Many are interested in adopting cloud computing technology, but have concerns about the security of their data. This issue has motivated extensive research to address potential vulnerabilities, with a major focus on access control. A related cloud computing concern is controlling what users can do with data to which they have been granted access. A need for this control, called usage management, has led to a number of conceptual approaches for both conventional and cloud computing, all of which will require an enforcement mechanism within the processor’s domain. The goal of this research is to prove that it is possible to implement a completely software-based enforcement mechanism that can operate independently of the application software. The implementation is based on a formal operational model. A number of implementation approaches were considered in formulating the enforcement strategy. Then, leveraging software instrumentation capabilities and extending tools developed for taint analysis, we developed a software-based usage management enforcement mechanism that uses dynamic data flow tracking. Based on usage flow policies that are
specified in machine readable licenses, the enforcement mechanism can permit or inhibit data flows to standard interfaces, data files, and network sockets. The enforcement mechanism does not require direct access to any hardware, so it can be used very effectively in a cloud computing environment. This demonstrated capability now provides information owners an ability to control what authorized users can do with the information.