Cloud Security
EECS 263 Presentation

By: Hridaya Patel and Kavita Kumar

Presentation Overview

- Concerns and questions organizations and individuals ask themselves when using the cloud.
- Background information on why many companies and the general IT infrastructure is moving to the cloud.
- Next, what Cloud Computing is and why security in the cloud is of utmost important in today’s technology landscape.
- Lastly, solutions and security strategy organizations people can take based on their risk evaluations.

Introduction

Cloud Computing Introductory Videos:

1. What is Cloud Computing?
   https://www.youtube.com/watch?v=ae_DKNwK_ms
2. Virtual Machines and how they power the cloud:
   https://www.youtube.com/watch?v=GIdVRB5yNsk

Background

- Cloud computing is a highly complex software service being accessed through a network
- Constant vulnerabilities
- Security model that is compliant with government standards and also the risk policy they choose.
  - Data-Centric
  - We have to assume there WILL BE a breach.
  - Risk posture
  - Prioritize the data
  - Implement a resilient incident response to any cyber attack.

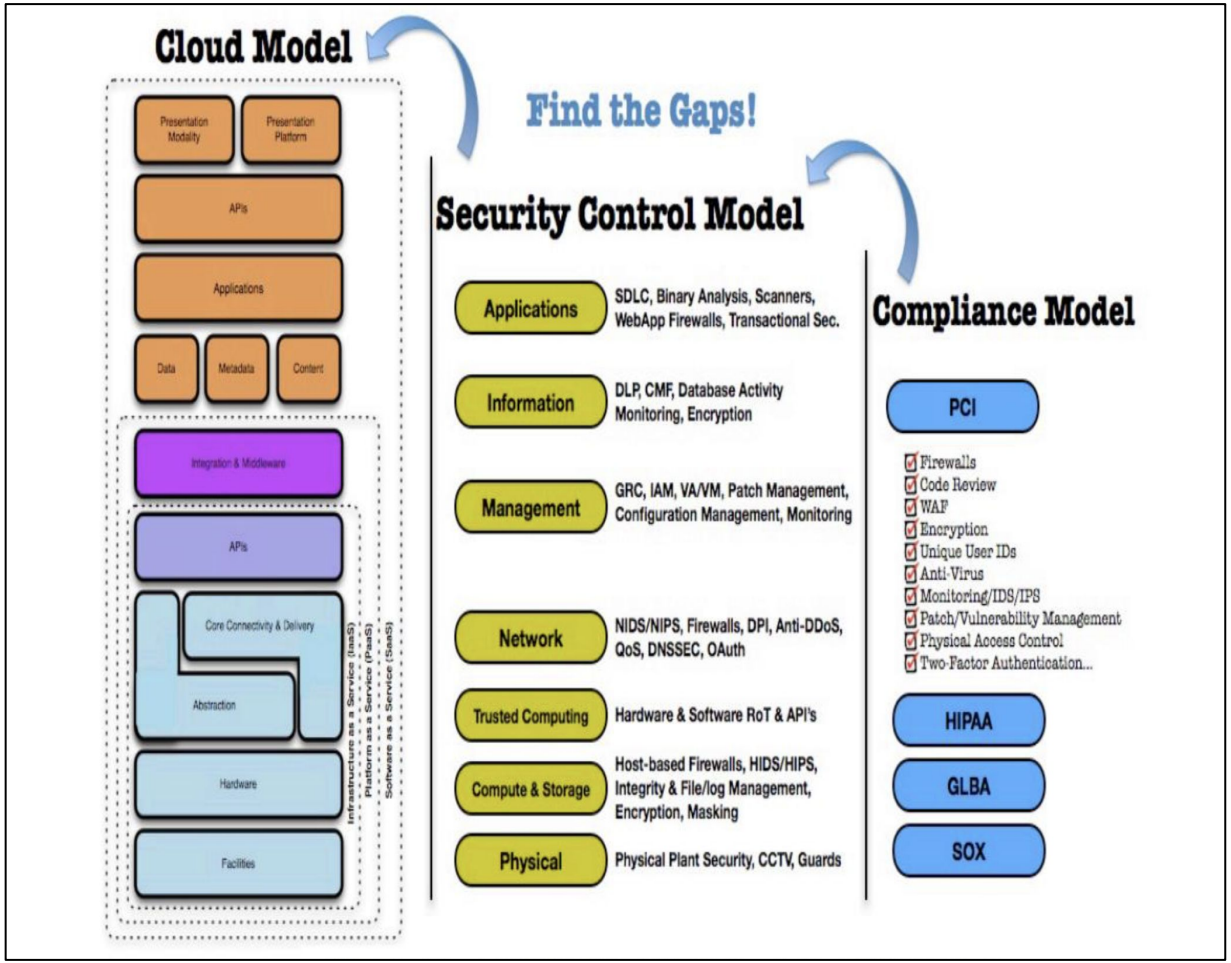

Figure 1: Cloud, Security and Compliance Model

Background Continued: Computing Security Problem and Strategy

- The cloud is a metaphor for the Internet
- Abstraction for a complex infrastructure
- Private cloud refers to internal data centers of a business or other organization not made available to the general public.
- Symmetric key can get high security but encryption and decryption is slow.
- WS-Security, WS-Reliability, WS-Trust, WS-Authorization, WS-Secure Conversation
- Single security method cannot solve the cloud computing security problem

