Security & Privacy Issues in Mobile Cloud Computing

Manmohan Chaturvedi[1] , Sapna Malik, Preeti Aggarwal and Shilpa Bahl

Ansal University, Gurgaon- 122011, India

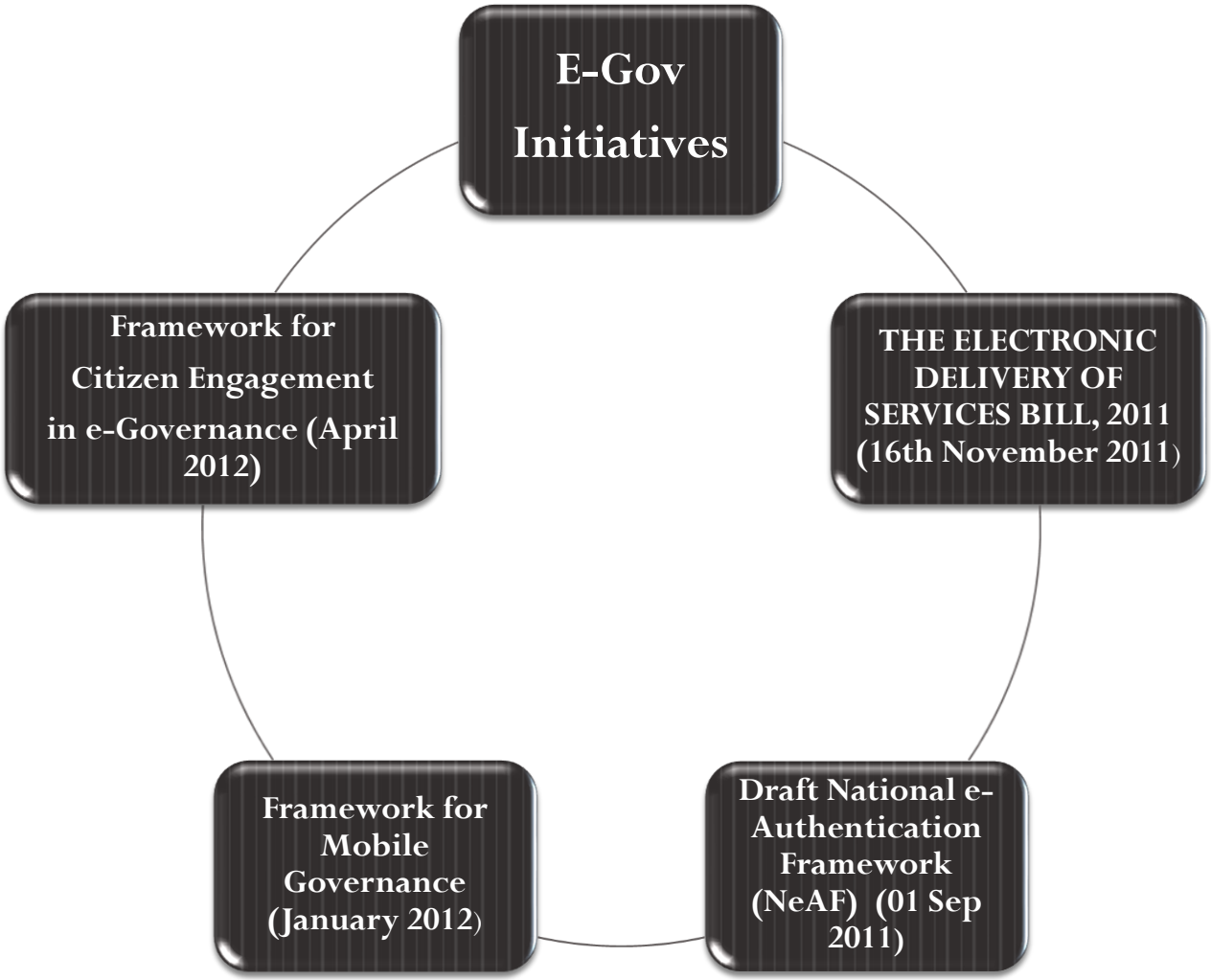
[1]mmchaturvedi@ansaluniversity.edu.in

Indian Context

- The potential uptake of the mobile computing in tandem with cloud paradigm offers possibilities that can spur a huge market in developing Indian economy

