ABSTRACT

In this era characterized by rapid technological innovations, mobile devices such as tablets and smartphones have become inevitable due to the variety of services they offer. As a result, computing capacity as well as storage needs of these devices are increasing tremendously. To ensure users continue to enjoy the portability, flexibility and accessibility that these devices continue to provide, there is need for a secure and user friendly data storage solution. However, despite the benefits of this technology, there are increased risks to the information that is accessible from the mobile devices. The main problem is the risk of private and confidential data being exposed to unauthorized persons and the risk of permanent loss or damage of that data. These problems are escalated by the fact that most information is stored in the devices' internal memory, making them easily accessible. Mobile devices are susceptible to loss and the pins and patterns used as security controls are easy to by-pass because they have minimal encryptions. In the event of human error whereby the user forgets to delete downloaded confidential content from cloud-based platforms, it remains in the mobile device from where it can be accessed easily. This creates a need for secure ways of storing data in a cost-effective and convenient manner. The objective of this study was to design, implement and validate a secure cloud based approach for mobile devices' user data. The study adopted design and development methodology which followed the entire design and development process from analyses to evaluation. From this methodology, the research employed the strategy of mixed method using a systematic process of collecting data, at first during prototype and then throughout the rest of study. This method allowed for continued development and implementation of the product. The solution was prototyped in an android based environment and developed using Java programming language together with MySQL for the database. The mobile data privacy solution proposed by this study provides a security solution to users to be able to store sensitive data and access it on their mobile devices. The solution focuses on securing the data on the mobile devices by storing it in an encrypted format and uploading it to the cloud. In addition, the downloaded data is timed to self-destruct after user consumption, eliminating unauthorized person or application from reading the information without a decryption key. The developed solution was able to provide security for the users' confidential data while making it available. The tool enabled its users to store the selected sensitive files from their mobile devices in an encrypted format. To achieve this, we used the algorithm AES 256 to encrypt the data with a key only known to the user and upload it to the cloud for secure storage. The secure mobile tool was developed and fulfilled the requirements specification successfully. It met all the security parameters stated hence optimizing mobile user data storage security.