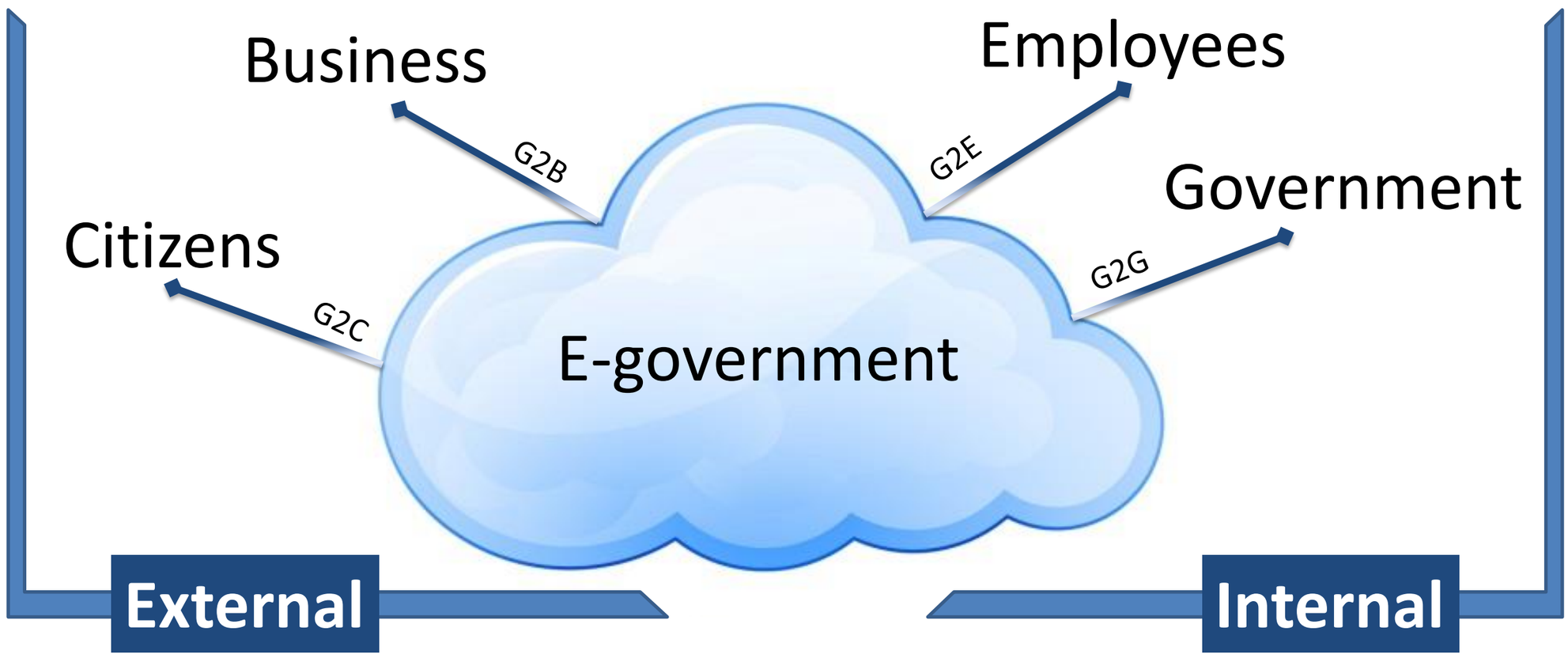
A comprehensive model for evaluating e-government security

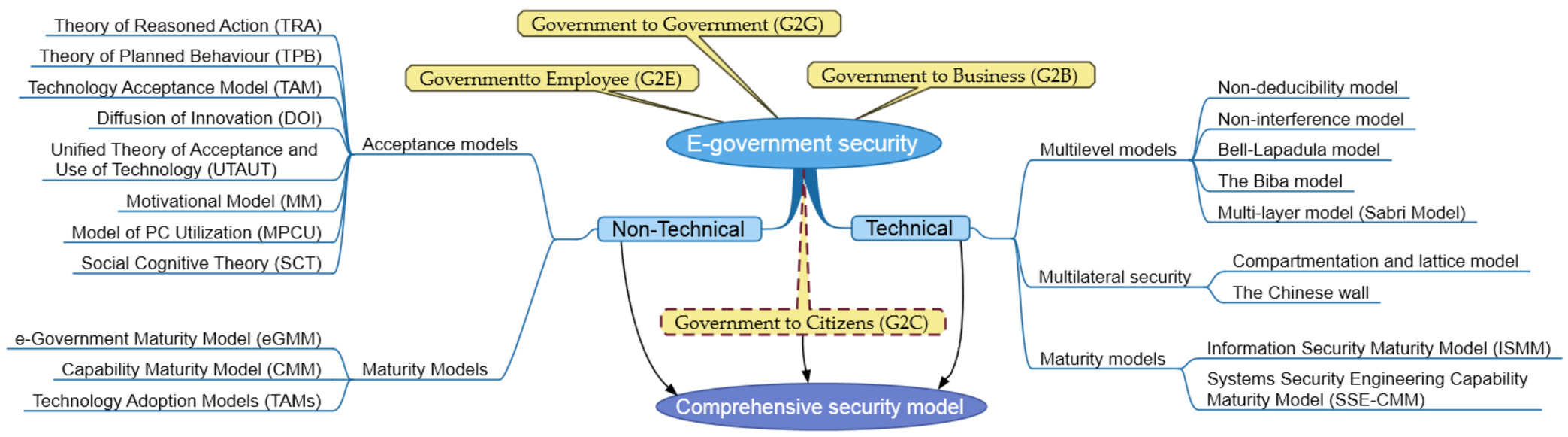
Nawaf Alharbi
PhD student at Centre for Security, Communications and Network Research, Plymouth University
Email: nawaf.alharbi@plymouth.ac.uk

Introduction

E-government is defined as a way to improve the quality of government services and to encourage greater participation in democratic processes, by using innovative ICT technologies . However, the adoption of e-government is often slowed down by the lack of trusted and secure medium for the authentication of users. In addition, several security risks, such as confidentiality, integrity, non-repudiation and controllability have been identified.



Current existing models and theories



Objective

Creating a comprehensive model is highly needed. This model will take the most useful features of current models together with new approaches and it will cover missing elements that were not covered before. This new model will also consider additional issues (beyond the current models) that relate specifically to G2C and it will contain all security aspects (technical and non-technical). Heads of government departments will be more confident about the level of e-government security by applying this model and it will help them to make a right decision.