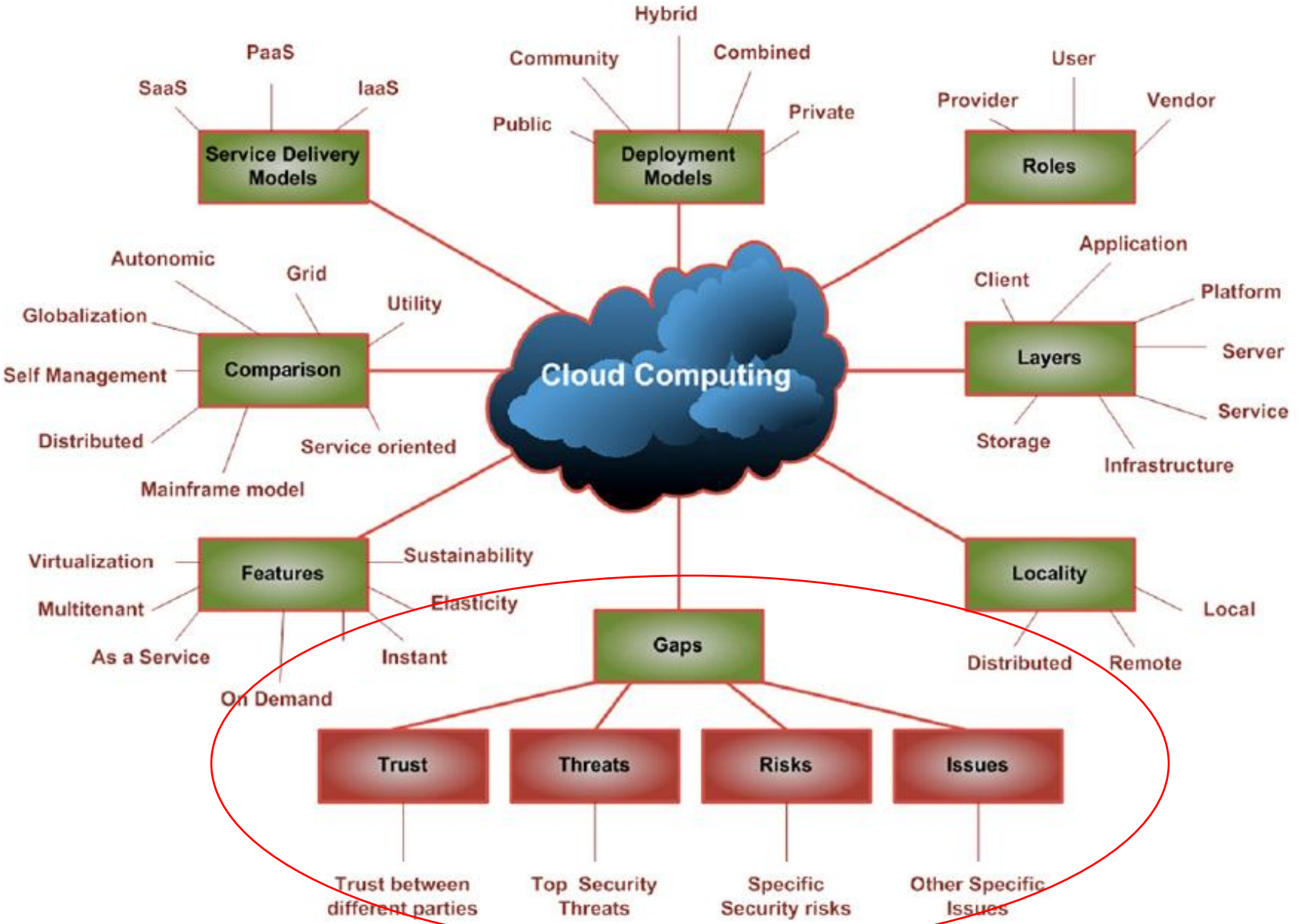
- However, the privacy and security concerns because of the necessity to store data at remote locations seem to be an inhibitor for both corporations and individuals

