International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

Enhanced Enterprise Device Theft Detection System

[1]Basnayake B.M.N.K., [2]Pinto N.V.C., [3]Bulugammana B.M.P.P., [4]Wijerathne W.N.D., [5]Ms. Thamali Dassanayake, [6]Mr. Uditha Dharmakeerthi

[1,2,3,4]Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Sri Lanka
[5]Department of Information Technology, Sri Lanka Institute of Information Technology, Sri Lanka
[6]Department of Computer Science and Network Engineering, Sri Lanka Institute of Information Technology, Sri Lanka
Authors E-mail: [1]it20089504@my.sliit.lk, [2]it20022624@my.sliit.lk, [3]it20221546@my.sliit.lk, [4]it20259884@my.sliit.lk, [5]thamali.d@sliit.lk, [6]uditha.d@sliit.lk

***Abstract* - Issues regarding device security have been highlighted by the increasing use of devices for information access in a variety of situations, particularly in the context of rising laptop theft. By implementing an Enhanced Enterprise Device Theft Detection System at universities, this research explores how to protect both the device itself and the data it contains. To prevent illegal access to or theft of computers and tablets, this innovative approach combines the strength of CCTV cameras with mobile applications. Users and security professionals are immediately informed of possible thefts using this complete system, enabling fast response. This system's technique, which includes user identification, "Away Mode" activation, real-time image gathering, alarm triggering, and the possibility to follow thieves' location, is the focus of the research. To ensure the system's performance, security, scalability, usability, stability, maintainability, and compatibility, this article also tackles the system's non-functional needs. This solution demonstrates a strong strategy for protecting devices and preventing data breaches by combining modern technology with a meticulously created operational architecture. Beyond just the individual user, it has consequences for businesses and organizations as well, thereby reducing risks, boosting security, and strengthening the fundamental foundation of our linked digital world.**

Keywords: CCTV, Away mode, Alarm triggering, Scalability, Data breaches.

I. INTRODUCTION

The way information is obtained has changed significantly in a time when technology is all over and digital connectivity is expanding at an exponential rate. The use of devices has increased because of this paradigm change, especially laptops, which provide unparalleled accessibility and adaptability. But this development has also resulted in an affecting rise in laptop theft, posing serious risks to both the physical goods and the private information they hold. Considering the seriousness of these risks, this research paper explores the topic of device security, illuminating the complex problems that device theft and data breaches present.

According to recent studies, laptop theft is by far the most common type of device theft, making up an astounding 43% of recorded instances. Laptop theft is closely followed by smartphone theft and tablet theft, accounting for 21% and 16% of reported cases, respectively. According to the statistics, every 53 seconds a laptop theft is identified [1]. Such thefts have far-reaching effects, including financial difficulties and the possible disclosure of sensitive information. Businesses are particularly affected by these effects since data breaches may lead to lost productivity, harm to their reputations, and legal and financial responsibilities.

Although common safety measures like passwords and security software provide some protection, dedicated attackers may frequently get over these barriers by using brute-force attacks, phishing schemes, and malware. Furthermore, it's not always guaranteed that users will follow recommended practices, such as using strong passwords and updating software [2].

This research work presents an innovative approach to strengthen device security in response to these challenges. The system is intended to identify and prevent unauthorized access to and theft of electronic equipment, particularly concentrating on laptops and tablets in educational institutions, by using the capabilities of CCTV cameras [3]. The approach includes several crucial elements, such as recognizing authorized users and devices, turning on "Away Mode" to notify the system, taking pictures of possible criminals, and sending out real-time notifications to both users and security officials. Additionally, the system's ability to monitor the activities of thieves within the building via networked CCTV cameras provides another level of security.

This article includes the non-functional needs of the proposed system, including performance, security, scalability, usability, reliability, maintainability, and compatibility, in addition to its technical components. This research contributes to the continuing discussion on device security and presents a

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

viable answer for protecting electronic assets and sensitive data in a world that is becoming more linked by offering an in-depth structure that faces device theft from several viewpoints.

