engineering proceedings

MDPI

Proceeding Paper

Integration of Cyber-Security Locks with SCADA Software for Smart Surveillance Management [†]

Duaa Ayesha *, Tayyaba Iqbal and Ghulam Asghar

Mechanical Engineering Department, Capital University of Science and Technology (CUST), Islamabad 44000, Pakistan; tayyabaiqbal7724@gmail.com (T.I.); ghulam.asghar@cust.edu.pk (G.A.)

* Correspondence: duaaayesha68@gmail.com

[†] Presented at the Third International Conference on Advances in Mechanical Engineering 2023 (ICAME-23), Islamabad, Pakistan, 24 August 2023.

Abstract: Due to the augmented engrossment of technology in security, everything moves towards a cohesive system. Smart cyber-lock technology is one of the eminent concepts with the potential to solve emerging safety and security issues. This work aims to establish an efficient system of safety and security through the integration of smart cyber-locks with a software package. The smart monitoring and evaluation of security-intensive sites are accomplished through cyber-link software, and the audit reports of security processes are generated on a quarterly basis. The comparative analyses of the case study data represent that the illegal security breaches decline quite noticeably after the successful implementation and synchronization of cyber-security locks with SCADA software.

Keywords: cyber-lock; cyber-security; cyber-link; surveillance; smart technology; monitoring and evaluation

1. Introduction

Cyber-locks are known as key-centric access control systems considered to increase security, liability, and authorized control of a system. The inimitable design of electronic-lock cylinders and programmable smart-keys of cyber-locks resolve the security difficulties that no other scheme can [1]. Cyber-audit is a software that is used in project security management and allows for the assignment of keys by setting expirations and staff monitoring, audit trails, access schedules, and custom reports. It manages the schedules with administrative and customized access to the individuals who hold a key in the concerned department. The generated output is used to create custom audit reports with email notifications for specific events. The questions of when, who, and why are evaluated through data analysis using an authorized identification process [2].

The Internet of Things (IoT)-enabled door lock system is used to manage automation and has various advanced features. This smart-door locking system has the ability to open and close the door through an authentication process [3]. Another study [4] addressed the intelligent door lock system built on raspberry Pi (RPI). The system was synchronized with Android and Java (enterprise edition) EE to scan the concerned persons' fingerprint data as the input interface, and RPI cameras were used for the process of monitoring in the door lock. Hadis et al. [5] demonstrated that the dependence related to the access is reduced with the control over the server in a cyber-lock system. Attributes are set that have the role, date, location, and fine-granted control for the access permissions.

The application and usefulness of cyber-locks have been addressed by numerous studies; however, there is a scarcity in research focused on the synchronization of smart-locks with software for efficient vigilance. Therefore, this study would attempt to integrate cyber-locks and SCADA (supervisory control and data acquisition) software for the proficient monitoring and enhancement of the security of an asset.

check for updates

Citation: Ayesha, D.; Iqbal, T.; Asghar, G. Integration of Cyber-Security Locks with SCADA Software for Smart Surveillance Management. *Eng. Proc.* **2023**, *45*, 17. https://doi.org/10.3390/engproc2023045017

Academic Editors: Mohammad Javed Hyder, Muhammad Mahabat Khan, Muhammad Irfan and Manzar Masud

Published: 11 September 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

2. Methodology

This research scheme is divided into two parts: (i) monitoring and (ii) evaluation. Cyber-link and SCADA software are managed in parallel for the synchronization of results. For the live monitoring of sites where cyber-locks are installed, the SCADA system is controlled and managed from the control room of the parent organization. Default parameters are set in SCADA through which non-stop (24/7) data monitoring is accomplished. The SCADA is operated through the telecommunication signals, so if any signal issue occurs, its modem stops the communication. Due to this issue, the SCADA software requires a reset, and an ON-SCAN alarm is produced for enduring the communication process. On completion of the reset, the SCADA is again managed from the control room and further developments are performed. Cyber-link software is checked and analyzed in parallel after every scheduled activity of the site.

The interface of cyber-link software is divided into three main portions for the monitoring process, as depicted in Figure 1. All data related to cyber-locks are communicated over the software that is checked and analyzed through three main sections. The first is about the display of a cyber-lock activity report, in which complete details of each activity over the site are noted with the proper date and time marked. The second section is related to the history of key/lock attempts performed over the site. The third section is associated with the access chart, as it shows the key assignments to the concerned lock and person. Only the concerned person with their unique key could open the lock; otherwise, an alarm is produced due to unauthorized attempts, in case any other/invalid key is inserted in the lock.