Evolving Government Policy

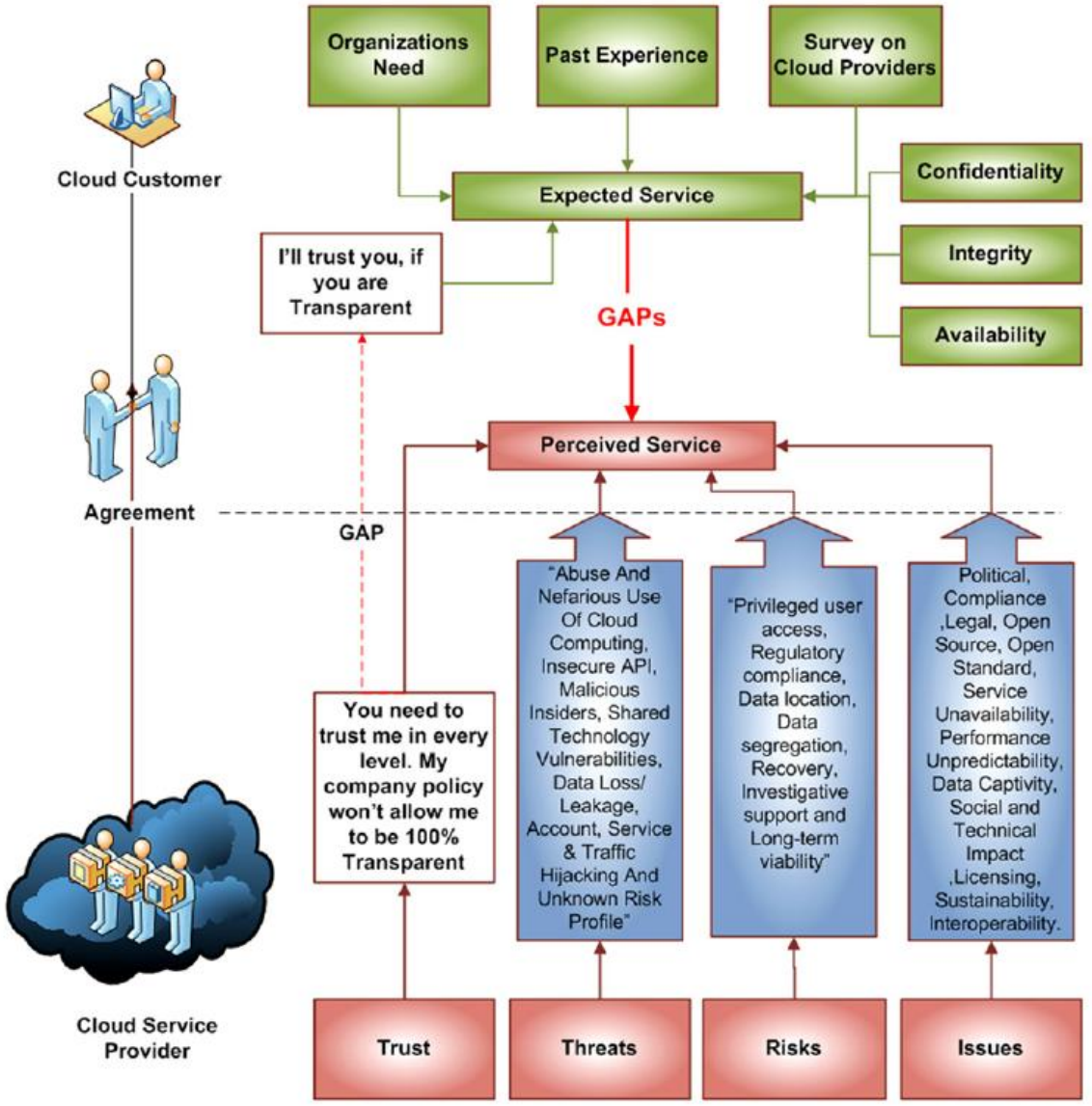


Cloud Computing Paradigm

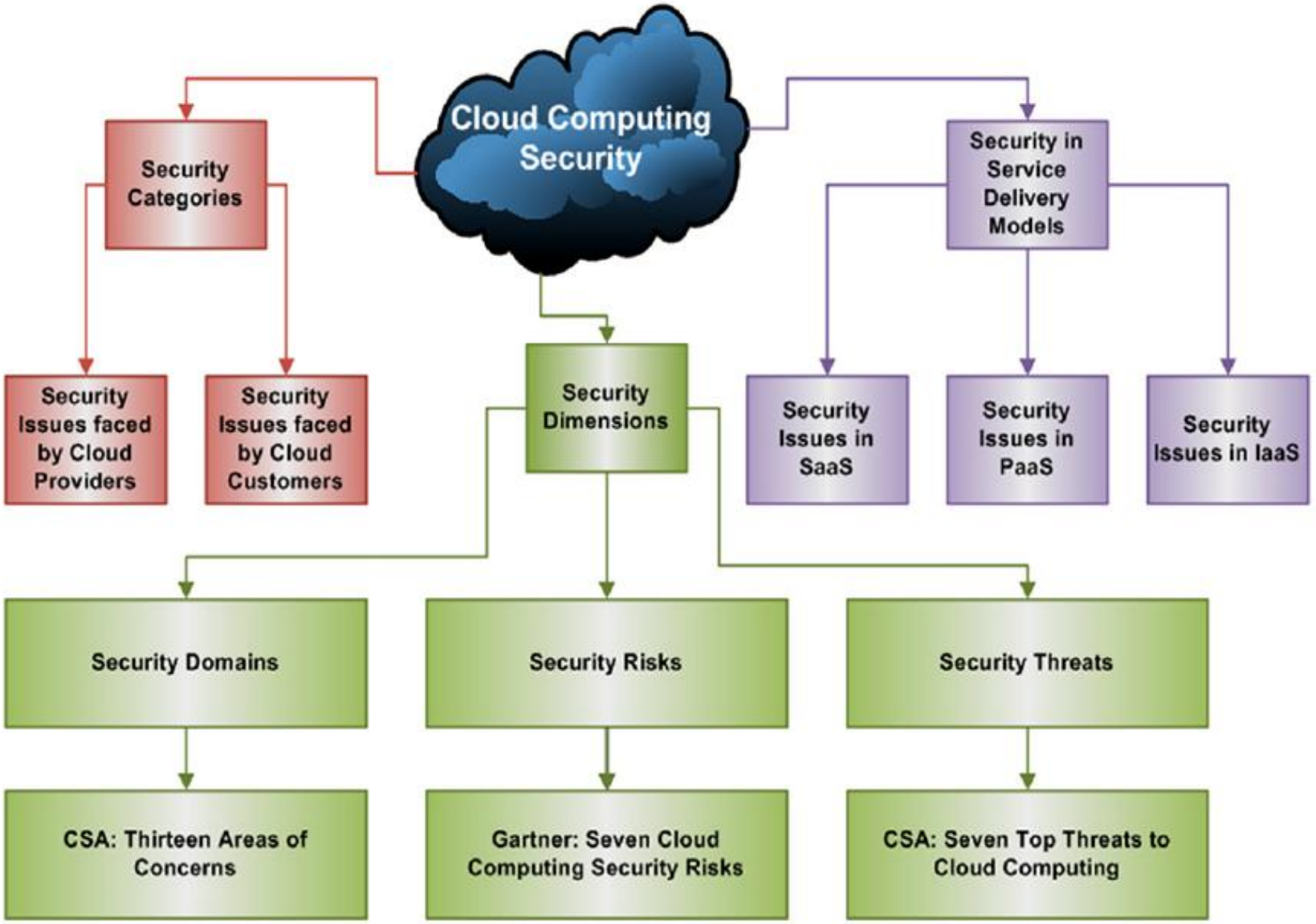
(Md.T. Khorshed et al,2012)



Cloud computing gaps (Md.T. Khorshed et al,2012)



Cloud computing security (Md.T. Khorshed et al,2012)



Mobile Computing Challenges

- Mobile devices being battery powered, have limited processing power, low storage, less security, unpredictable Internet connectivity, and less energy

- It is difficult to enforce a standardized credential protection mechanism due to variety of mobile devices.

