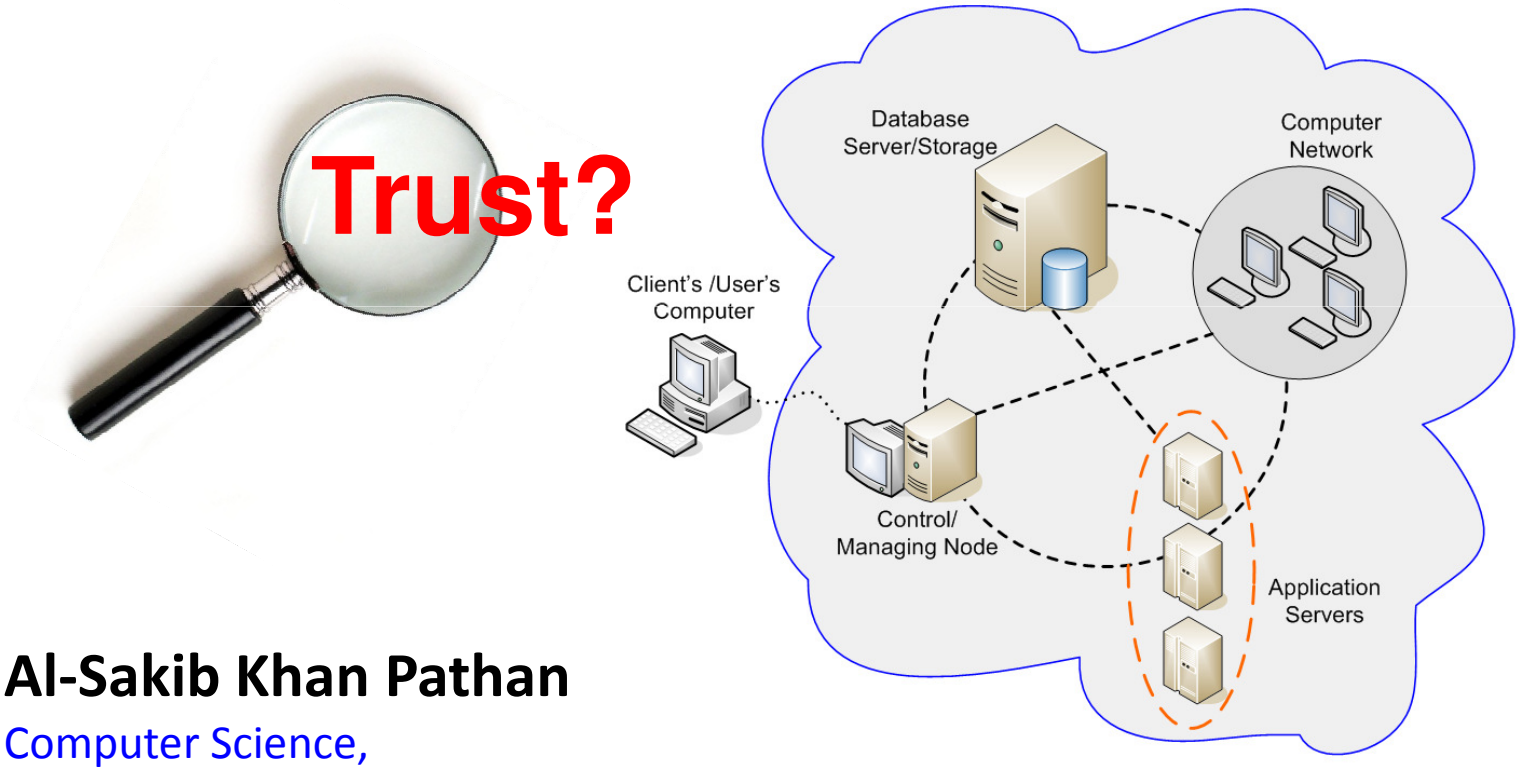
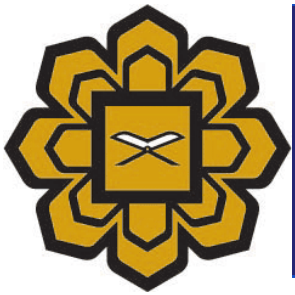
Building Customer Trust in Cloud Computing Model