II. LITERATURE SURVEY

A) Visual Image Processing

To extract useful information and derive insightful conclusions, cutting-edge visual image processing includes modifying and analyzing visual data, such as photos and videos. This technology improves, alters, and interprets visual material via the use of algorithms and computational techniques. Visual image processing is essential to this research work's ability to spot possible security concerns and unauthorized access. By using this technology, the system can analyze real-time photos taken by carefully placed CCTV cameras to recognize people, identify behavioral patterns, and distinguish between authorized users and prospective intruders [4]. The system's visual image processing skills include webcam detection and facial recognition as significant features. CCTV cameras strategically positioned across monitored areas continually record live footage of people using gadgets nearby. The system's online backend then receives these photos for additional processing. These photographs are subjected to sophisticated face recognition algorithms, allowing the system to precisely identify people and possible security problems. This real-time analysis equips the system to react to security problems quickly and precisely, setting off alerts, sending out messages, and giving users and security employees insightful data. The combination of real-time detection techniques and visual image processing emphasizes the relationship between technology and security, highlighting the crucial part it plays in creating a safer digital environment while boosting the system's effectiveness in protecting devices and critical data.

B) Keystroke Dynamics for Enhanced Device Security

A fundamental level of protection against unauthorized access has been offered by traditional security mechanisms like passwords and security software. However, dedicated attackers have taken advantage of weaknesses using techniques including malware, phishing schemes, and brute-force attacks [5]. User compliance with security best practices also varies, which emphasizes the need for stronger, more flexible security solutions.

This research work combines keyboard dynamics as a reliable behavioral biometric method in addition to visual image analysis. Keystroke dynamics involves examining the typing habits and traits that different users display. Subtle variations in keystroke timings, dwell periods, and typing rhythm are observed and recorded as a user interacts with the device's keyboard. Advanced statistical and machine learning tools, such as principal component analysis (PCA) and support vector machines (SVM), are then used to analyze these distinct patterns [6]. The system can distinguish between authentic users and suspected impostors trying unauthorized access by developing a unique typing profile for each authorized user. The system's capacity to guarantee device integrity and data protection is enhanced by the seamless background operation of keystroke dynamics, which adds an additional layer of security.

C) Closed-Circuit Television (CCTV) Cameras

CCTV cameras are surveillance tools made to record and collect video in a particular space. The security structure of the suggested system heavily relies on these cameras. They enable continuous visual surveillance of the surroundings where gadgets are used or kept and are strategically positioned across monitored areas, such as university campuses. This live video stream turns into a crucial source of information for spotting possible threats, shady transactions, or unauthorized users. CCTV footage is processed and examined to look for patterns of behavior, unauthorized entry attempts, and potential theft occurrences [7].

D) Real-Time Image Gathering and Processing

A potential approach to enhancing security is the idea of employing mobile applications and Closed-Circuit Television (CCTV) cameras to detect and respond to laptop theft. This novel strategy aims to include visual image processing methods for user identification. A real-time image of the person using the device is taken and sent to the application's backend. This visual recognition method strengthens the system's capacity to distinguish between authorized users and possible thieves by adding an additional degree of identification verification [8].

Through the built-in cameras, the surveillance network of the system records a real-time image of the user whenever they interact with a device, such as a laptop or tablet. These photos are instantly transmitted to the backend of the program for processing. Along with giving a visual record of device activity, this procedure is a vital part of the system's user identification and verification capabilities.

Rapid facial recognition analysis is made possible by the backend's integration of visual image processing technologies. In this analysis, the system's database of authorized user profiles is compared with the collected photos. The system can then tell apart between authorized users and prospective thieves trying to get unauthorized access.

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

Furthermore, the system's precision and responsiveness are improved using camera-detecting technologies. This technology makes sure that photographs are consistently taken, regardless of the illumination or any obstacles, which improves the system's capacity to properly identify people.

E) Away Mode Activation

Users can switch on this system security feature while they are not physically in possession of their devices. Users may tell the system that the device should be on increased alert for potential security risks by turning on this mode using the application. This can entail making sensors more sensitive, stepping up surveillance, or putting in place more security measures. When the user isn't around, "Away Mode" works as a proactive defense mechanism to deter theft or unauthorized access.

