REVIEW OF INTERNATIONAL GEOGRAPHICAL EDUCATION

ISSN: 2146-0353 ● © RIGEO ● 11(7), SPRING, 2021

www.rigeo.org

Research Article

A Development of Cyber-Physical Intelligent Model Based Multi-factor authentication of un authorised device for Insider Attacks

Ridhwan Rani[1]
Faculty of Technical And Vocational Education
Universiti Tun Hussein Onn Malaysia, MALAYSIA
mridhwan@uthm.edu.my

Munirah Ahmad Azraai[2]
Faculty of Technical And Vocational Education
Universiti Tun Hussein Onn Malaysia, MALAYSIA
munirahaz@uthm.edu.my

Raja Mariatul Qibtiah[3]
Department of Electrical Engineering
German Malaysia Institute, Jln Ilmiah, Tmn University, MALAYSIA
mariatul_qibtiah@gmi.edu.my

Hairun Nisa Daud[4]
Department of Electrical Engineering
German Malaysia Institute, Jln Ilmiah, Tmn University, , MALAYSIA
hairunnisa@gmi.edu.my

H.Imran[5]
Faculty of Technical And Vocational Education
Universiti Tun Hussein Onn Malaysia, MALAYSIA
imranh@uthm.edu.my

S.M.Zulfadhli[6]
Faculty of Technical And Vocational Education
Universiti Tun Hussein Onn Malaysia, MALAYSIA
zulfadhli@uthm.edu.my

Abstract

This study focuses on cybersecurity threats, including data breaches caused by trusted individuals. In some cases, outsiders posed as trusted users, possibly through phishing, to gain valid credentials and access an organisation's system. In the meantime, data breaches also occur when employees of an organisation intentionally leak sensitive data. Due to the malicious intentions in both situations, they cause a security gap where the users' authenticity, specifically, whether they are the real owner of the accounts or some hackers, are questioned. In this sense, data breaches remain a major threat to this day. The Cy-Phy Pro possess a detection system that could prevent data breaches. It is based on the OWASP Top 10 list, which ranks web application security concerns that make them vulnerable to such attack. The system uses physical device detection to identify suspicious behaviours of a trusted user with the possibility of malicious intent to exploit organisational assets. Once the system detects unauthorised device use, it starts screenshotting the latest activity and capturing webcam images of the user. The information is compiled to alert the administrator via email when an intrusion is detected. The evidence will be saved in a folder that is automatically synchronised to cloud storage. Hence when an intruder tries to delete traces of evidence, the administrator could still view it in the cloud and remotely. The system is also capable of whitelisting certain devices. This is useful for PC owners as the system could recognise the authorised device owned by the authentic user. Furthermore, the framework facilitates multi-factor authentication and a time-based one-time password technique to examine the intrusion logs and protect the information saved in the intrusion log database.

Keywords

Cybersecurity, Cyber Physical, Insider Attacks, Threat, Network Security

To cite this article: Rani, R, , Azraai, M, A, Qibtiah, R, M, Daud , H , N, H.Imran[5] , and S.M.Zulfadhli, (2021) Intelligent System Of Duo Functional Bagpack. *Review of International Geographical Education (RIGEO), 11*(7), 601-611. doi: 10.48047/rigeo. 11.07. 60

Submitted: 10-10-2020 ● **Revised:** 14-12-2020 ● **Accepted:** 18-02-2021

Introduction

Insider attacks are launched by malicious users entrusted with authorised (i.e., insider) access to a system. Insider attacks contribute to 29% of all reported electronic crimes ranging from stealing corporate data to propagating malware, which has caused tremendous damages [1]. The objective of anomaly detection is to detect deviation from a pre-determined model of normal system behaviour. Nonetheless, since an insider has authorised access and extensive knowledge of the victim system, it can be more difficult to separate normal system behaviour from insider attacks than the external ones. Due to this, experimental studies show that many generic approaches for anomaly detection. They suffer from a high false-positive rate which hinders the effective detection of insider attacks. There are also instances of attackers in anomaly detection is or naive attackers. These attackers blindly launch their attacks without the knowledge of the system and historical attacks. Therefore, it is more difficult to analyse their unstable behaviours than their objectives. Most existing studies have focused on inside attackers' behaviour and design new anomaly detection techniques. Unfortunately, this state-of-the-art system has yet to provide a satisfactory solution.