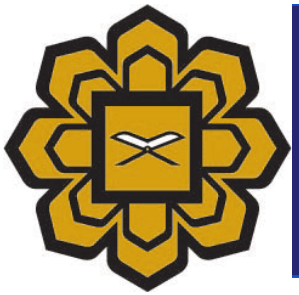
Al-Sakib Khan Pathan
Computer Science,
International Islamic University Malaysia, Malaysia
sakib@iium.edu.my

NDC LABORATORY



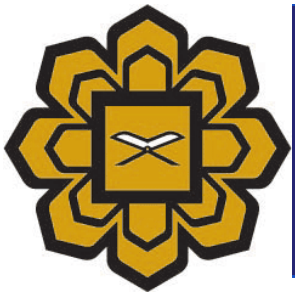
Outline of This Presentation

- Introduction and Motivation
- Required and Key Features of Cloud Computing
- Benefits and Advantages
- Our Proposal and Related Issues
- Analysis of Various Aspects
- Conclusions and Future Research Directions



Introduction

- Cloud computing delivers a variety of IT (Information Technology) enabled hardware, software resources, and services to users over the Internet.
- The services include:
  - Software-as-a-Service (SaaS),
  - Communications-as-a-Service (CaaS),
  - Infrastructure-as-a-Service (IaaS),
  - Platform-as-a-Service (PaaS), and
  - Network-as-a-Service (NaaS).



Introduction (Ctnd.)

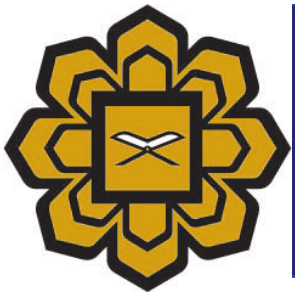
- In the recent years, significant amount of computation works have been done using the facilities of Cloud computing.

- This is because this technology has greatly reduced IT costs by offloading data and computation to Cloud computing services.

Motivation

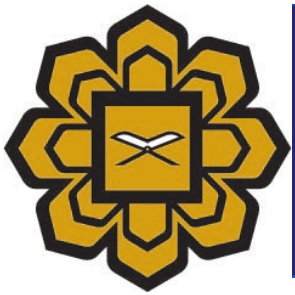
- In spite of increased usage of such computing, still now many companies are reluctant to join the Cloud computing environment due to the outstanding security and trust issues.
- This is what has motivated us to propose this concept of an infrastructure for trusted Cloud.

- Brandon, J., "*Trust in data storage security hits ten-year low*," [Online] Business Cloud News, December 4, 2013, Available at: http://www.businesscloudnews.com/2013/12/04/trust-in-data-storage-security-hits-ten-year-low/ [Last accessed: 19 March 2015]
- *"Business Trust in Data Security in the Cloud at an All-Time Low*," [Online] redOrbit, September 25, 2014, Available at: http://www.redorbit.com/news/technology/1113242614/business-trust-in-data-security-in-the-cloud-at-an/ [Last accessed: 19 March 2015]



Features of Cloud Computing

- Resource Pooling and Elasticity
  - Resources should be pooled to give service to a large number of users.
  - A multi-tenancy strategy is used to dynamically allocate and de-allocate different kinds of resources according to the demands of the users.
- Self-Service and On-demand Service
  - The user should be able to access computing capabilities whenever the need arises and in this process, there should not be any interaction from the Cloud-service provider.

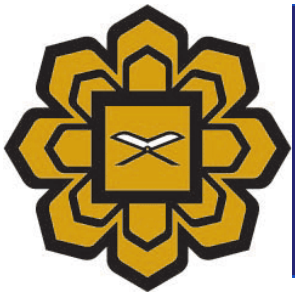


Features of Cloud Computing

- Pricing Factor
  - Billing should be done on usage and possibly, with the minimum charge for the users.
- Quality of Service (QoS)
  - One of the prime factors/features that the users would look for!
  - QoS guarantee must be specified in the Service Level Agreements (SLA) or in the agreement/contract.

Benefits and Advantages in Brief

- Cost Reduction
  - A significant advantage is the elimination of investment cost for stand-alone software/servers.
- Scalability and Speed of Cloud Services
  - No need to install hardware or software for new applications on the user's side.
- New technologies for performing tasks with less burden
- Location selection for infrastructure development
- Any type of device and anytime, anywhere computing



Our Proposal

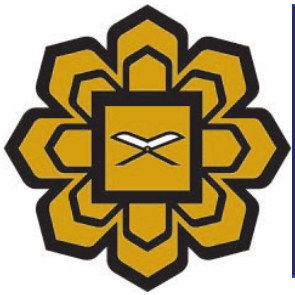
- Given all these aspects and rationale behind Cloud Computing, it is imperative to find reliable solution to ensure trust in such environment.