F) Behaviour-Based Biometrics: Mouse Dynamics

Mouse dynamics is a behavioral biometric that examines users' individual mouse movement patterns. By analyzing the various mouse movement patterns, it may determine if the current user is the approved owner. This method is based on the time series data of mouse movements, such as speed, direction, and acceleration, being recorded and examined. To distinguish between authorized users and prospective invaders, advanced analytical techniques like principal component analysis (PCA) and deep learning 1D-cnn model are used. By seeing distinguishing patterns that confirm the identification of the rightful owner, mouse dynamics give an extra degree of security.

III. SYSTEM ARCHTECTURE

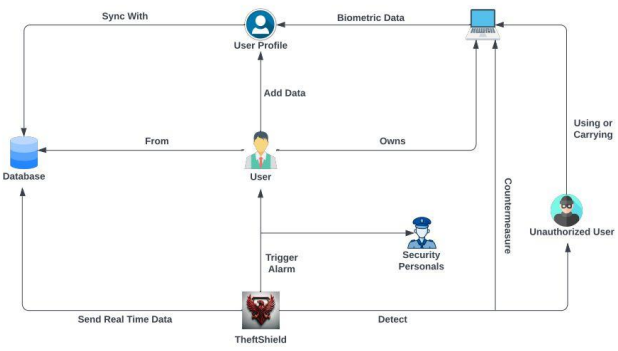

Figure 1: System Architecture

The design and architecture of this research work reflects a seamless combination of modern technology and critical components with the goal of delivering strong device security and real-time threat detection. Utilizing the strength of visual image processing, behavioral biometrics, and cutting-edge software frameworks, the system is painstakingly designed to combat the growing issues of device theft and unauthorized access within educational institutions. The architectural foundation of the system's main parts and their interconnections are described in depth in the following sections.

A) Component Overview

The design of this research work includes several essential components, each of which contributes to the system's overall functioning and security.

- CCTV Cameras: Strategically placed across the monitored regions, these surveillance tools record live video feeds of the surroundings, enabling ongoing observation and information gathering.
- Application: Through a specific mobile application, users communicate with the system. Real-time alerts, "Away Mode" activation, and user authentication are just a few of the capabilities offered by the app.
- Frontend Interface: Users and security experts can interact with the system through the user interface, which is available through web browsers. It displays user authentication prompts, device status, and real-time notifications.
- Web Backend: The web backend acts as the heart of processing, collecting, and analyzing data from mobile devices and CCTV cameras. It includes real-time threat assessments, behavioral biometrics, and visual image processing techniques.
- Database: User profiles, device details, history data, and authentication records are all stored in a reliable database. It makes effective data management and retrieval possible.

B) Operational Flow

The mentioned components are easily integrated into this research work's operating flow, guaranteeing a consistent user experience and effective threat detection. The essential operating steps comprise:

- User Interaction: Using the mobile application or web browser interface, users interact with the system. When the device is left unattended, they can turn on "Away Mode" or get real-time device status.
- Visual image processing: CCTV cameras record live images of people using technology. The web backend receives these photographs and does face recognition processing on them.
- Keystroke Dynamics Analysis: As users type on a device's keyboard, keystroke dynamics are being continually recorded in the background. To create user-specific typing profiles, the captured data is examined

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

using cutting-edge statistical and machine-learning approaches.

- Verification using behavioral biometrics: Analysis of mouse motion improves user verification. The system identifies authorized users and prospective intruders based on individual behaviors by watching mouse movement patterns.
- Threat Analysis and Notification: The online backend analyses threats in real-time by processing behavioral and visual data. Real-time notifications are created and provided to users and security staff via the front-end interface and mobile application in the event of possible threats or unauthorized access.
- User Authentication: Users are requested to enter their credentials using the secure web browser interface when they restart their devices. To provide strong device security, the system integrates visual image processing with conventional credential-based verification.

C) Integration of Technologies

The system's architecture effortlessly integrates a variety of technologies to meet its security goals:

