Performance Evaluation of Fingerprint, Auto-Pin and Password-Based Security Systems in Cloud Computing Environment

Authors : Emmanuel Ogala

Abstract : Cloud computing has been envisioned as the next-generation architecture of Information Technology (IT) enterprise. In contrast to traditional solutions where IT services are under physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This is due to the fact that the systems are opened to the whole world and as people tries to have access into the system, many people also are there trying day-in day-out on having unauthorized access into the system. This research contributes to the improvement of cloud computing security for better operation. The work is motivated by two problems: first, the observed easy access to cloud computing resources and complexity of attacks to vital cloud computing data system NIC requires that dynamic security mechanism evolves to stay capable of preventing illegitimate access. Second; lack of good methodology for performance test and evaluation of biometric security algorithms for securing records in cloud computing environment. The aim of this research was to evaluate the performance of an integrated security system (ISS) for securing exams records in cloud computing environment. In this research, we designed and implemented an ISS consisting of three security mechanisms of biometric (fingerprint), auto-PIN and password into one stream of access control and used for securing examination records in Kogi State University, Anyigba. Conclusively, the system we built has been able to overcome guessing abilities of hackers who guesses people password or pin. We are certain about this because the added security system (fingerprint) needs the presence of the user of the software before a login access can be granted. This is based on the placement of his finger on the fingerprint biometrics scanner for capturing and verification purpose for user's authenticity confirmation. The study adopted the conceptual of quantitative design. Object oriented and design methodology was adopted. In the analysis and design, PHP, HTML5, CSS, Visual Studio Java Script, and web 2.0 technologies were used to implement the model of ISS for cloud computing environment. Note; PHP, HTML5, CSS were used in conjunction with visual Studio front end engine design tools and MySQL + Access 7.0 were used for the backend engine and Java Script was used for object arrangement and also validation of user input for security check. Finally, the performance of the developed framework was evaluated by comparing with two other existing security systems (Auto-PIN and password) within the school and the results showed that the developed approach (fingerprint) allows overcoming the two main weaknesses of the existing systems and will work perfectly well if fully implemented.

Keywords : performance evaluation, fingerprint, auto-pin, password-based, security systems, cloud computing environment