- We introduce the concept of ---

INTERNATIONAL CENTER FOR MONITORING CLOUD COMPUTING PROVIDERS (ICMCCP)

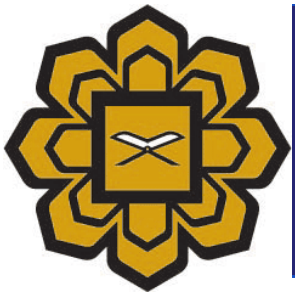
Our Proposal (Cntd.)

- ICMCCP Overview
  - ICMCCP is established on an idea somewhat like a Central bank that regulates other banks in a country; however, the difference is that it would be a global entity, not limited to local.
  - A Headquarter (HQ) for the ICMCCP will be placed in one of the countries in the globe. Then, several branches of it would cover the entire globe, with at least one branch in each country or geographically separate location.



Our Proposal (Cntd.)

- All these branches will follow the HQ of the ICMCCP for any kind of policy that is employed centrally.
- All branches and the HQ will be connected in one computer network.
- Each Cloud Provider (CP) in a particular country would be then connected with the ICMCCP branch in that country/location, i.e., the HQ of the ICMCCP, all ICMCCP branches, and all CPs in the world will be connected in one world-wide network.

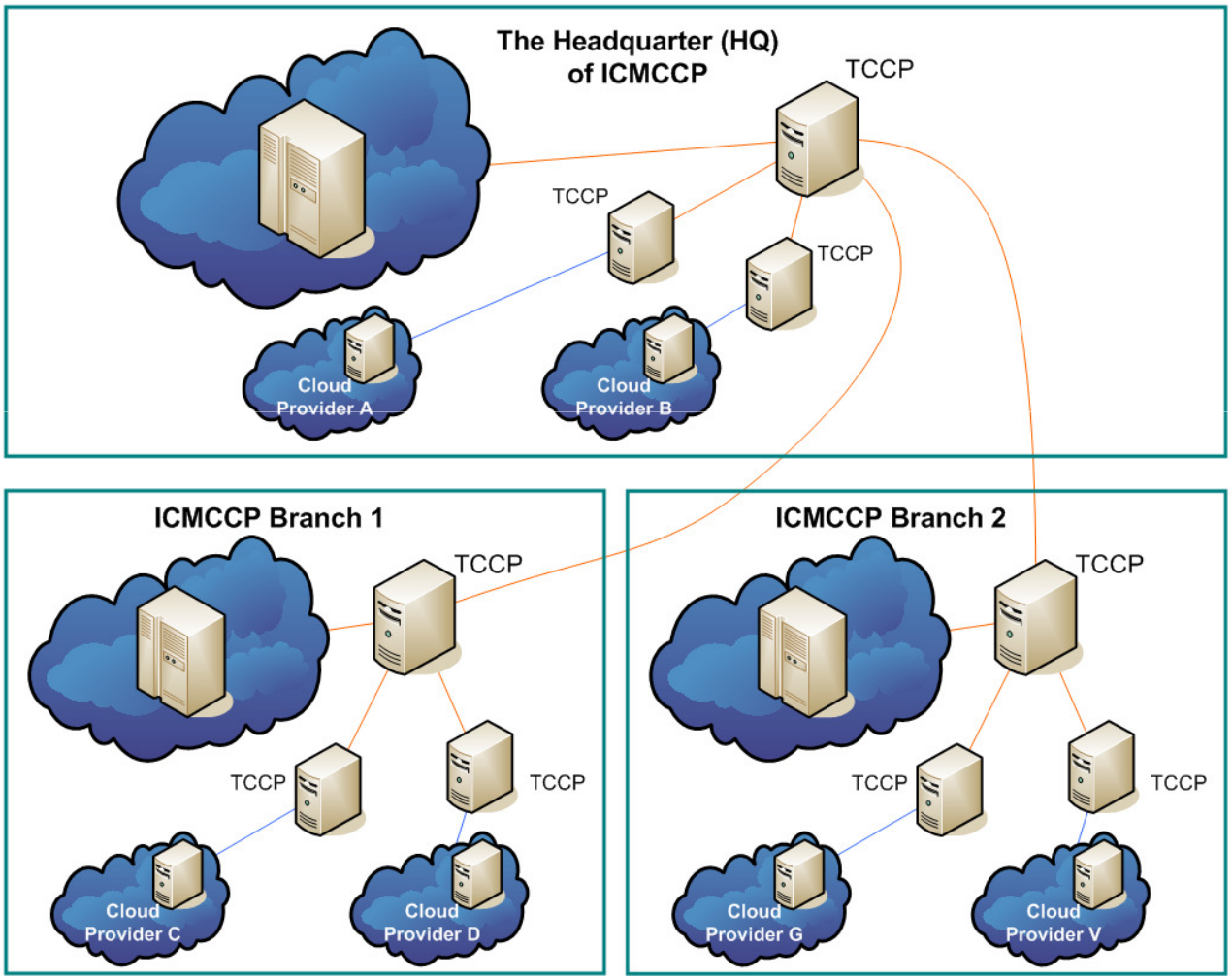


Our Proposal (Cntd.)

- A practical constraint is that no Cloud Provider (CP) can be forced to join the ICMCCP, but the concept is built on the fact that the customers will trust only those Cloud provides that are connected and certified by the ICMCCP, once it is established.
  - ICMCCP is supposed to be a non-profit organization and the required fund to run it could be generated from the CPs and branches that would get the monitoring service that in turn would provide the user a trusted service for Cloud.

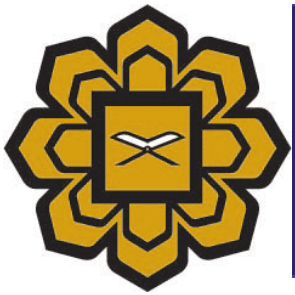
The ICMCCP Architecture

Figure 1



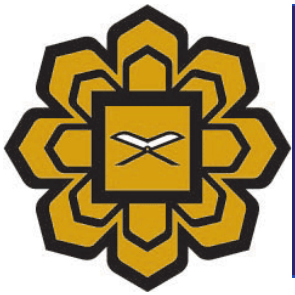
Our Proposal (Cntd.)

- The Constitution of ICMCCP
  - ICMCCP would have a constitution or a set of fundamental principles according to which the organization would be governed.
  - In the process of writing the constitution, experts in Cloud computing, networking, communications, law, banking, and policy making will be involved.
