ABSTRACT

The rapid growth in the size and variety of Internet Services has made the task of optimally configuring, deploying, and executing an Internet Service challenging. The thesis proposes a model for this. The basic model is structured as a sequence of identical execution stages with a stationary random request pattern as input with the added facility of accommodating overloads when needed. Different service rules as well as differentiated services are implemented in the system through a new data structure '*Tokens-Basket*' (bounded QUEUE) added over and above the server's service architecture. Different Internet Service architectures can be realized with the model and studied. Capturing Quality of Service (QoS) parameters specified in Service Level Agreement (SLA), identifying dominant ones amongst them, QoS enhancement, monitoring metrics, evolving strategies, and implementing them are all facilitated here. The utility of the model is demonstrated by mapping an E-Commerce application to it and analyzing its performance through simulation. Providing well-conditioned services is enabled by the model.

The present sophistication level of hackers demands authentication schemes to be based on more than one factor. Evaluating multi-factor authentication solutions particularly at times of peak loads on server requires a look at the measures like security and scalability of the technology, hurdles to user adoption, cost, and deployability.

The thesis presents a scheme that performs a comprehensive multi-factor authentication process based on QR-Code based OTP. The scheme satisfies the important requirements including friendliness, resistance to various kinds of sophisticated attacks and stolen credentials. Further it enhances the availability of Internet Services mainly at times of peak loads.