The North American Electric Reliability Corporation (NERC) has ranked protection system failure as the number one cause of power disruptions [2]. Thus, it is critical to identify the root cause of protection system failures to return the system to normal operation. When a component in a protection system fails to perform as intended, functions accidentally, or works outside of its expected protection zone, it is said to be mal-operating. Physical breakdowns or cyber-induced reasons could be to blame for such misbehaviour. Cyber anomalies can raise the risk of operating system damage and defensive systems based on the physical kind of cyber in terms of security breaches. Insider attacks are low-frequency high-impact events. The quest for a screening tool that relies on personality and other characteristics to detect employees at risk of posing an insider threat is understandable but remains unfulfilled. Like other low incidence phenomena, such as workplace violence and suicide, inside attacker profiles suffer from the problem that even a highly sensitive test will yield an unacceptably high level of false positives.

Since cyberattacks can be launched through various cyber and physical interfaces, cyber-physical system security has become increasingly difficult. Traditional cybersecurity measures are ineffective against both internal and external threats. Hence, Cy-Phy Pro is a system that could defend cyber components and data from outside threats. This research focuses on the following challenging situations:

Insider attacker's gain unauthorised access to data.

A USB device is a plug and play device that can store data and transfer them to other devices via a USB port. They have been used for ages, and most organisations are using these devices for data storage. However, there is a serious security concern as these devices do not offer protection against data exfiltration by unauthorised user and insider attacks.

Lack of defence against unsuspecting victims.

Insider threat is one of the most significant threats faced by an organisation. However, even though just one disloyal staff can do catastrophic damage to a company, this threat is often overlooked by organisations. In this regard, organisations often think that investigating these threats makes them seem distrustful and diminishes their staff loyalty. Furthermore, when the data is breached using an unattended PC, the intruder can easily copy the data using a USB device. While the fault falls on the owner for leaving the PC unattended, any staff around the vicinity can also be blamed.

The intrusion made by insiders remains unreported.

While there are many data breaches reported in recent years, there are only a few sources

and evidence indicating data breached via USB device exfiltration. Hence, the only way to find out about these breaches is to through an application with an active USB log.
This study uncovered new research directions in cyber-physical coordinated situation awareness and active defence, which can improve the performance of Cyber-Physical Protector in dealing with cyber-attacks. Cy-Phy Pro aspires to be a first step in safeguarding authorised users against data breaches perpetrated by an insider or an employee within a company. The main demographic for this study comprises small and medium-sized businesses. Section II describes the research solution approach for studying and implementing the concept. Section III discusses the key technologies for infrastructure situation and active defence. The next section, Section IV, validates the performance of cyber-physical through an example of a regional frequency protection system. Finally, Section V concludes the article.

Background

Isnin, S.N & Sedek, M. [3] described an insider threat as a malicious threat to an organisation from people within the organisation, such as employees, former employees, contractor or business associates. These people have inside information concerning the organisation security practices, data and computer system. These threats involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property or sabotage of a computer system. Insider threat is ranked as the most significant cybersecurity issue which threatens government and private information infrastructures. Economic, transportation, communication, energy and security systems, among other systems, are highly reliant on ICT. Small business will be unable to continue their day-to-day operations without access to the current cyber infrastructure. In addition, ICT provides mechanisms for a more efficient and convenient transfer of information. Malaysia is regarded as one of the top ten countries vulnerable to cyberattacks, besides the United States and North Korea. According to a cyber-security expert, Isnin S.N, 65 per cent of organisations in Malaysia are facing risks of cyberattacks. Furthermore, Cybersecurity Malaysia noted that there are10 thousand reports regarding cyber-attack and crimes every year.
Attackers may use different techniques to harm a particular organisation in different ways. It impacts an organisation in different ways like economically, business disruptions etc. There is no specific solution to attack, but the awareness and implementation of policies is the best suggestion to this growing era. When the word of cyber attackers combined is can be defined as the threats from a person with their technique to attack and harm or sabotage something by using the information technology such as the internet, systems and others. Most organisation have their own asset or confidential data and information that need to be protected. All the confidential data, including details of the employees, documentation, design, financial and others. Employees or authorised parties can compromise an organisation's security with their overzealousness in getting their job done. Each organisation has a different mix of employees, consultants, management, partners, and complex infrastructure, making handling insider threats a daunting challenge. Through insider attacks, organisations face potential damage through the loss of revenue, reputation, intellectual property or even human life.