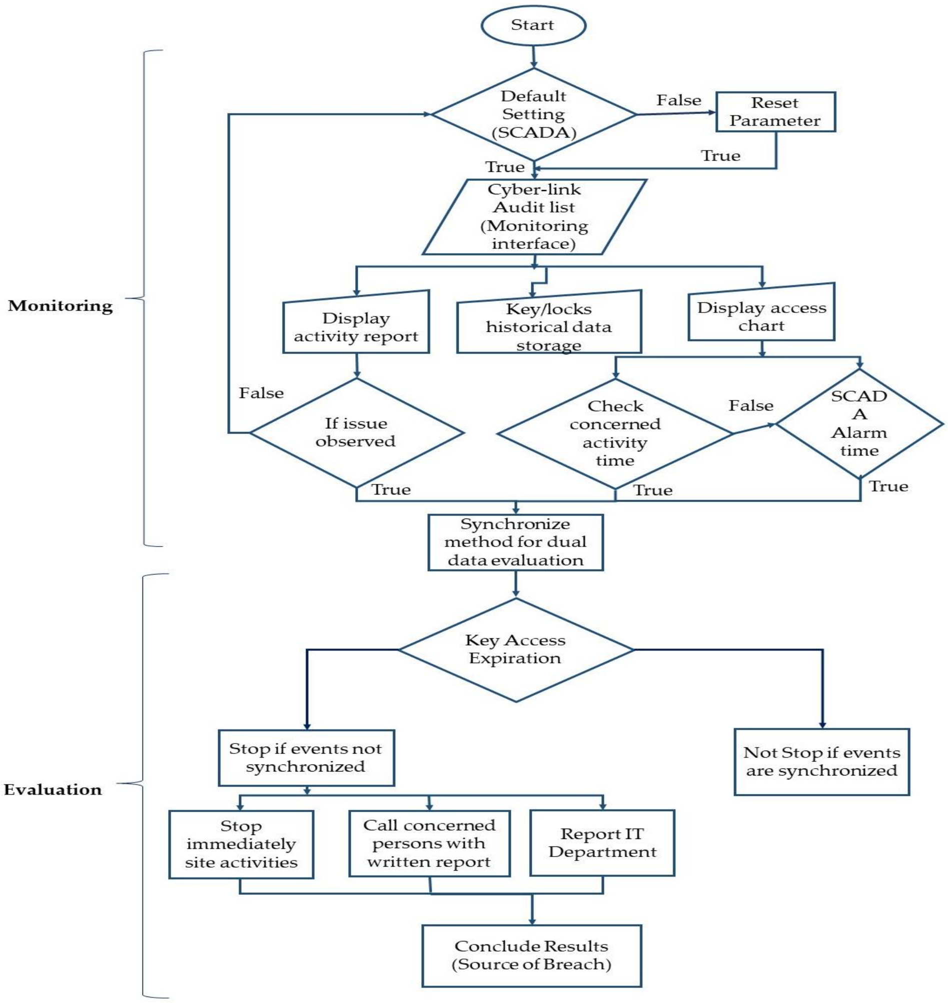
Start
Default Setting (SCADA)
False
Reset Parameter
True
True
Cyber-link Audit list (Monitoring interface)
Monitoring
Display activity report
Key/locks historical data storage
Display access chart
False
If issue observed
Check concerned activity time
False
SCAD A Alarm time
True
True
True
Synchronize method for dual data evaluation
Key Access Expiration
Stop if events not synchronized
Not Stop if events are synchronized
Evaluation
Stop immediately site activities
Call concerned persons with written report
Report IT Department
Conclude Results (Source of Breach)

Figure 1. Flow chart of monitoring and evaluation process.

In case of an issue observed in an activity report, prompt action is taken by checking the access chart. Through an access chart, the two situations are analyzed in parallel by checking the concerted activities' times, both in the cyber-link and SCADA (alarm time). Both of them are synchronized; hence, the data evaluation process is accomplished. Through data analysis, a security breach is checked out, and as a result of this, key access is finalized. If any type of security breach is observed in the data, the following three steps are performed: (i) The organization reports to the IT department to check other parameters and security breaches for the clearance of other activities. (ii) The concerned supervisor is immediately called to stop the site activities without any delay. (iii) Written evidence is mandatory from the concerned person of the site and consumer; otherwise, the issue is not resolved. By examining all the results, if an issue is identified and then the responsibility is fixed regarding the breach source, the key for the concerned zone is stop If no issue is noticed and/or the issue is resolved at the same time, then the site activities are sustained without any interruption.

3. Results and Discussion

The quarterly audit data of five sites were used to analyze the results of breaches before and after the cyber-locks' synchronization with SCADA software. Additionally, three types of security breaches were observed: user premises access, cyber-attacks, and human error, as shown in Figure 2.