Security Threats in Cloud Computing

- Lack of security is the only hurdle in wide adoption of cloud computing.
- From the user perspective the lack of security might be the only real disadvantage to the cloud.
  - Users are very skeptical side about cloud security since they do not want loss of data and privacy.
- Top security concerns for cloud computing:
  - Data loss
  - Leakage of Data
  - Client's trust
  - User's Authentication
  - Malicious users handling
  - Wrong usage of Cloud computing and its services
  - Hijacking of sessions while accessing data
- Solution: Make sure your cloud is compliant with government laws and also insure that your cloud service provider has a good track record for providing good security in the cloud.

Security Threats in Cloud Computing

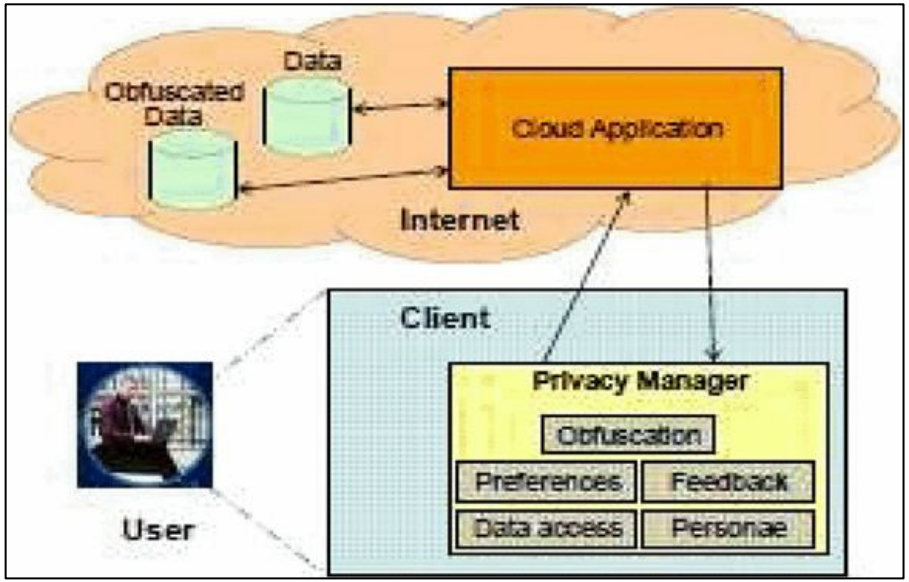

Figure 2: Privacy Manager

- Obfuscation
- Privacy Manager
- Data can be understood by knowing obfuscation code
- Encryption requires key – used to encrypt data and decrypt