Insider threats and the risks associated are not new to companies in Malaysia. However, most companies choose not to confront the risk openly. They prefer to handle it subtly as they are reluctant to their experience and difficulties dealing with issues related to insider threats. In addition, it is probably due to the fear of revealing that employees within their organisation commit wrongdoings or fraud. This will bring a negative reputation and customer's perception. Such as insider attacks could result in reputation loss to the affected organisation. In 2008, a seminal article was published entitled 'Honeypots: Insider Attack and Cyber Security: Beyond the Hacker' [4]. It mainly discusses the nature and scope of the insider attack problem from the financial industry's perspective. The article inspires an ongoing research initiative to solve some of the vexing problems regarding computer security. These issues include critical IT infrastructure protection, insider threats, awareness, and dealing with nefarious human activities that respect organisations' liberties and privacy policies while providing the best protection of critical resources and services. In this light, insider problem is considered as the ultimate security problem.

Steven M. Bellovin, in his book, stated that "Insider attacks are difficult to detect either by human or technical issues." Neetesh (2020) supported this view and mentioned that controlling an insider who already has access to the company's highly protected data is a very challenging task. Furthermore, insider attacks could potentially bring severe damages to an organisation's finances and social credibility. Hence, there is a need for reliable security frameworks that ensure confidentiality, integrity, authenticity and availability of organisational information assets by including the comprehensive study of employee behaviour. Another study by [5] focused on the existing physical, technical and administrative controls, their objectives and limitations, insider behaviour analysis and future challenges in handling insider threats. These studies provide detailed analyses of insider behaviours that may hinder organisation security.

Threat identification and data protection

S. Rathore's et. al [6] concepts are founded on the most recent available knowledge and data. There are several types of threat identification that are found. First is multimedia content related issues which are concerns regarding shared ownership, manipulation, video conference, tangging and data breach. Second is traditional cyber threats regard to phishing, malware, inference attack and profile cloning. Then, social threats as well as threat classification that are concerns about cyber bullying and grooming, cyberstalking rumours, fake news and terrorizing people. Last that are to be found is web application related issues which are broken access control, eavesdropping and malicious application permission dialog [7].

For the cyber physical issues, included in a group of traditional cyber threats. An attacker can access information about a client's regular savings range and login password, among other things, by employing certain tricks. This article describes the important ones. Attack by inference due to the nature of social networks, a large number of connected friends and other users can also serve as an excellent source of information about a particular individual. Certain works demonstrate that it is possible to check a user's friend list and the information they provide about the user in order to obtain a complete set of a person's traits and attributes [8] [9]. As a consequence, they are exposed to transactions that may result in cyber physical attacks against the contact.

Another serious threat that has been discovered is the attack on profile cloning. Thus, the attacker can take advantage of the victim's identity, reputation, image, and so on. Cloning of aggressive profiles additionally, attackers can download images and files from other accounts and pass them off as their own. For instance, YouTube frequently steals and reposts videos without obtaining appropriate permissions in order to increase clicks and views. Not all of this information is reported, and when similar profiles are used, indigenous users may become confused. In reality, this method can involve a great deal of danger. After researching the victim's individual and business profiles, the perpetrator can physically steal the data by posing as an employee who is considered knowledgeable about the ins and outs of the perpetrator's business. This is considered as an intrusion of the organizations such as businesses and individual in terms of security precautions [10].

Proposed Solution Approach

In recent years, there has been an increase in the number of protection systems that aren't working properly. Concerns about reliability have been given significant emphasis [11]. Malicious cyber-attacks have been recognised as one of the possible causes of protection failure. Modern digital equipment is geographically scattered in detecting systems, and their functions are dependent on computerised communication infrastructure. As a result, if the communication protocols are known, expert attackers may use security flaws and vulnerabilities in the software to tamper with confidential documents. Therefore, it is critical to analyse the system's behaviour after the errors occur to recognise and distinguish faults and physical cyber-attacks in such conditions. The Cy-Phy Pro systems consist of three main components:

Application:

Cy-Phy Pro detection system is application-based. It is capable of detecting foreign devices and recognising whitelisted devices. This capability prevents unnecessary false alarm on authorised users and differentiates authorised and unauthorised users with malicious intentions against the organisation. When access is initiated by a foreign device not listed in the white device, the system will begin to capture the image of the intruder and screenshot the latest activity before logging it into the database.