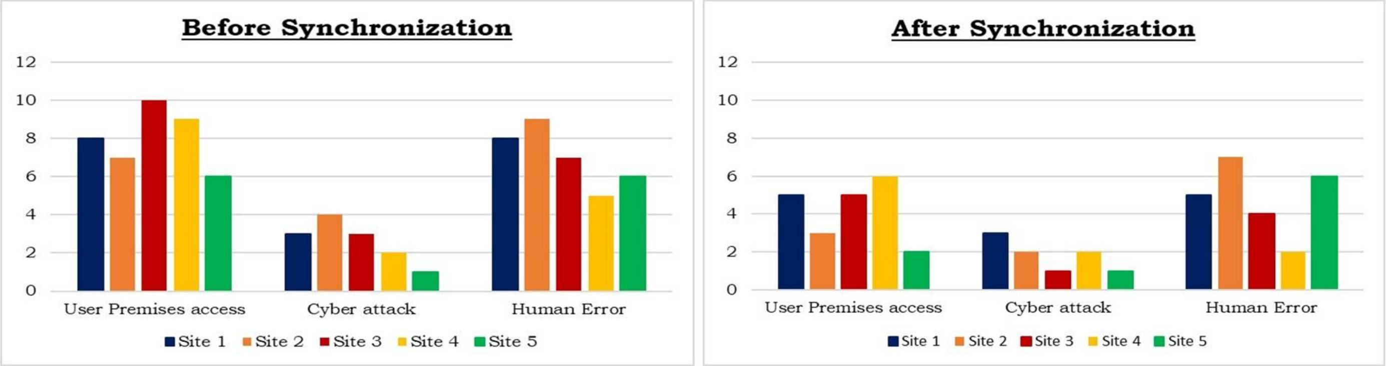

Figure 2. Results of security breaches before and after synchronization of cyber-link and SCADA.

User premises access attempts were large in number before the synchronization of cyber-locks and SCADA, as site supervisors approached the system easily and made physical changes on the site without any fear of being caught. However, after the installation and synchronization of cyber-locks and SCADA, user premises access without notice became very difficult, and more than one access in a day required written permission. Cyber-attacks happened on modem data and other site systems; hackers tried to gain access to site data. Cyber-attacks were also managed successfully without compromising on security because consumers and supervisors were both alerted after the synchronization of the system. Human errors occurred mostly due to the reset issue of the modem and other systems installed over the site. Team members neglected some issues during the troubleshooting and routine work on the site. Due to the negligence of supervisors and other team members, human errors were faced before the synchronization of the system. It was observed that human errors were also reduced to some extent after the modification of the system but not completely. The comparison of all security breach data in Figure 2 represents that the user premises access was reduced quite significantly, from 40 to 21, whereas the cyber-attacks and human errors were also decreased, from 13 to 9 and 35 to 24, respectively.

4. Conclusions

The comparative results of this study encourage security-intensive organizations to adopt cyber-security locks to enhance the safety and security of their assets. Through the implementation and synchronization of cyber-link and SCADA, security breaches were reduced to a significant extent. User premises access breaches were controlled properly, due to which site issues were decreased and efficient surveillance was maintained. Illegal approaches to the site by the employees of an organization or outsiders became difficult and incidents of security breaches were also minimized.

Author Contributions: Conceptualization, methodology: D.A.; investigation, resources: T.I.; writing—original draft preparation: D.A.; writing—review and editing: G.A.; visualization: T.I.; supervision: G.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bjartmar Hylta, S.; Söderberg, P. Smart Locks for Smart Customers?: A Study of the Diffusion of Smart Locks in an Urban Area. Master Thesis, School of Industrial Engineering and Management (ITM), KTH, Stockholm, Sweden, 2017.
2. CyberAudit-Web Management Software. Available online: https://cyberlock.com/product-lines/cyberaudit-web/ (accessed on 10 July 2023).
3. Adiono, T.; Fuada, S.; Anindya, S.F.; Purwanda, I.G.; Fathany, M.Y. IoT-enabled door lock system. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 445–449. [CrossRef]
4. Zhang, X.; Song, M.; Xu, Y.; Dai, Z.; Zhang, W. Intelligent door lock system based on raspberry Pi. In Proceedings of the 2021 2nd International Conference on Artificial Intelligence and Information Systems, Chongqing, China, 28–30 May 2021; pp. 1–7.
5. Hadis, M.S.; Palantei, E.; Ilham, A.A.; Hendra, A. Design of smart lock system for doors with special features using bluetooth technology. In Proceedings of the 2018 International Conference on Information and Communications Technology, Yogyakarta, Indonesia, 6–7 March 2018; pp. 396–400.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.