Security Model

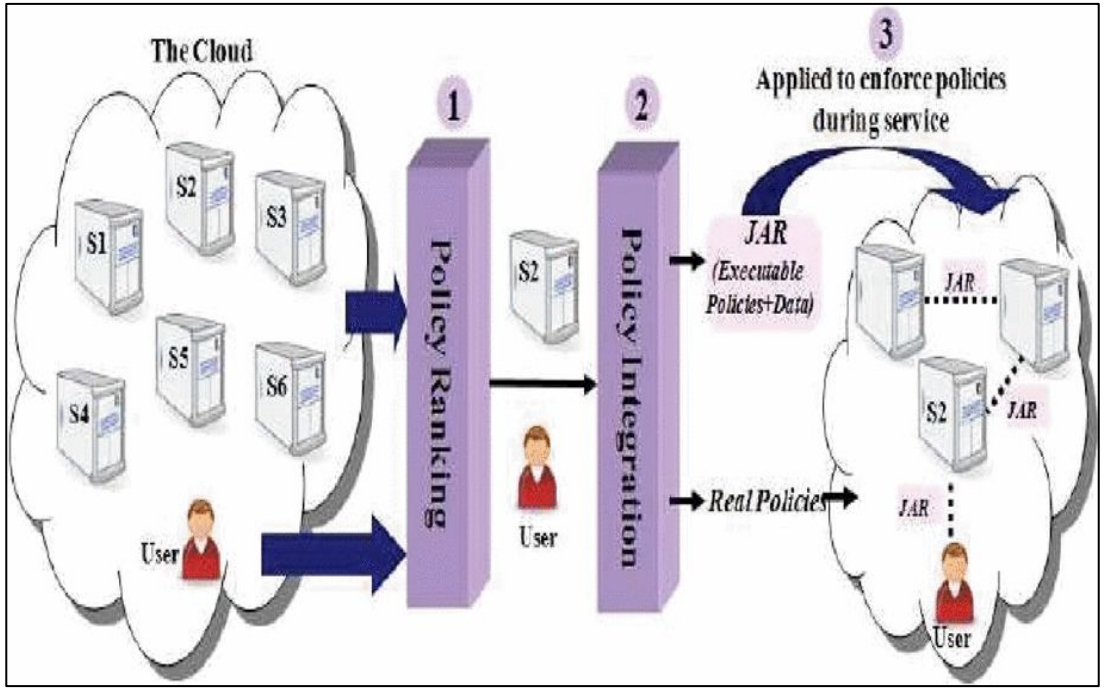

Figure 3: JAR Policy Model

- Assign different grades to servers.
- User has different rights and authentication.
- Provides Correctness,Time-Efficiency, Scalability, Security, Robustness and Reliability

Cloud Computing Security--Trends and Research Directions

Implication II: Secure physical computing, storage and network access environment

- Typical data-center related security measures related to physical access
- It is often noted that major security breaches and threats come from internal staff.
- Remote location - very few people know the exact location
- Limit access location
- Some problems: fire, earthquake, hvac issues

Note: Cloud services access through browsers and thin mobile devices running HTML-5. Browser = no mean of handling XML encryption and rely on SSL layer for handshake. Potential threat.

Cloud Computing Security--Trends and Research Directions (Continued)

Information Centric Security (ICS)

- Public cloud is stored outside of organizational boundaries
- We need to insert context specific access metadata in the information itself
- Strong encryption of the entire data may not be useful
- Extensible Access Control Markup Language (XACML)
- Any access request to the data can then be verified through an assertion or by checking with central server.
- Cryptographic Message Syntax (CMS)

Steps Towards a Security Assessment Framework

1. Characterize the application's security requirements
2. Characterize and review cloud provider's security strengths and vulnerabilities
3. Map application's security characteristics and cloud security characteristics to perform a fit analysis

Cloud Security Model in Relation to Health Compliance

- A business such as a hospital needs to have legal compliance in accordance to US cyber laws.
  - HIPAA - Health Insurance Portability and Accountability Act
  - PHI - protected health information
- Compliance is extremely important
  - Transfer patient records to the Cloud Infrastructure in the modern tech space.

Addressing cloud computing security issues

- Trust depends on deployment model
- cryptography to ensure the confidentiality, integrity and authenticity of data and communications, while attempting to address specific security vulnerabilities.
- A TTP (Trusted Third Party) is essentially a Trusted Authority delegated with the responsibility of addressing a number of security issues in a multilevel distributed environment.
- Ps are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI). Public Key Infrastructure provides technically sound and legally acceptable means to implement
- Cryptographic Separation in which processes, computations and data are concealed in such a way that they appear intangible to outsiders

Cloud computing security: The scientific challenge, and a survey of solutions

Ways to Achieve Cloud Security:

- **Fully Homomorphic Encryption:** the data owner can encrypt the data before sending it to the cloud. It is an encryption technique that allows a party that holds ciphertexts to perform certain operations on the ciphertexts, which mirror the corresponding operations on the plaintexts.
- **Key Translation in browser:** With this approach, data is encrypted before being uploaded to the cloud, and the data owners retain the keys.
- **Hardware anchored security (Excalibur):** The final approach to achieving confidentiality from the cloud provider is based on special hardware on the cloud side.
- **CryptDB:** CryptDB (Raluca et al., 2012) is a framework that allows query processing over an encrypted database. The database is stored and managed by the cloud provider, but data items are encrypted with keys that are not under the cloud provider’s control.