Database:

A database is used to store intrusion & login histories. These logs record the time and date of the intrusion, the details of the host, including the MAC address, IP address, hostname, and lastly, the VSN of the unauthorised USB device. Moreover, the evidence will be synchronised and backed up to the cloud using Google Drive API. This is useful for the administrator to review the situation case by case.

Web Application:

Web applications mainly consist of user authentication before accessing the database of intrusion logs. This is a security feature in the system because we want to avoid data breaches at all costs. The security method implemented utilises Google Authenticator, a time-based one-time password algorithm to authenticate users when they come across the web application. An authorised user may access the database through a multi-factor authentication using login credentials and the display of a customised QR code that generates the link to our web application.

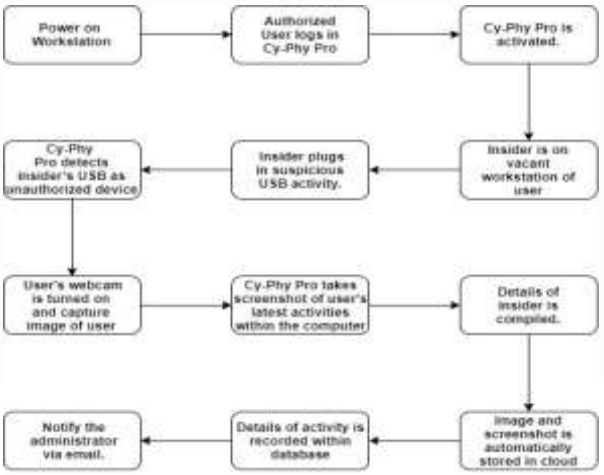


Figure 1. Model Of Cy-Phy Pro's Detection System

The figure above is the block diagram illustrating the processes in the Cy-Phy Pro system when it detects an unauthorised device once the authorised user activates the system through the application. Details of insider refer to the evidence collected by the system. The evidence comprises webcam images of intruders and screenshots of their latest activity. It is compiled and stored in a local file, and the file is automatically synchronised to cloud storage. This is useful in cases where the intruder tries to delete the traces of evidence. The files in the cloud will be stored safely and can be accessed remotely.

Infrastructure For Cyber-Physical Detection

In many instances, information from the physical side of the system can support the detection and tracking of cyber-attacks. Physical security measures can avoid or lessen the risk of cyber-attacks. Hence, thorough research of a coordinated strategy of cyber-physical situation awareness and active protection is necessary.

Phase1: Detect foreign devices.

The detection system can detect foreign devices by programming the application to detect the VSN of each device connected to the PC. If the VSN of a device is unrecognised, the application rules it as an intrusion. For many years, insiders have used USB devices to copy or transfer the victim's files as an exfiltration of data.

Phase2: Whitelist certain devices.

The capability of the detection system is extended by allowing users to whitelist certain devices. This feature is useful to avoid false positive alarms. In other words, there is a recorded list of authorised or approving devices that can access the PC without alerting the administrator. Therefore, the application can whitelist authorised devices and users can add devices through the application.

Phase 3: Capture webcam images of intruder and screenshot their latest activity.

Once the system successfully identifies an unauthorised device plugged into the PC, the webcam will silently turn on to capture the image of the intruder without him/her noticing and screenshot the latest activity. Then the evidence will be stored in a local file. Nevertheless, the system also captures the PC details, such as the date and time of intrusion, MAC address, IP address and the VSN of unauthorised device. All of this information is stored in the database.

Phase 4: Send email notification to the administrator.

After the actions have been carried out, the system sends out an email to notify the administrator regarding an intrusion. Thus, the administrator will be the first to know of an intrusion. This is achieved using a Java mail API.