  - The constitution should reflect the customers' aspirations as well.
  - ICMCCP would have power to take legal actions against fraudulent activities.



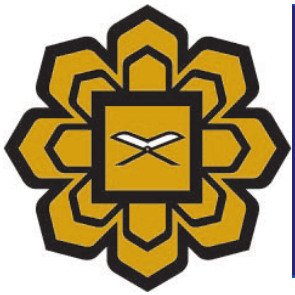
An Example

- An example to illustrate the need for a constitution:
  - Let us consider that a country establishes a Cloud Provider (CP) just for political reason. This CP's name given is Global Cloud Provider (GCP). It appears as a private CP for the customers but it has been made for other purposes.
  - To prevent such a case from occurring, there should be a mechanism for the ICMCCP to verify each CP's status.



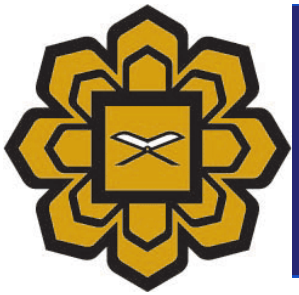
An Example …

- The ICMCCP will make good effort to discover the nature of each CP that is included in its list through technical programs and in another way - that is employing manual security techniques.
- If the ICMCCP discovers a deceitful CP, it will blacklist that CP and raise the legal case to the court.
- The ICMCCP will advertise to all branches that the GCP (as in this example) is not a legitimate provider.



Trust?

- Dealing with Lack of Trust
  - Many of the CPs today are not fully trusted by the customers. Lack of trust narrows down the potential high usage of the Clouds. Hence, a CP must include in its SLA that no data in any form would be released (to others) without the authorization of the owner of the data.
  - There should be some kind of layering or data segmentation method so that complete data may not be retrieved from a single device.



Attacks Against Cloud Servers?

- Dealing with Attacks against Cloud Servers
  - Even if trust is established in the minds of the customers, it is highly likely that the CPs would face different kinds of security attacks against their servers and devices.
  - This issue will not be solved forever, but it is possible for the CPs to try to keep their servers secure by using the latest available countermeasures.
  - A vigilant system administration could ensure the best achievable reliable service by thwarting different kinds of potential attacks.

