Decoding the Complexities: A Comprehensive Guide to Cloud and Virtualization Security

Irfanul Hoque ID: 21301232

Rakhin Mostafa ID: 20101084

Rizvy Ahmed kamal ID: 23141083

Sadiul Arefin Rafi ID: 20101120

Introduction

- Virtualization’s rising prominence in cloud computing
- Logical partitioning of hardware and software resources for multiple tenants.
- Enhanced flexibility but heightened security concerns
- **Virtualization in Cloud:**
  - Virtualization allows logical partitioning of resources (CPU, memory, storage, network).
  - Managed by hypervisor/Virtual Machine Monitor (VMM) .
- **Security Risks and Complexity:**
  - Virtualization's complexity expands attack surface.
  - Improperly designed isolation can become a security risk.

Literature Review

- Examination of research papers on security issues in cloud computing. Focus on identifying challenges and proposing mitigating methods.
- Key Security Issues:
  - Privileged user access exposing data during transmission.
  - Regulatory compliance responsibility even with service providers [7].
  - Ambiguities in data location, segregation, and encryption.
  - Disaster recovery needs, difficulty in identifying provider wrongdoing.
  - Concerns about long-term viability after acquisitions.
  - Balachandra et al.'s coverage of data locations, segregation, recovery .
  - Addressing data localization, trust dynamics, accounting challenges.

Cloud Computing Virtualization

- Functional Execution Isolation
- Specialized Environments
- Ease of Management
- Flexibility in operations like start, migration, termination.
- Depends on underlying hardware availability.
- Coexistence of Legacy and New Applications
- Testing and Debugging
- Enhancement of Reliability

Decoding the Complexities: A Comprehensive Guide to Cloud and Virtualization Security

Irfanul Hoque ID: 21301232

Rakhin Mostafa ID: 20101084

Rizvy Ahmed kamal ID: 23141083

Sadiul Arefin Rafi ID: 20101120

Security threats to virtualization in cloud computing

- Virtual Machine Migration:
  - Hot migration without VM shutdown.
  - Mitigation: Strong encryption during migration.
- Virtual Machine Escape:
  - Mutual isolation and resource sharing.
  - Threat to Hypervisor and host.
- Rootkit Attack:
  - Hides processes, files, network links.
  - Often combined with Trojans, backdoors.

Countermeasures for Virtualization Security in Cloud Computing

1. Encryption and Key Management (EKM):

- Protect data against loss and theft.

- Encryption at rest, in transit, and on backup

2 Intrusion Detection Tools:

- Multi-tenant cloud attractive to intruders.

- Ensure safe and secure environment, block intruders.

3. Virtual Firewall (VF):

- Protects VMs and VMM.

Conclusion

1.Enhancing Resource Management and Flexibility:

- Increases availability and flexibility of hardware resources.

2. Security Challenges in Virtualization:

- Evolving security dimensions demand attention.

3. Understanding and Recognizing Threats:

- Classifying major security issues in cloud and virtualization

4. In-depth Analysis for Security Enhancement:

- Comprehensive review and analysis of challenges.

5. Countermeasures and Strengthening Protection