- Visual Image Processing: The real-time visual image processing method is at the center of the system's technical fusion. This component uses advanced algorithms to make use of facial recognition's capacity to identify people as well as identify possible dangers. The system has the discriminating capacity to spot suspicious patterns and abnormalities thanks to the symbiotic interaction between algorithmic processing and visual data collecting, which strengthens the security framework. Keystroke Dynamics Analysis: To verify the identity of the user, machine learning methods such as principal component analysis (PCA) and support vector machines (SVM) analyze keystroke dynamics.
- Keystroke Dynamic Analysis: The examination of keystroke dynamics is another complex area of user interaction, and it is here that machine learning techniques take center stage. The system goes into the world of keystrokes, painstakingly recording the unique typing habits of each user by using cutting-edge methods like principal component analysis (PCA) and support vector machines (SVM). This thorough analysis not only accurately confirms user identification but also becomes better with time, resulting in the creation of unique typing profiles that act as digital fingerprints.
- Mouse Dynamics Analysis: Mouse movement patterns provide a novel aspect of the technological orchestration of the system. Machine learning techniques are used to interpret the subtleties of user behavior through their mouse activities, much as the keystroke dynamics analysis. This in-depth study adds to the continuous user verification procedure, resulting in a complex verification environment that strengthens security through unique behavioral characteristics. Database management: User profiles, device data, and historical records are stored and retrieved from the database effectively.
- Web Application Interface: The web application interface emerges as a channel for user interaction because it serves as the interface between users and the underlying technical wonders. Users are given the ability to engage with the system's operations with ease thanks to its user-facing aspect, which stands out for its accessible design and straightforward layout. Users have more control over tasks like starting the "Away Mode," seeing real-time device status, and responding to real-time danger alarms thanks to this interface.
- Database Management: A key component of the system's technical integration is the smooth administration of crucial data. User profiles, historical data, and device-specific information are all stored in the database management component. Its effectiveness guarantees that information is quickly retrieved and stored, and its function in historical record-keeping gives the system contextual awareness. This feature increases the system's ability to adjust, pick up new information, and develop its danger detection abilities over time.

D) Technology Stack

To provide smooth integration and top performance, this research work was developed using a variety of technology stacks.

- Frontend: ReactJS was used to build the frontend interface, allowing for quick and flexible user interactions.
- Backend: The Laravel-powered web backend controls data processing, real-time analysis, and component communication.
- Python is used for machine learning applications including facial recognition, keyboard dynamics analysis, and mouse dynamics analysis. Scikit-learn and TensorFlow packages are used.
- Database Management: Relational database management system MySQL is used for database administration, ensuring effective data storage and retrieval.
- WebRTC: Real-time communication between devices is made possible with WebRTC technology, allowing for the smooth exchange of pictures and warnings.

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

IV. METHODOLOGY

The implementation and assessment of this research work's methodology is presented in full in this chapter. The system's development, and testing phases, as well as the procedures for gathering and analyzing data, are all covered by the approach. The study seeks to show that the suggested solution may improve device security and deter theft while also being feasible and practical.

A) Integration of CCTV Cameras

A key aspect of the security architecture of this research work is the integration of Closed-Circuit Television (CCTV) cameras. Real-time video footage of the monitored regions is crucially captured by these cameras, allowing for continuous monitoring and data collecting to spot possible threats, unauthorized entry attempts, and suspicious activity. Strategic camera placement, hardware configuration, and smooth backend connection are all required for the system's integration of CCTV cameras. This allows for analysis and the creation of real-time alerts.

Strategic Placement: CCTV cameras are carefully placed across the university campus, with an emphasis on areas where there is a significant volume of foot traffic, device usage, and possible theft threats. Libraries, computer laboratories, study rooms, and common areas are a few examples of places where people commonly use laptops and tablets. The positioning attempts to maximize coverage and guarantee that crucial regions are continuously under monitoring, contributing to a thorough security network.

Data transmission and backend integration: The network infrastructure connects the cameras to the system's backend servers. Through this interface, the video feeds from the cameras may be transmitted in real-time to the backend, where the gathered data is processed, examined, and compared against different criteria to identify possible security concerns. The backend oversees managing the massive amount of video data, analyzing images in real time, and producing alerts based on preset rules and patterns.

Threat Detection and Notification: The system sends immediate notifications when it discovers possible threats, unauthorized access, or suspicious behavior. These alerts are produced in accordance with established criteria, which may include identifying unauthorized users trying to access equipment, identifying odd movement patterns, or detecting actions that differ from typical user behaviors. Through the front-end interface and mobile application, the notifications are given to security employees as well as users, enabling quick responses to any possible security breaches.