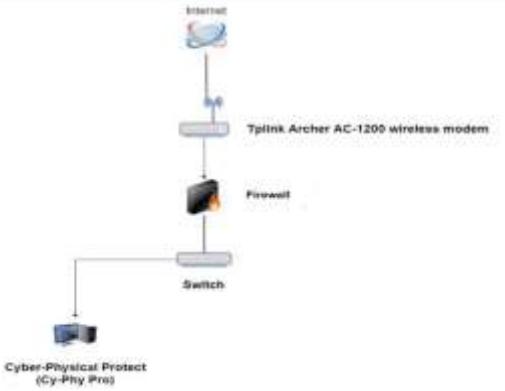


Figure 2. Physical Diagram

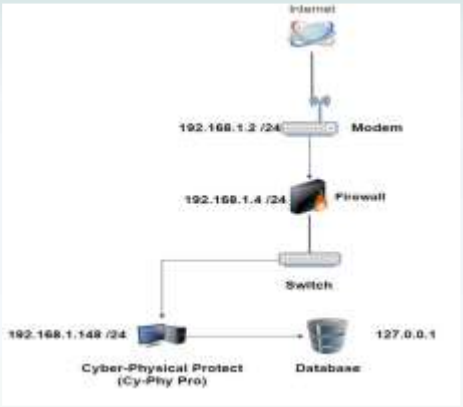


Figure 3. Logical Diagram

The tables above show the illustration of network infrastructure. Since the targeted audience is SMEs, the network infrastructure is constructed similar to a working environment to ensure the product meets future customers' needs. The logical diagram includes the IP address of network equipment used in the network

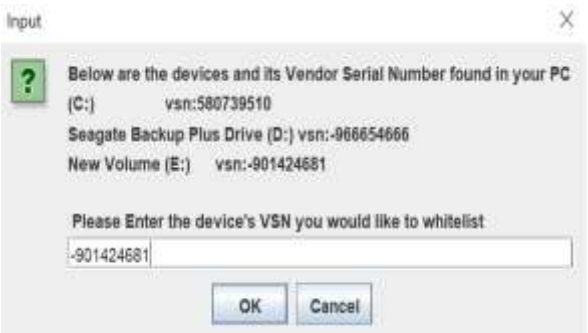
Cy-Phy Pro Safety Constraint

Synchronising to cloud storage :

The detection system will automatically send the captured image and screenshot of the intruder activity to the cloud as a contingency plan and backup. This is useful in case the intruder tries to delete the evidence of the intrusion activity. In addition, the administrator can remotely access the cloud and view the evidence once the administrator is notified of an intrusion via email. This feature helps an organisation detect the culprit when such things like this happen to speed up the investigation process of a data breach.

- The multi-factor authentication in the application starts when a user chooses the 'view history logs' option. Security is a major issue in every step. Hence, MFA is implemented within the application where the user is prompted to enter login credentials then prepare the correct QR code to access history logs. The MFA creates redundancy which is necessary to increase the security layer within the application to protect the database from unauthorised access.
- Time-based one-time password algorithm using Google Authenticator on our web application: The user must install Google Authenticator on their mobile phone. It provides another redundancy layer in the web application and loads an authentication page. It instructs the user to enter the right code from the Google Authenticator mobile application. The code expires every 30 seconds as it is a time-based one-time password algorithm. It generates a temporary passcode with an algorithm based on the current time of day as an authentication factor. This is categorised as an MFA method.

Performance Evaluation And Results



This study has considered the commissioning and testing of this system to evaluate its potential approach. A one-USB device was introduced to allow the PC to detect information among themselves. Finally, simulations were carried out by considering various physical and cyber events.

Detect foreign devices.

The detection system scans for any devices connected to the PC and detects their VSN. Figure 4 and 5 show the results of devices found in the PC as part of the testing system. Then, it detects which of the devices found in figure 5 is an unauthorised device. As shown in figure 4, New Volume (E :) is the culprit.