- The aforementioned limitations of mobile devices are always obstacles for computationally intensive and storage demanding applications on a mobile

Mobile Cloud Computing (MCC) Paradigm

- To augment the capability, capacity and battery time of the mobile devices, computationally intensive and storage demanding jobs should be moved to cloud

- Careful planning is required before offloading the jobs on a cloud server by considering the network conditions and communication overhead to make offloading beneficial for mobile users

Needed Eco-system

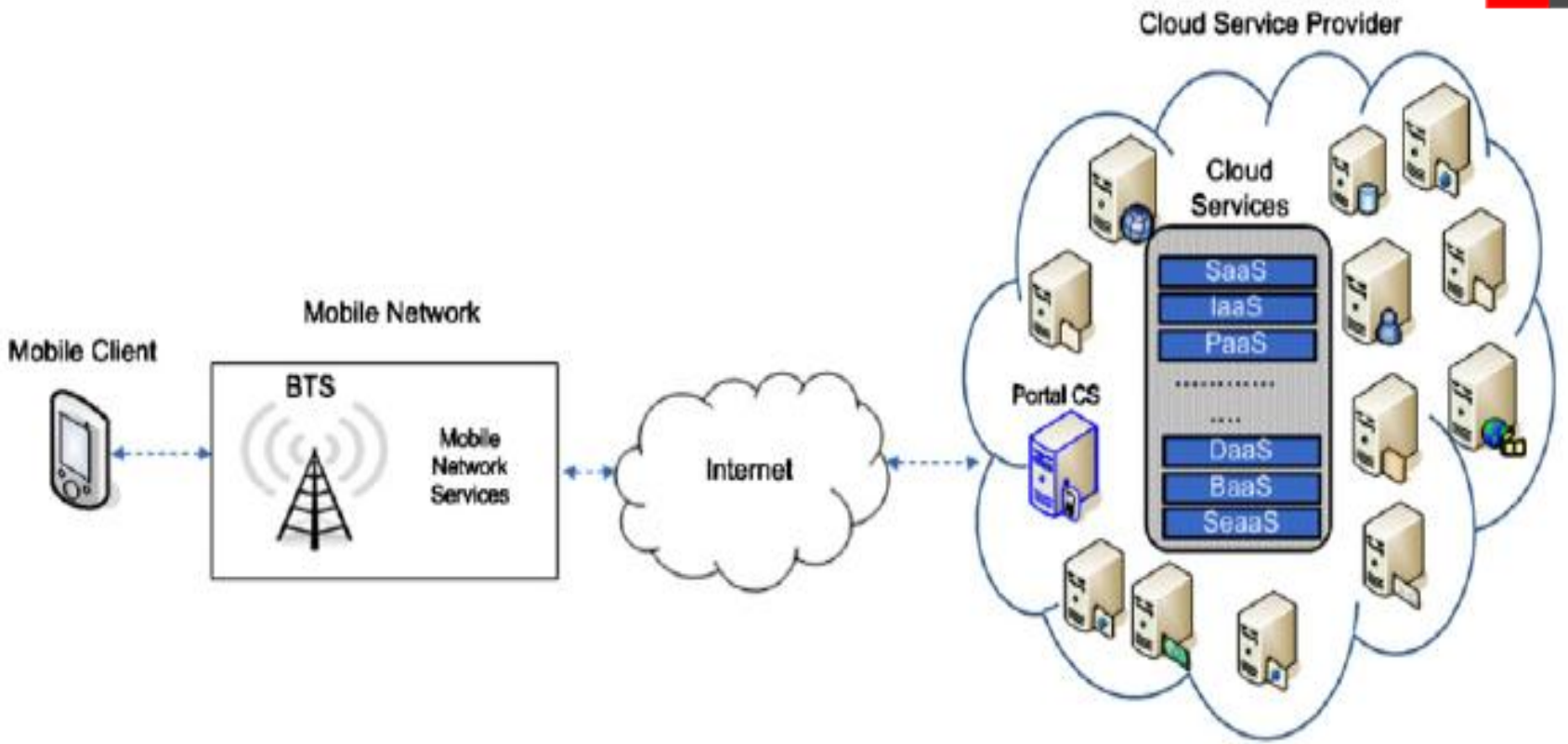
- There is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices.
- There is need to develop a security framework by making perfect balance between cost of Cloud usage and energy usage in mobile device for providing security.
- The security and privacy protection services can be achieved with the help of secure cloud application services.

