and Data Privacy (*A Practical Analysis)*

1. Introduction:

Cloud computing has been recognized as a foundational building key for modern IT infrastructures, as it supports better scalability, flexibility, and cost-efficiency to organizations across diverse sectors. It offers diffenrent ranges of services such as PaaS, Saas, and IaaS depending of the organizations requirement. However, the wide-scale adoption of cloud services such as AWS, Google cloud platform (GCP), Microsoft Azure and others, has also added some new dimension of cyber threats, posing significant challenges to cloud security and data privacy.

This project proposal seeks to investigate the impact of cyber attacks on cloud security and data privacy, employing different approach that integrates real-world case studies and experimental analysis.

2. Research Objectives:

The main aim of this research project will be to understand the ripple effects of this organised transfer from cyber attacks to cloud security and the extent it influences data safety.

Taking the research objectives in particular, the thesis will cover the following, but not limited to if time permits.

- Analyzing real-world case studies of cyber attacks targeting cloud infrastructures.
- Define experiments that run in a controlled environment to perform different kinds of cyber attacks to the cloud. For this, I will use the AWS cloud as well as IAC(Terraform) to build my demo infrastructure and add a self-healing feature to it.
- What this could allow us to do is to identify vulnerabilities that were imported by the use of cloud infrastructures and to evaluate their impact on security and data privacy.
- Proposing real strategies to fortify cloud security frameworks and mitigate cyber threats, also design architectures for best practices.

3. Literature Review:

The literature review will provide a comprehensive overview of existing research and theoretical frameworks in the field of cybersecurity and cloud computing.. Particular research studies examining cyber attacks, threat modeling and risk assessment, as well as the theoretical backdrop to cloud security will be considered.

4. Methodology:

The research methodology will combine a pragmatic approach using qualitative case studies and quantitative experimental analysis. By conducting a case study analysis of relevant real-world cyber attacks on critical cloud infrastructures, I will seek to unveil what types of tactics are being used by the perpetrators.

And, at the same time a controlled experiments would be conducted as well by simulating different types of cyber attack using a cloud environment (to be developed using AWS cloud platform or in deployment with a rasberrypi), to go deep within the vulnerabilities, reduce them into small steps and micro-decisions, and then understand the possibilities more granularly and in substantial relation to the privacy of data.

5. Expected Outcomes:

The expected outcomes of this research project would include:

- A comprehensive understanding of the impact of cyber attacks on cloud security and data privacy.
- Empirical evidence derived from real-world case studies and experimental analysis.
- Actionable insights and recommendations for fortifying cloud security frameworks and mitigating cyber threats.
- Contributions to the existing body of knowledge in the fields of cybersecurity and cloud computing.

6. Timeline:

The proposed timeline for the research project would be provided after discussion and update to the project plan document.

7. Conclusion:

In conclusion, this project proposal seeks to address the growing need for empirical research on the impact of cyberattacks on cloud security and data privacy by way of which spans a range of projects leading to the use of real-world case studies and experimental research. It is to provide insights and recommendations for action to strengthen the system and reduce cyber threats