Abstract

User authentication is a method for authenticating a user. It is conducted by another party that communicate with the user. Usually, the authentication is done using verification of username, password, and biometric. There was a method proposed by Seung .et.al where the user authentication process was done using biometric (fingerprint) and password. However, the authentication can be succeeded by authenticating the user based on the password or the fingerprint. Thus, a fake user who knows the password of the legitimate user may be authenticate as the legitimate user without examining the fingerprint. Besides, the time complexity of the previous method for authentication process is high. Furthermore, there is opportunity of fake authenticator device for obtaining the fingerprint and password of the legitimate user because there is no authentication process for examining whether the device is the legitimate one. This problem can be solved using Elliptic Curve and Keccak Hash Function. The Elliptic Curve is used for conducting device authentication for examining whether the device is a legitimate one, while Keccak Hash Function is used for improving the user authentication process, such that the authentication process can be succeeded only if both password and fingerprint is authenticated. The result of experiment shows that the user authentication processing time decreased 35.06 ms - 41.6 ms compared with the method proposed by Seung .et.al, while the probability of obtaining the fingerprint and password using the proposed method is less than the previous method of 2^{-57}. It is proven that the proposed method is strong against fake device attack for stealing the biometric information and password.

Keywords: Authentication, Elliptic Curve, Keccak Hash Function.