Needed Eco-system (Contd)

- There is need to develop security framework according to different trust level of cloud server and type of cloud server.
- There is a need for a secure communication channel between cloud and the mobile device.
- The most challenging aspects in MCC are guaranteeing user privacy and the provision of mobile application security that uses cloud resources.
- In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users

Mobile cloud computing architecture (A.N. Khan et al.,12)

A.N. Khan et al. / Future Generation Computer Systems (doi:10.1016/j.future.2012.08.003



Mobile Cloud Computing(MCC)-Definition

A service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

Mobile Cloud Application-Category

- Client Model-How mobile device access services in the cloud.
- Client/Cloud Model-application is divided into components and distributed between mobile device and cloud.
- Cloud Model-mobile is considered as a part of cloud and used as integral part of cloud by exploiting its storage and computing capacity by sharing it in cloud.

Security Framework for MCC

- Data Security framework-Secure User's Data stored in cloud

- Application Security Framework-Secure Data & Computation in cloud for Mobile User.

Evaluation Criteria for Data Security Framework

- Basic Theory-mathematical principal or cryptographic principle
- Data protection-on mobile or on cloud
- Scalability-can cope up with increasing no of users without degrading performance of security framework
- Assumption- fully trusted semi trusted or distrusted cloud server.
- Data Access-provide automated or semi automated encryption of file
- Authentication of originator of user's files on cloud

Evaluation Criteria for Application Security Framework

- Application type
- Security Features.
- Assumptions
- Scalability
- Cloud server-single node or distributed nodes

Security services on different layers (A.N. Khan et al.,12)


Mobile Device 1


Mobile Device 2


Mobile Device 3

Secure Cloud Application Services

Privacy Protection	Data Integrity Verification	Authorization	Authentication	Content Security
Key Management	User Management	Encryption On Demand	IDS	.....

Application Layer
Platform Layer
Infrastructure Layer

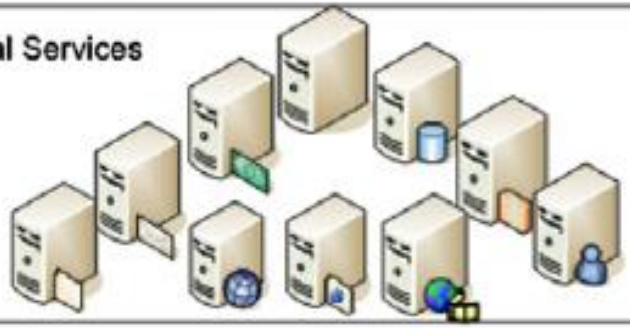
Secure Cloud Process Hosting Services

VM Secure Segregation	VM Secure Monitor	VM Secure Mirror	VM Secure Migration	VM Isolation
Cloud Service Monitor	Storage Security Verification	Risk Evaluation	Audit	.....

