Security Risk in Cloud Computing

Sarah Hollingsworth

COMP 630

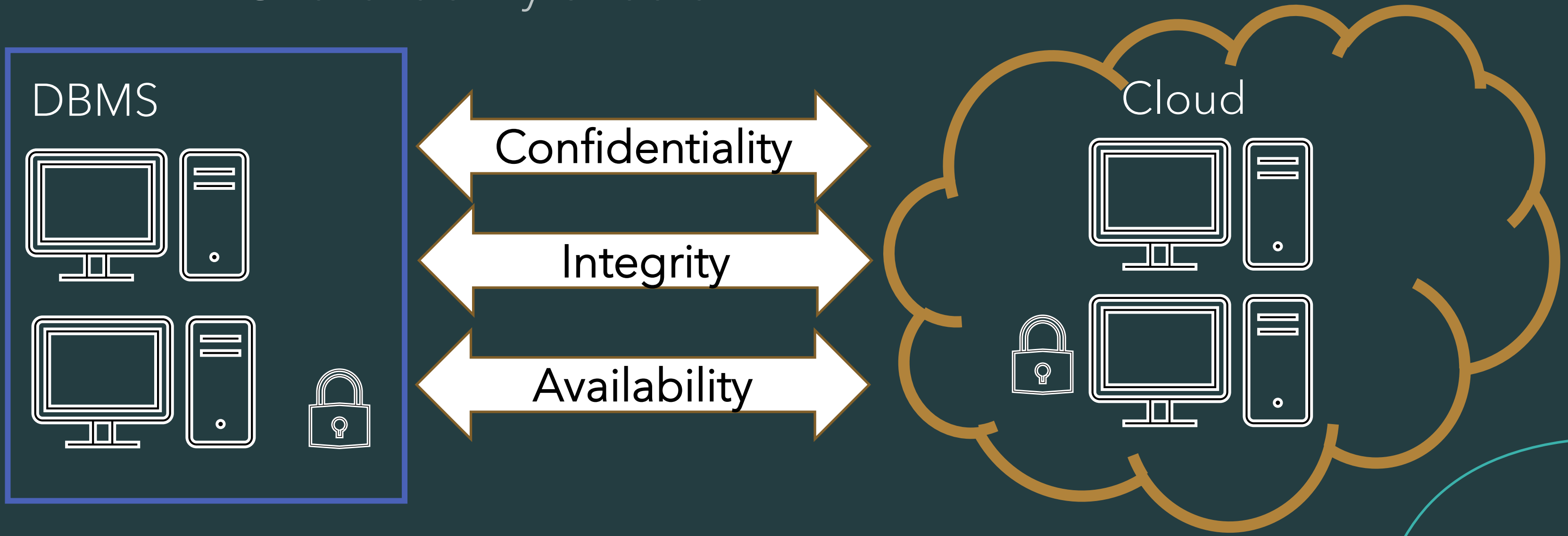
Franklin University

Cloud Computing Security Risk

- As corporations expand their Information Systems to include cloud computing technologies, they must evaluate the security risk associated with these new technologies
- Security Principles
    - Confidentiality
    - Integrity
    - Availability
- Proposed Model: Dynamic Secure Interconnection Mechanism
- Example: Financial Institution Information System Model
- Conclusions

Security Principles

- When implementing the Cloud Computing security model, the design should address the three security principles; Confidentiality, Integrity, and Availability.
- Failure to address these principles can lead to security breaches through:
  - Unauthorized exposure of data
  - Incorrect data modification
  - Unavailability of data



Security Principle: Confidentiality

- Problem: By not placing proper controls, data can be inadvertently or maliciously accessed or exposed by unauthorized users
- Confidentiality breaches can result in:
  - Loss of proprietary information
  - Exposure of privacy information
  - Identity theft
  - Civil and Legal Penalties
    - Consumer Financial Protection Bureau (CFPB), Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act
- Solution
  - Access control mechanisms
  - Data encryption

Security Principles: Integrity

- Problem: By not applying controls, data can be intentionally or unintentionally accessed or modified, resulting in corrupted or nefariously destroyed data
- Integrity breaches can result in:
  - Use of corrupted or modified data
  - Erroneous or poor decisions
  - Financial loss
  - Reputational harm
- Solution
  - Access control mechanisms
  - Semantic integrity constraints

