

Cloud computing challenges, privacy concerns, security mechanisms and management.

Kelechi Micheal Jacobs.

UNIVERSITY OF WALES OF TRINITY SIANT DAVID, LONDON. 1302898. Final year poster 2018/19.

Aim, Objectives & Motivational Decisions:
“To provide a sound understanding of cloud computing technology, privacy concerns. Security management and risk management”

1. Introduction:
2. what is cloud computing?
3. Essential characteristics of cloud computing.
4. Deployment models.
5. Cloud computing models.
6. Advantages and disadvantages of cloud computing.

Privacy in cloud computing:

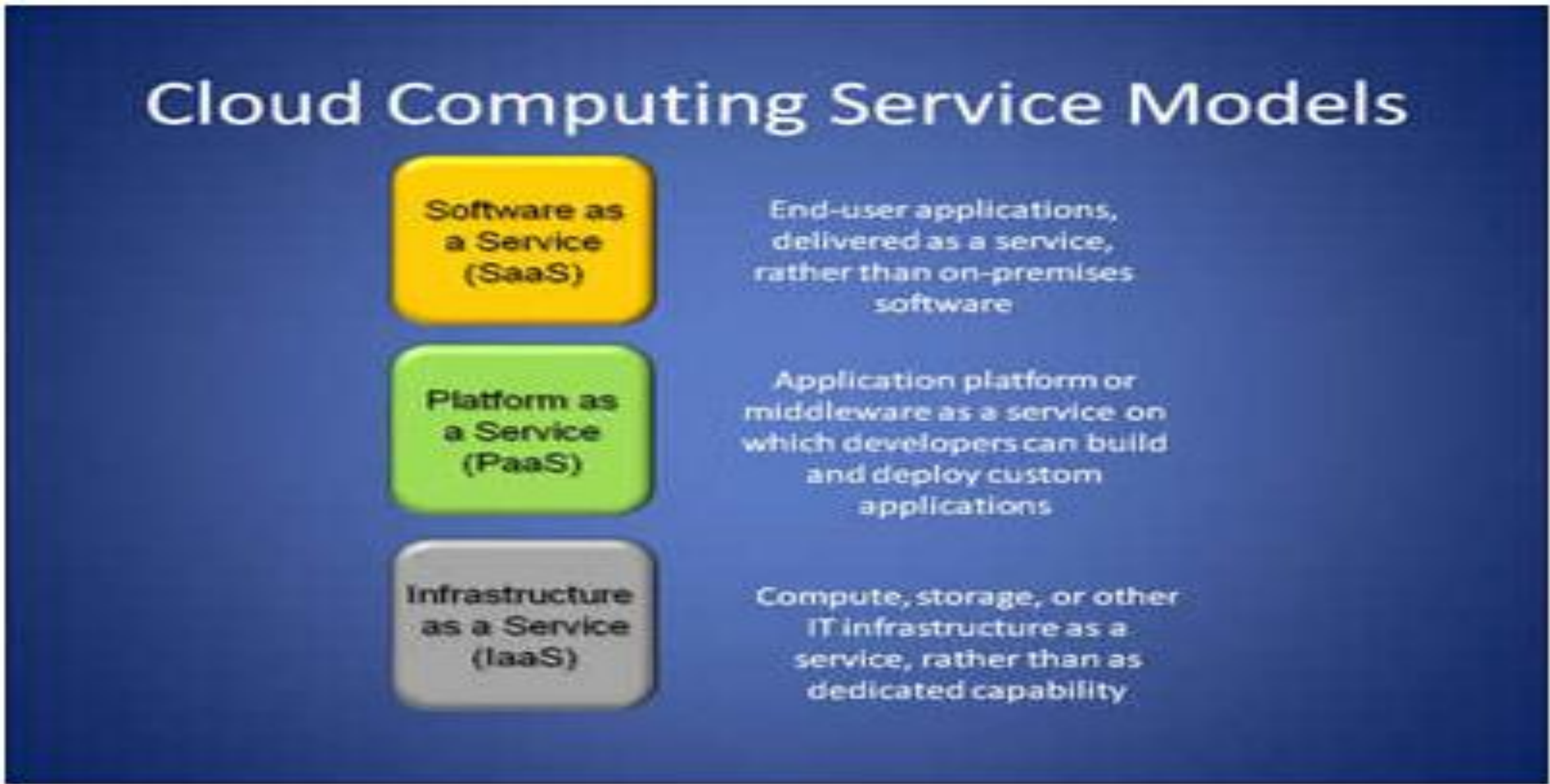
1. Overview.
2. PII – personal identification info.
3. Types of PII.
4. Types of privacy concerns in CCT.

1. Lack of expertise.

2. A potential unauthorised sec. usage.

3. Litigation.

4. Complexity of regulatory compliance.
5. Mechanism to prevent privacy issues.



Security in cloud computing:

1. The 5 fundamentals of security in CCT.
2. Types of security attacks:

1. Data loss

2. Data breaching

3. Dos attacks

4. Cloud abuses.
3. Mechanisms to secure the cloud.

Risk management:

1. What is risk?
2. Risk classification.
3. Accessing risks.
4. CSA (cloud security alliance.

Risk analysis:

1. Quantitative analysis.
2. Qualitative analysis.
3. Auditing analysis.

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

Review

Hazardous Material Release

Consequence

Modelling

Source

Hazard

Effect

Quantitative Frequency Analysis

Risk Estimation

Final Thoughts

Quantifying Risk

If more than one type of receptor can be impacted by an event, then the total risk from an undesirable event can be calculated as:

$Risk_h$

R_h

Risk from an undesirable event, h

$=$

$\sum_{k=1}^K \sum_{i=1}^N$

$Consequence_{i,h,k}$

$* Frequency_{i,h,k}$

Consequence of undesirable event, h

Frequency of consequence i, from event h

where k is each receptor (ie. people, equipment, the environment, production)

8

Practical/future work/conclusion:

1. Man in the middle attack
2. Take online course to enhance my knowledge on CCT.
3. Practically able to learn about hacking intrusions and network security.
4. Further my learning activities to a master’s in network security.