Infrastructure Layer
Supervisor Layer

Secure Cloud Physical Services

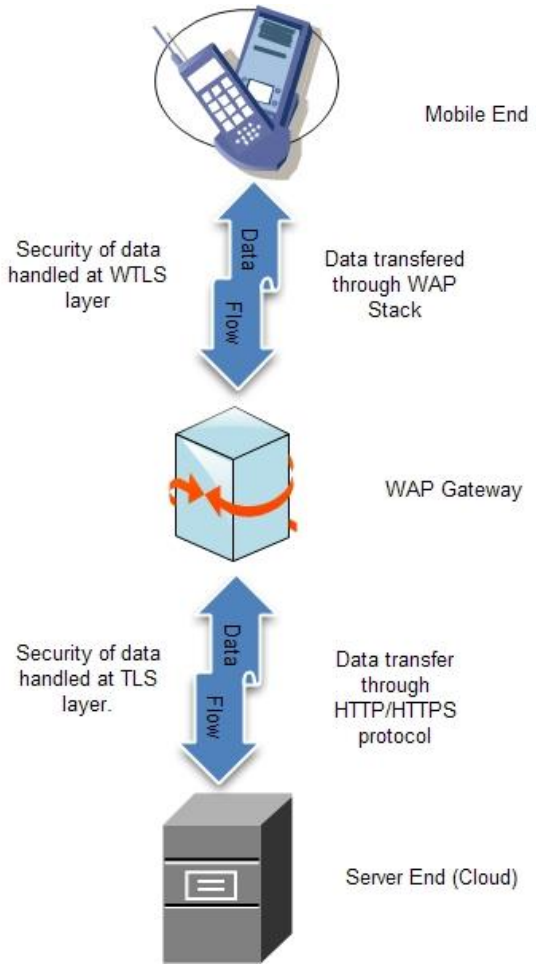
Physical Surveillance	Video Surveillance
SENSOR & ALARMS	Emergency Communication



Backbone Layer

Layout Of Communication

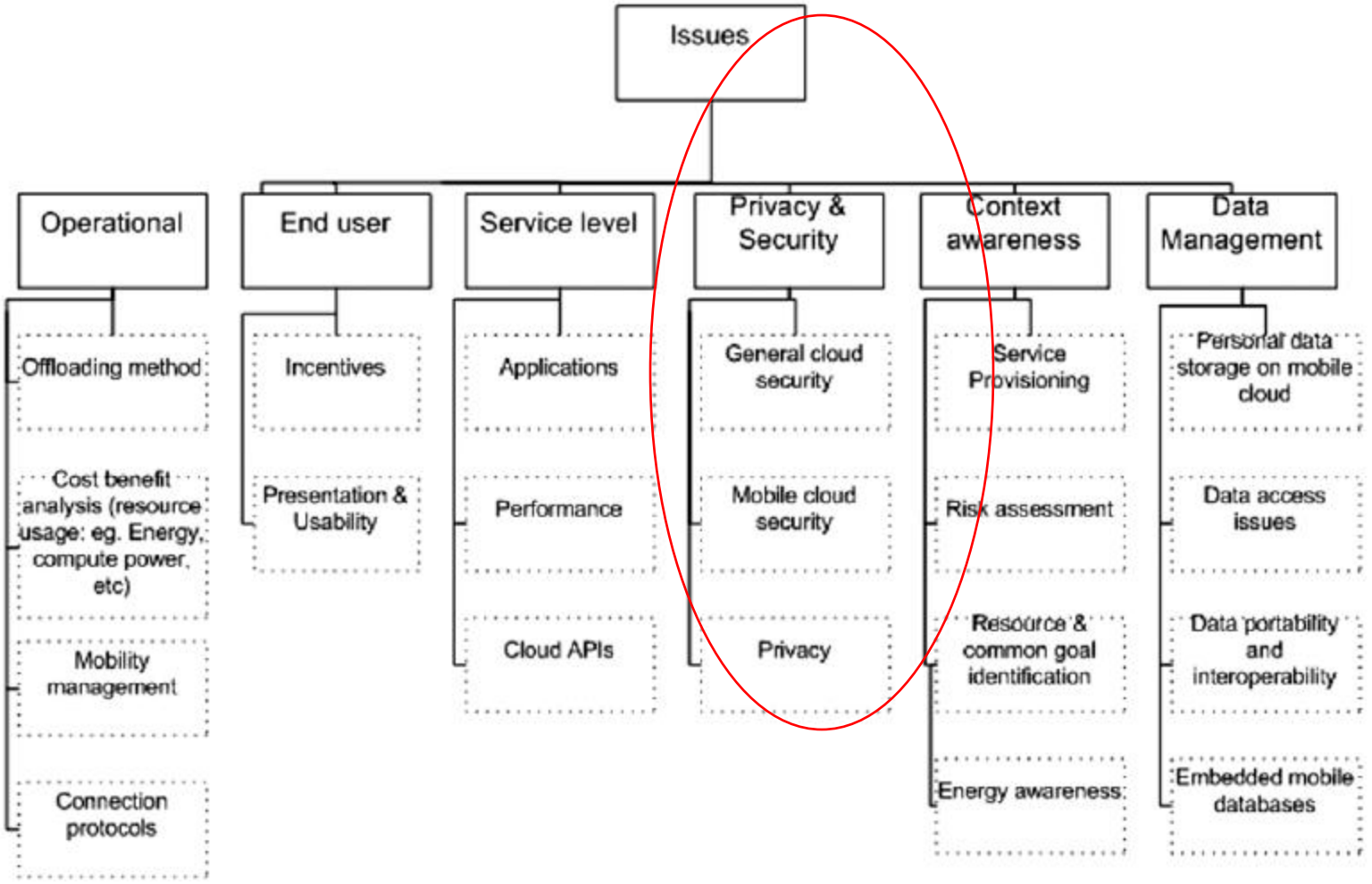
- Mobile End
  - Low End with limited power and Computational ability
- WAP Gateway
  - Act as a bridge between WAP protocol and HTTP/HTTPS protocol.
- Cloud Server
  - Server end, highly efficient for computation and memory rich.