Figure 4. Test Run To Scan For Devices Connected To Pc

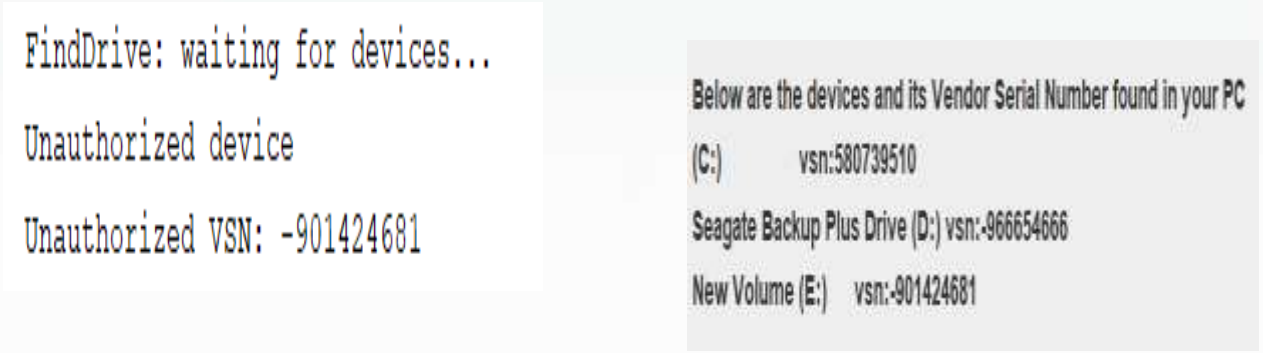


Figure 5. Test Run For Detection Of Unauthorised Device.

- **Whitelist certain devices.**

This feature enables users to enter the device they want to in the whitelist, as shown in figure 6. These whitelisted devices are stored within an array list known as the 'whitelist'.

- Capture webcam images of intruder and screenshot their latest activity.

Once the system detects unauthorised devices from the whitelist, it begins a sequence of action where it turns on the webcam to capture the intruder's images and screenshot their latest activity. These are kept locally in a specially created folder for evidence storage. Figure 7 shows the successful test run of this feature.

Figure 6. Insert The Whitelist Device

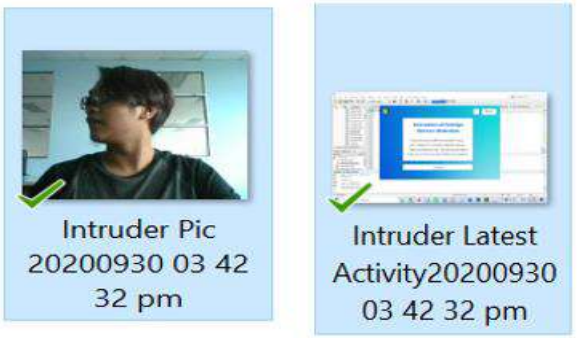


Figure 7. Capture Image Of Intruder And Latest Activity.

- Send email notifications to the administrator.

The last action of the detection system is notifying the administrator via email through the Java Mail API. Figure 8 shows that the administrator has received the email from Cy-Phy Pro.

- Synchronise to cloud storage.

After setting up the Google Drive API, the administrator has to select the destination folder where the evidence is stored and automatically synchronise them to cloud storage. Figure 9 below shows the successful testing of the evidence backing up to the cloud.

Figure 8. Sending Email To Administrator

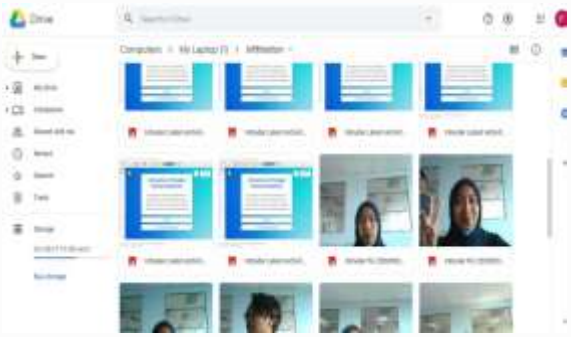


Figure 9. Check The Stored Evidence In Cloud Storage.

A subset of security attack scenarios was identified from all the physical and cyber detection of the Cy-Phy Pro. These scenarios exemplify the trusted user with physical device integration. They are meant to represent a set of relevant and simply reproducible security attack scenarios useful to test the system's response to potential security attacks. Once started, the detection system will search for any unlawful devices. When it senses an incursion, it will go through the steps indicated below and give effective results.

1. Capture the image of the intruder and screenshot the latest activity. The file location of these images is stored at C:\Users\User\Desktop\Intrusion Docs\Infiltration.
2. Gather PC details such as date and time of intrusion, MAC address, IP address, hostname, the running OS and VSN of unauthorised device. It will obtain some of these details except the VSN of the unauthorised device.
3. Record the intrusion and PC details into the database. All the recorded log in the database that was created. Other than that, there is also login history in the Cy-Phy Pro database that records the user login history in the application.
4. Send an email to notify the administrator. The administrator (sent to eerdina@gmail.com) successfully received the email regarding an intrusion that has happened.
5. Evidence is synchronised to cloud storage. The administrator logs in to Google Drive to view the evidence from the victim's PC remotely.