Security Principles: Availability

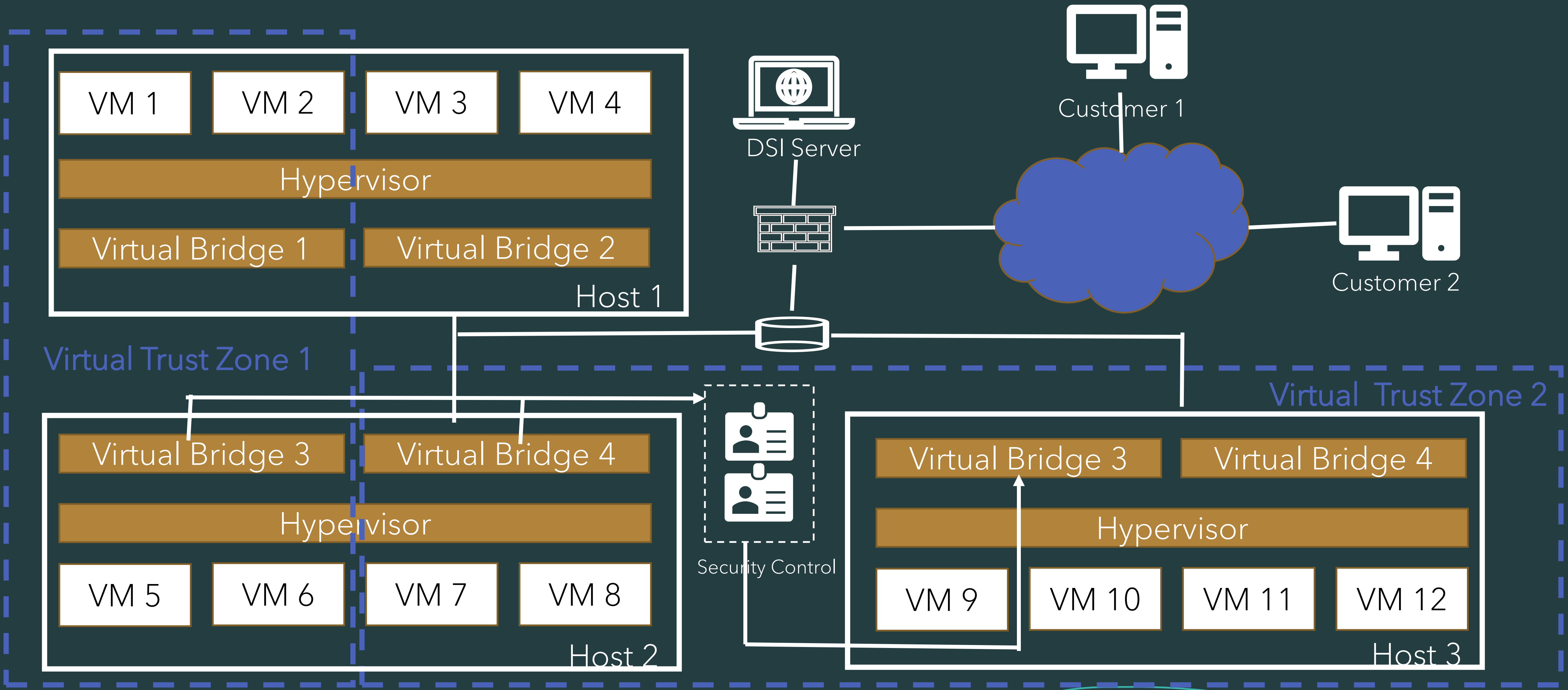
- Problem: Hardware and software failures or errors, malicious activity, malware or viruses, environmental failures including fire, flood and loss of power can result in loss of data availability
- Availability breaches can result in:
  - Business discontinuity
  - Detriment of reputation
  - Loss of revenue
- Solution
  - Concurrency controls
  - Recovery subsystems
  - Data replication

Proposed Model: Dynamic Secure Interconnection Mechanism

- Dynamic Secure Interconnection (DSI) Mechanism
  - Virtual layer establishes a secure connection between the server, clients, and virtual bridges, which creates a trust zone between Virtual Machines (VMs) and the cloud computing system
- Virtual Trust Zone
  - Virtual Machines (VMs) implement the security policies, allowing customers to login and obtain service from a cloud computing system, by allotting resources to the VMs comparable to a traditional CPU
- Virtual Bridge
  - By assigning each VM its own virtual MAC and virtual IP addresses, the module implemented on the Virtual Machine Monitor (VMM) communicates packets of secure information from the VM to other VMs or the cloud

Adapted from (L. He, 2016)

