Abstract

With the exponential growth of the internet users, the demand for better performance, high scalability, dynamism of contents, increasing size and complexity of the web pages have placed heavy load on the web servers. This work presents a systematic study of performance, scalability and security mechanisms of contemporary web server systems based on their architecture (multi-threaded and event-driven) and implementation space (kernel-space and user-space). Using inductive methodologies, a detailed comparative performance analysis of various web servers, on different platforms, for varying types of workloads have been performed. Web servers host different categories of workloads, some of these workloads demand high computational resources and heavy database processing, which makes the load of a web server even more critical. The performance of the web servers under study, while running such compute and database retrieve intensive applications programmed in various dynamic web programming languages, has been analysed on different underlying operating system platforms. The results obtained have been validated by fitting them in a multi variate linear regression model. Several web server architectures reported in the literature have been investigated. A study detailing upon the performance of these architectures on single and multiprocessor environments has also been reviewed. Scalability of a web server is influenced by the architecture of a web server software and/or web server cluster. Having motivated by this fact, scalability of web server architectures have been evaluated by scaling-up and scaling-out the servers on a cluster web server system. Servers were scaled-up by adding more processor cores to the server node and scaled-out by adding more server nodes to the cluster. A novel hybrid architectural model for web servers has been proposed, implemented and evaluated against the web servers under study for various workload types. The results have been validated with a strong experimental evaluation. The demand for high performance and scalability has also raised the issue of having best security mechanisms in-place to secure a web server system. A security mechanism is a precaution/policy/procedure/configuration option that is used to secure a system against attacks by avoiding known vulnerabilities. Finally, an
approach to identify, evaluate and compare the security mechanisms for web servers has been presented. A case study for the comparison of security mechanisms in-place for the web server installations under study has also been performed. All the results presented in this thesis have been validated with a strong experimental evaluation