Conclusion

This article describes a data breach and exfiltration approach to monitor a cyber-physical transmission protection system and detect malicious behaviour on the transmission protection system. Physical device detection allows the application to detect suspicious activities of a trusted person with malevolent intent to exploit organisational assets. The key contributions of this work are the implementation of cyber-attack models to simulate protection system mal-operation due to cyber-attacks and the application's ability to make a significant difference in current organisations if implemented on a wide scale. Another purpose of the study is to send an email notification to authorised users when an intrusion is discovered. The proposed technique was validated using a real-time testbed which includes a hardware switch, a cyber-attack model, and a FortiGate 30E series. It provides a fast and secure SD-WAN solution in a compact fan-less desktop form factor for mid-sized organisations. Furthermore, the algorithm on a test system shows that the suggested data breach-based technique effectively diagnoses aberrant transmission protection system operations caused by physical and cyber factors. Lastly, Cy-Phy-Pro could increase the efficiency and effectiveness of catching insider attacks. Thus, while Insider attacks within an organisation are 90% undetectable, the Cy-Phy-Pro requires no excessive security protocol. \This decreases insider attack and helps protect organisations against data breach.

Acknowledgement

Communication of this research is made possible through monetary assistance by Universiti Tun Hussein Onn Malaysia and the UTHM Publisher's Office via Publication Fund E15216.

Recommendation

This project proposes a data breach protection system that can be implemented on a larger scale, such as in an Enterprise workspace like in Fortune 500 companies currently thriving in cities like New York. User registration will allow more users to use the application. The system will become more applicable in bigger organisations. This could increase organisation safety and higher protection against insider attacks. Such effort can potentially save companies billions of dollars against data breach. The next improvement is to allow better access to the intrusion logs. At present, the intrusion log can only be viewed at php My Admin. It would be better for future versions to display the history logs in a web application so that administrators can view the data more easily. This function will also facilitate e seamless search of metadata. Lastly, a better system's flexibility will allow more efficient communication to the users or administrator in terms of notification acceptance. It will help them be more alert of intrusion events place and respond to them.

References

Zhu, Q, Qin,Y., Y. Zhou and C.J, "Hierarchical Flow Model- Based Impact Assessment of Cyberattacks for Critical Infrastructures.," Systems Journal, 2019.

A. Arman, V.V. G Krishnan, S. Armina Foroutan and M. Touhiduzzaman, "Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems," in IACC-0821, Pullman, 2018.

Isnin, S.N. and Sedek, M., "A Review on Insider Threat Status in Malaysian Organization," International Journal of Academic Research in Business & Social Sciences, vol. 8, no. 10, pp. 1208-1215, 16 Sept 2018.

S. M. Bellovin, Honeypots: Insider Attack and Cyber Security: Beyond the Hacker, Columbia: Springer Science & Business Media, 2008.

Neetesh Saxena, Emma Hayes and Elisa Bertino, "Impact and Key Challenges of Insider Threats on Organizations and Critical Business," MDPI electronics, vol. 9, pp. 1460-1469, 2020.

S. Rathore, , P.K. Shamra, , V. Loia, , Y.-S. Jeong, and J.H. Park, "Social network security: Issues, challenges threats, and solutions," Information Sciences, vol. 421, pp. 43-69, December 2017.

Abdul Hamid, Monsur Alam, Hafsina Sheherin and Al-Sakib Khan Pathan, "Cyber Security Concerns in Social Networking Service," International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 2, pp. 198-211, August 2020.

M. Diomidous, , K. Chardalias, , A. Magita, , P. Koutoni, P. Panagiotopoulou, and J. Mantas, "Social and Psychological Effects of the Internet Use," Acta Informatica Medica, vol. 24, no. 1, pp. 66-68, 2016.

R. Heatherly, , M. Kantarcioglu, and B. Thuraisingha, "Preventing private information inference attacks on social networks," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 8, pp. 1849-1862, August 2013.

A. A. Obeidat, "Novel Approach for Intrusion Detection Using Simulated Annealing Algorithm Combined with Hopfield Neural Network," International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 3, pp. 289-294, Decmber 2020.

S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infratructures using ensemble modeling," IEEE Transaction Industry Information, vol. 11, no. 1, pp. 104-111, 2015.