Dynamic Secure Interconnection Mechanism Model

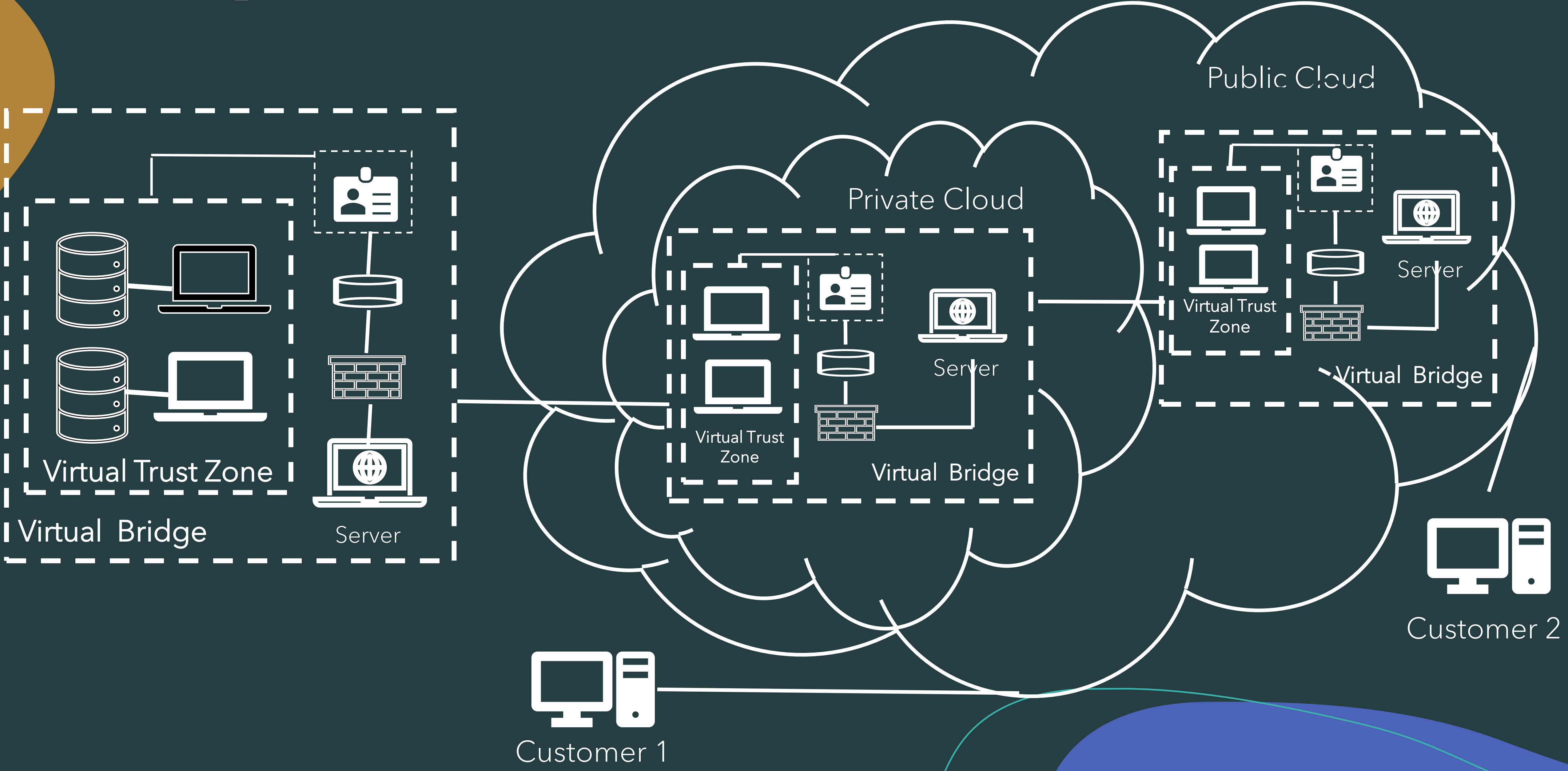


Adapted from (L. He, 2016)

Example: Financial Institution Information System Model

- Financial Institution Information System Model
  - RDBMS
    - Includes physical storage of data
  - Hybrid Cloud
    - In-house Private Cloud
    - Public Cloud
- Allows financial institutions to incorporate security principles in the design of the model
  - Access control mechanisms and encryption at the RDBMS, Private and Public Cloud levels
  - Integrity constraints at the RDBMS, Private and Public Cloud levels
  - Recovery subsystems at the RDBMS level
  - Concurrency controls and data replication at the RDBMS, Private and Public Cloud levels

Example: Financial Institution Information System Model



Conclusions

- Advantages
  - Defined relation schema and SQL query language
  - Hybrid Cloud
    - Storage and computation capabilities
    - Secure access for clients to view information
- Evaluate
  - Model Type
    - RDMBS
    - Public Cloud
    - Private Cloud
    - Hybrid Cloud
    - Community Cloud
  - Cloud and/or Physical Storage
  - Replacement of CPUs with VMs
  - Build DSI Mechanism

Resources

Gray, J. (2019, April). Basic Principles of Database Security. ISSA Journal, pp. 22-27.

L. He, F. H. (2016, June). Dynamic Secure Interconnection for Security Enhancement in Cloud Computing. International Journal of Computers, Communications & Control., pp. 348-357.

Shirvani, M. H., Rahmani, A. M., & Sahaf, A. (2018, March). An iterative mathematical decision model for cloud migration: A cost and security risk approach. Software: Practice and Experience, pp. 449-485.

Youssef, A. E., & Alageel, M. (2012, July). A Framework for Secure Cloud Computing. IJCSI International Journal of Computer Science.