Two Main Parts

- As understood by now, ICMCCP has mainly two parts:
  - (a) Constitutional part, and
  - (b) Technical part.
- While the constitutional part was presented before, the technical part has a significant role in making ICMCCP secure by using the newest reliable technologies that can provide security for all CPs in the globe.

TCCP: The Core Software

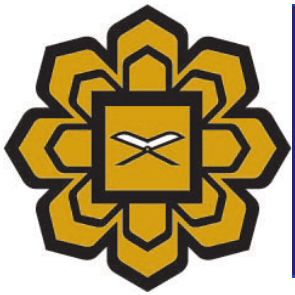
- We have mentioned before that the Headquarter of the ICMCCP, all ICMCCP branches, and all CPs in the world will be connected with one network.
- Hence, a new software could be developed for monitoring all CPs that are enlisted with the ICMCCP. Let us call this software as Tracing Cloud Computing Provider (TCCP).

TCCP: The Core Software …

- This software will be installed in the HQ of the ICMCCP, in all ICMCCP branches, and in all CPs.
- The TCCP will keep monitoring any interaction with each CP in the globe and all recorded interactions would be archived in the local branches to be provided to the HQ for audit and verifications.

TCCP: The Core Software …

- Periodically, the ICMCCP will analyze the data collected by the TCCP to see whether there is any form of irregularity in accessing the CPs.
- The ICMCCP HQ itself will have more security protections and software installed to keep the CPs more trusted to the customers.
- In Figure 1, we showed how the ICMCCP HQ, branches, and CPs would be connected. The software entity, TCCP is shown to link various CPs in different locations.



TCCP: The Core Software …

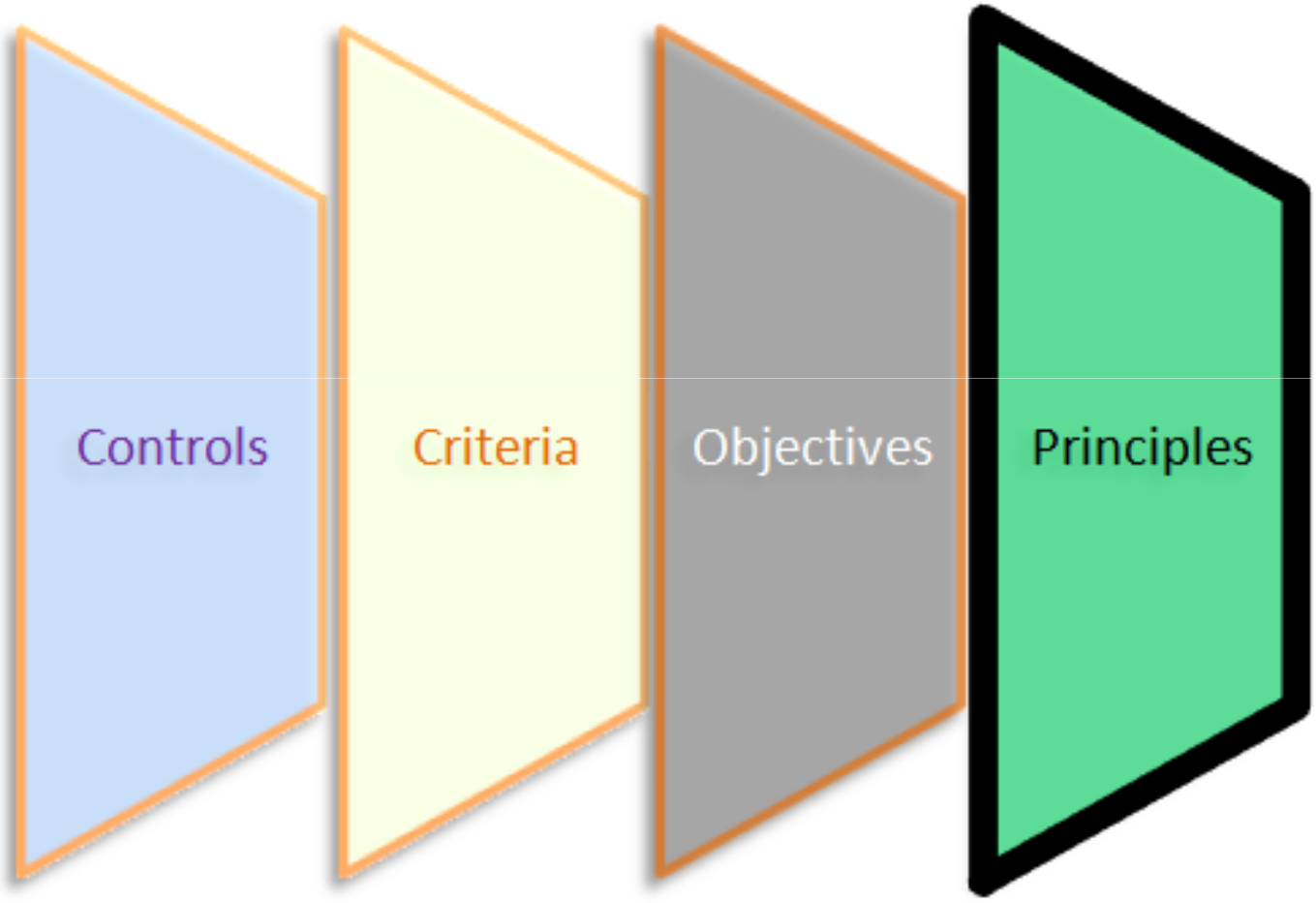
- TCCP is a critical software that is the essence of trust and security assurance in our model.
- Because, if a CP gives a third party any permission to access the data through the network, TCCP could monitor that and record the communications to report to the ICMCCP HQ.
- This software would also be able to detect the outside attackers.