***** Model Provided on the next slide!! *****

Hardware - Anchored Cloud Security

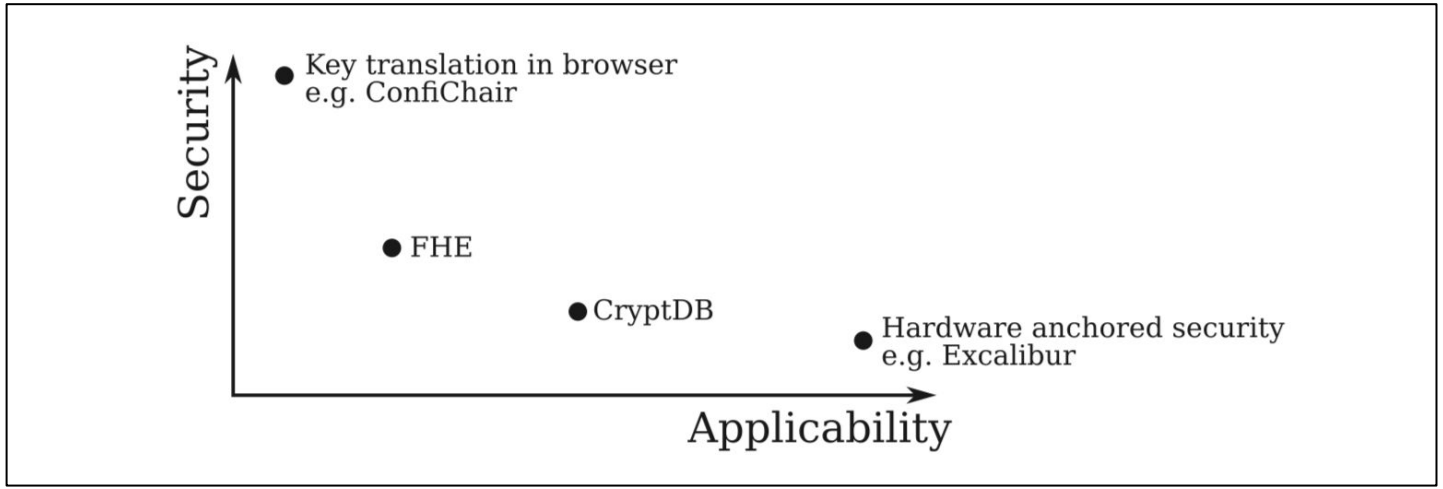

Figure 4: Four Approaches, Impressionistically Organized by Security and Applicability

- Figure shows the most applicable model in hardware- anchored security in the style of Excalibur.
- Most versatile of the four approaches
- Security guarantees
- Key translation

Cloud Security Alliance - Improving Metrics in Cyber Resiliency

- Billions of dollars spent on cyber security
- Large scale data breaches every year at the corporate and government level.
- Elapsed Time to Identify Failure (ETIF)
- Elapsed Time to Identify Threat (ETIH).
- Improve process and metrics
- Advances IDS algorithms needed to detect anomalies and improve cyber resiliency.
- Lower the ETIF, the smaller the loss of resiliency for an information system.
- We need to lower the time to identify failure in order to have a particular information system become more resilient (Ex: recovery time from a data breach is faster).

Example:Amazon Web Security Services and Tools

Link: https://aws.amazon.com/security/

Why go with AWS instead of Azure or Google?

- Amazon has a **great track record of customer service** as evidenced by their huge online success and product value in the stock market.
- Cloud Security is a **high priority for Amazon** because they want to keep up their reputation as a secure Cloud provider.
- They recently acquired a security company called SQRRL. They specialize in big data analytics and cybersecurity.
- **Amazon Offers:**
  - Infrastructure Security
  - DDoS Mitigation
  - Data ENcryption
  - Inventory and Configuration
  - Monitoring and Logging
  - Identity and Access Control
  - Penetration Testing

Top 12 Cloud Security Threats for the Future (2018 and beyond):

1. Data breaches (ex:ransomware in hospitals, ex: Equifax)
2. Insufficient Identity, Credential, and Access Management
3. Insecure interfaces and application programming interfaces (APIs)
4. System vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats (APTs)
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service (DoS)
12. Shared technology vulnerabilities
13. Threat Intelligence for x86 processors: Spectre and Meltdown flaws
14. Extra https://www.amdflaws.com
    a. Several critical flaws revealed by CTS Labs regarding AMD Ryzen hardware.

References

1. “Cloud Security Bolstered by Threat Modeling.” *Information Security News, IT Security News and Cybersecurity Insights: SecurityWeek*, www.securityweek.com/cloud-security-bolstered-threat-modeling.
2. (n.d.). Retrieved from http://ieeexplore.ieee.org/document/6202020/
3. (n.d.). Retrieved from http://ieeexplore.ieee.org/document/6202020/
4. Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). Cloud Computing Security--Trends and Research Directions. 2011 IEEE World Congress on Services. doi:10.1109/services.2011.20
5. Oloughlin, J., & Gillam, L. (2015). Addressing Issues of Cloud Resilience, Security and Performance through Simple Detection of Co-locating Sibling Virtual Machine Instances. Proceedings of the 5th International Conference on Cloud Computing and Services Science. doi:10.5220/0005485000600067
6. Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software, 86(9), 2263-2268. doi:10.1016/j.jss.2012.12.025
7. Dwivedi, A., Tebben, D., & Harshavardhana, P. (2010). Characterizing cyber-resiliency. 2010 - Milcom 2010 Military Communications Conference. doi:10.1109/milcom.2010.5680128
8. Violino, B. (2018, January 05). 12 top cloud security threats for 2018: The dirty dozen. Retrieved from https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html