AN ANALYSIS OF SYSTEM SECURITY VULNERABILITIES TOWARDS ENHANCING AUTHENTICATION TECHNOLOGIES IN COVID-19 ERA

Conference Paper · May 2022

CITATIONS
0

READS
102

3 authors:

Boniface Mwangi
Mount Kenya University
8 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Joyce W. Gikandi
Mount Kenya University
37 PUBLICATIONS **1,423** CITATIONS
SEE PROFILE

Geoffrey Wambugu
Murang'a University of Technology, Kenya
26 PUBLICATIONS **59** CITATIONS
SEE PROFILE

2nd International Conference on Peace, Security and Social Enterprise. Mount Kenya University May2022

Sub-theme 6: Cyber Crime & Security

Link to Books of Abstract: https://cgsr.mku.ac.ke/2nd-international-conference-on-peace-security-and-social-enterprise-book-of-abstracts/

AN ANALYSIS OF SYSTEM SECURITY VULNERABILITIES TOWARDS ENHANCING AUTHENTICATION TECHNOLOGIES IN COVID-19 ERA

Boniface Mwangi Wambui
School of Computing and informatics
Mount Kenya University
Thika, Kenya.
Email:bonniemwangi91@gmail.com

Joyce W Gikandi
School of Computing and informatics
Mount Kenya University
Thika, Kenya.
Email: jwgikandi@mku.ac.ke

Geoffrey Mariga Wambugu
School of Computing and Information Technology
Murang'a University of Technology
Murang'a – Kenya
Email:gmariga@mut.ac.ke

John Kamau
School of Computing and informatics
Mount Kenya University
Thika, Kenya.
Email:jkamau@ mku.ac.ke

Abstract

The purpose or objective of this study was to examine the security weaknesses of existing systems as well as the internal dynamics that make them vulnerable to cyber-security attacks and then propose a better security system to help overcome the obstacles. There are a lot of vulnerabilities in the current systems due to an increase in spoofing attacks on the sensors. Furthermore, due to the physical touch nature of most authentication systems, they have been rendered useless with the outbreak of covid-19. Identity theft, spoofing, and the trustworthiness of authentication systems in higher education institutions are only a few of the major concerns jeopardizing system integrity and impeding excellent service delivery. Biometric systems have been applied in several areas such as education institutions, banks, and hospitals for authentication purposes. The use of biometric security techniques has been widely adopted in higher education institutions to monitor class attendance. These systems are increasingly being integrated into the webbased Management information systems thus increasing their vulnerability to spoofing. Moreover, existing biometric

systems are inadequate to authenticate the credentials of system users when they attempt to clock in. The False Rejection Rate of biometric technologies is high. Such issues highlight the inefficiency and ineffectiveness of the biometric system, jeopardizing its integrity and dependability. The success or failure of a biometric system is governed by a number of factors and application areas. Contactless authentication is one method that can be utilized to overcome these obstacles. Within the higher education context, this research adopted a mixed methodological approach and an experimental research design to analyze existing security models and then build a security model that offers contactless authentication and enhanced security from spoofing attacks. The new model exemplifies more reliable, safe, and secure systems. Based on 61.8% of the respondents, the current biometric system can be hacked which was more than 50% of the respondents while 34.1% of the respondents ascertained that there was no way in which it could be hacked and 1.6% were not sure whether it could be hacked. R2 of 73.4 % indicates that the data fit the model well in the assessed factors that influence the integrity of biometric systems because it is greater than 50%. The security systems model meets the criteria of a system that can improve data integrity, according to 87.5 % of the experts. Aliveness detection system such as the non-contact access palm vein security system should be used to overcome the challenges experienced or using cancellable biometrics, biometric cryptosystems, and steganography and watermarking. There is additional work to be done in this subject in order to develop an effective and flawless security solution.

Keywords: *Authentication, Biometrics; security; contactless; integrity; spoofing;*