Certificate Giving Procedure

- ICMCCP Certificate Giving Procedure
  - Step 1. First, the CP will send a letter to the Headquarter of the ICMCCP that it needs an ICMCCP certificate.
  - Step 2. After step one, a technical team from the HQ would be sent to the applicant's company to assess the application CP's systems, devices, security tools, etc.

Ensuring Internal Trust of CP

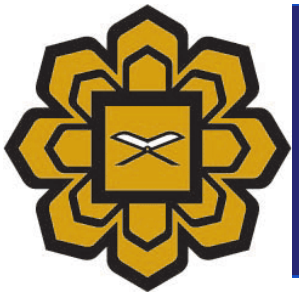
Figure 2: CP's internal trust



Three Important Principles

- Building Customer Trust – CP's Internal Integrity
  - Great Service Matters
  - Consistency Breeds Harmony
  - Transparency is Clear

Adams, M., "Three Ways To Build Customer Trust," Forbes Magazine, 22 April, 2014. Available at: http://www.forbes.com/sites/yec/2014/04/22/three-ways-to-build-customer-trust/ [last accessed on 26 July 2014]

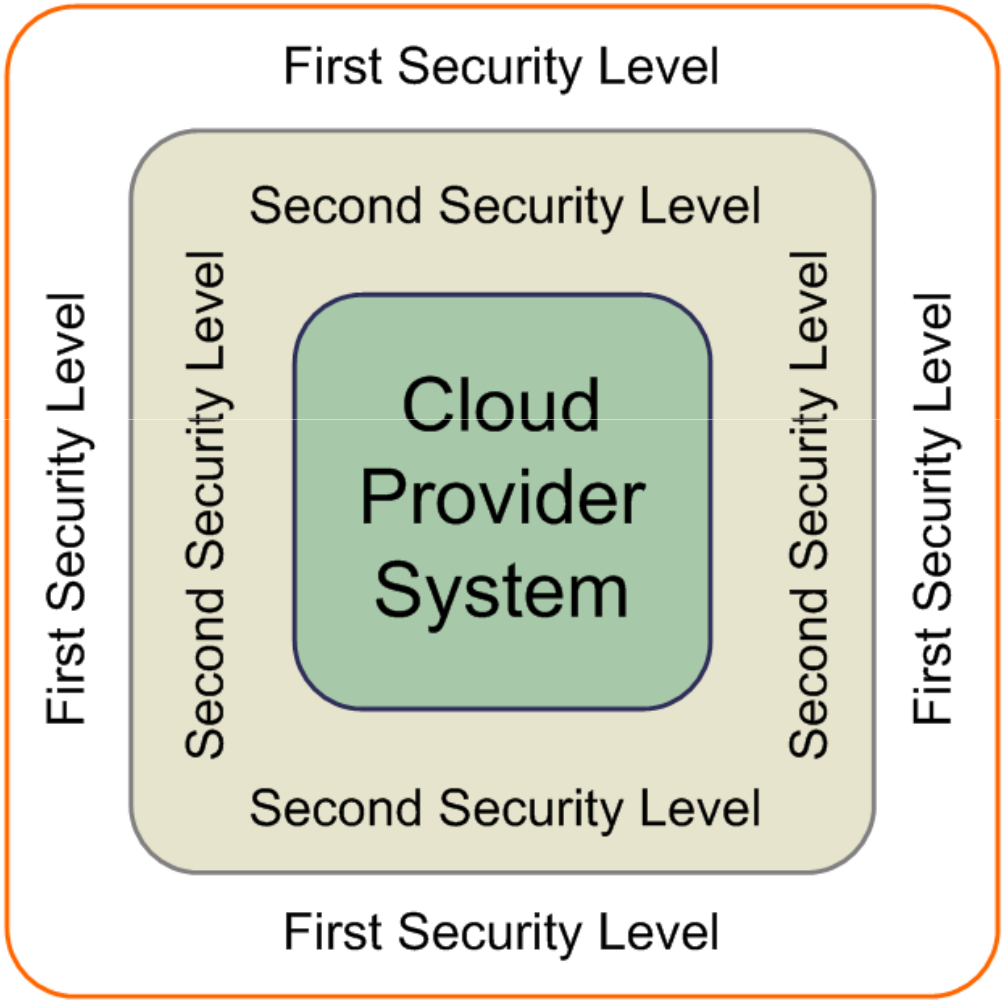


Security Levels

- Security and Operational Model of TCCP
  - There is a critical relation between trust and security of any computing and communications system.
  - There would be two levels of security,
    - **The First Security Level** - We will install the TCCP in the network-level for each CP. This type of TCCP is called TCCP Network-based. Any interaction in a Cloud Provider network-level will be captured by the TCCP.
    - **The Second Security Level** - We will install the TCCP in the Host-level for each CP as well. This level is called TCCP Host-based. Any interaction in the Host-level will also be captured by the TCCP.

Security Levels …

Figure 3: TCCP Security Levels.



Practical Constraints and Issues

- Potential Security Breach
  - The security levels would well-protect the computing resources and communications via the networks.
