

## Model-based system architecture for preventing XPath injection in database-centric web services environment

### ABSTRACT

Web services have become a powerful interface for back-end database systems. It is a self-describing component that can be used by other applications in a platform-independent manner. However, along the benefit of Web services, comes a serious risk of security breaches. Most web services are deployed with security flaws and these vulnerabilities make them exposed to XPath (XML Path Language) injection. This kind of attack can cause serious damage to the database at the backend of web services. This paper proposes a system architecture for prevention mechanism against XPath injection attacks within web services. The prevention mechanism employs the model-based approach to detect malicious queries and prevent them before they are executed on the web services backend database. This approach uses runtime monitoring to check on the dynamically-generated queries and compares them against the statistically-built model.

**Keyword:** Database security; Non-deterministic finite automata; Static analysis; Stored procedures; Web services; XPath injection