Objective of proposed research

- Our Research objective is to propose and develop an application security framework for client/cloud/cloudlet model in which security algorithms can be decided for a mobile entity dynamically in using Software as a Service (SaaS) delivery model .
- We will be focusing on not just the mobile security parameters but also on the cloud security related issues and respective parameters to the extent they impact security of user data

Proposed research as part of taxonomy of issues in mobile cloud computing (Fernando,2012)



The key illustrative areas of proposed research

- Preparation of semantic data for security parameters
- Cloud Security attributes
- Mobile Security features and respective parameters
- Security algorithm under different security requirements
- Platform Independent Security Architecture.

Possible Research Questions

- What could be semantic data for mobile and cloud security?
- How the Protocol Selection Procedure can be made intelligent with option for static protocol selection when necessary?
- How workload could be partitioned between mobile and cloud after factoring various related issues?

Possible options to be explored

- Trusted third party assuring specific security characteristics within a cloud.
- Identification of appropriate security parameters for a mobile and cloud.
- Dependency matrix of these parameters to metric security of a mobile cloud computing application.
- Generation of semantic data to facilitate selection of the security protocol by the middleware.
- Intelligent protocol selection process would help conserve resources. This would permit use of already selected protocol if the semantic data values are unchanged.

Proposed Validation Approaches

- Application security testing
- Governance Risk Compliance (GRC) testing
- Latency Testing

Key Challenges in proposed research

- During experimentation the simulator being used should acquire necessary information from both the OS and through the wireless medium.
- Balance between security and maintaining communication quality and system performance.
- We should provide a single security layer for different contexts of hardware, software and communication modes.

Key Challenges in proposed research (Contd)

- Need for the data semantics so as to determine different sensitivity levels of the data being transmitted, facilitating strong security mechanism only when they are actually needed rather than on the whole data.
- In the proposed approach , appropriate metrics and the parameters should be defined, to facilitate objective evaluation.
- Design of a Platform Independent Security Architecture, so that we can deploy lightweight part of security Framework on any Mobile device, without interface issues.

Concluding Remarks

- The proposed research would attempt to leverage the output of the doctoral research work of the co-authors in this domain

- Any collaboration on the proposed research can be suitably coordinated by Ansal University, Gurgaon, India

Thanks