- Practical Issues of Company Hegemony
  - A practical issue is the large companies' hegemony. Since, ICMCCP gives a general label or certificate to all types of companies/organizations, renowned and powerful companies may like to establish their own network of monitoring and verification. However, as ICMCCP is not associated with any specific company, it would be more desired to the users.

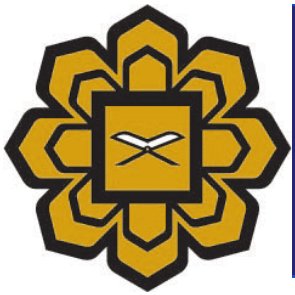
Final Words and Future Scopes

- We have basically dealt with the concept - policy making issues with little technical details.
- We suggest the ICMCCP as a professional and regulatory association for the advancement of cloud computing field.
- While this work is exploratory in nature about the possibility and scope of thinking in this line, there would be many other technical and practical constraints raised by experts that need to be solved in future.
- Hence, our work opens the door of many different discussions and directions of research.

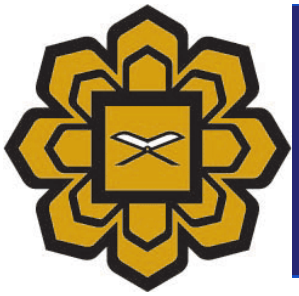
Two Main Source Papers

- Al-Sakib Khan Pathan and Mohssen M. Z. E. Mohammed, "*Building Customer Trust in Cloud Computing with an ICT-enabled Global Regulatory Body*", **Wireless Personal Communications**, Springer. [To Appear]

- Mohssen M. Z. E. Mohammed and Al-Sakib Khan Pathan, "*International Center for Monitoring Cloud Computing Providers (ICMCCP) for Ensuring Trusted Clouds*", **The 11th IEEE International Conference on Autonomic and Trusted Computing (ATC-2014)**, December 9-12, 2014, Ayodya Resort, Bali, Indonesia, pp. 571-576.



THANK YOU



Questions and Answers

Any query should be directed to:

sakib@iium.edu.my , sakib.pathan@gmail.com

???