B) User Authentication and Away Mode

The strong security measures and real-time threat detection capabilities of this research work are made possible by user authentication and the "Away Mode" function, which are essential parts of the system. When the user is not physically present, these features make sure that only authorized users may use their devices and that increased security measures are in place. The "Away Mode" function and the user authentication process are both described in depth below:

1) User Authentication

A key component in making sure that only authorized users are given access to their devices is user authentication. It entails authenticating the user's identity via a secure web interface before allowing access to the device's features. The system's user authentication procedure is as follows:

- User Interaction: Users are requested to input their credentials using a secure web browser interface when they restart their device or try to access it after a period of inactivity.
- Verification of Credentials: The system's backend receives the entered credentials, usually a username and password combination, for verification.
- Authentication procedure: The backend verifies the supplied credentials against the database's user profiles. The user is given access to the device and all its features if the entered credentials match those on file.
- Using visual image processing to increase security: The system may use visual image processing methods to increase the security of the authentication process. For extra verification, the system could use the device's camera to take a photo of the user and match it to their saved profile picture.
- Immediate Alert in Case of Unauthorized Access: The system immediately alerts the user if an unauthorized user tries to access the device. This warning, informing them of the unauthorized access attempt and probable security breach, is issued to the authorized user through the front-end interface and mobile application.

2) Away mode

A proactive security feature called "Away Mode" is available for customers to enable while they are not physically in control of their devices. To guard against theft and unauthorized access, this mode strengthens the device's security features and surveillance capabilities. The following procedures must be followed to activate and use "Away Mode":

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

- User Interaction: When they want to leave their device unattended, users can turn on "Away Mode" using the mobile application.
- Increased monitoring: When the system is activated, it intensifies its security measures by enhancing CCTV monitoring, making sensors more sensitive, and putting in place extra security procedures.
- Real-time Monitoring: Using the built-in CCTV cameras, the system continually scans the area around the device for any indications of unauthorized entry or suspicious activity.
- Immediate Alerts: Real-time notifications are sent out whenever the system notices any possible security threats, such as unauthorized users attempting to access the device. Both the user and security professionals receive these notifications via the front-end interface and mobile application.
- Preventing Unauthorized Access: "Away Mode" acts as a deterrent to potential thieves or unauthorized users by making it harder to breach the device's security thanks to the increased security features and real-time notifications.
- Enhanced User Control: Users can choose to switch off "Away Mode" when they get back to their devices, restoring the system to its regular operating condition.

C) Visual Image Processing and Analysis

This research work relies heavily on visual image processing to identify users, distinguish between authorized users and possible thieves, and send out real-time notifications. The system processes and analyses real-time CCTV camera pictures using sophisticated algorithms and computational approaches, enabling quick and precise danger identification. The capacity of this research work to recognize and react to possible threats and unauthorized access is critically dependent on the visual image processing algorithm. Facial recognition, pattern analysis, and real-time threat assessment are combined to enable the system to quickly identify security concerns and initiate the necessary countermeasures to safeguard electronic assets and sensitive data.

D) Keystroke Dynamics Implementation and Evaluation

The core component of this research work, keystroke dynamics, adds an extra layer of protection by examining users' typing habits and patterns. Keystroke dynamics must be implemented and evaluated through a sequence of stages that record, examine, and validate user-specific typing profiles. These procedures assist distinguish between legitimate users and possible imposters.

Data Gathering: As users engage with the device's keyboard, keystroke data is gathered at the start of the process. Several timing parameters, such as key press lengths, key press intervals, and typing rhythm, are captured while users type. Individual typing profiles are created using these timing features, which are recorded and documented in real-time.

Feature Extraction: After gathering the keystroke data, feature extraction algorithms are used to extract significant patterns from the timing data. Each temporal feature is given a statistical value, such as mean, standard deviation, and variance. These features offer a numerical illustration of each user's distinctive typing style [9].

Machine Learning Model: Based on the derived temporal characteristics, a machine learning model is developed to distinguish between authorized users and probable impostors. For this, methods like principal component analysis (PCA) and support vector machines (SVM) are frequently used. The model learns to identify the minute variations in typing styles that separate authorized users from real users throughout the training phase.

Creation of Typing Profiles: The system creates a user-specific typing profile for each authorized user using the learned machine learning model. This profile summarizes the user's typing behavior's statistical features and serves as a guide for further confirmation.

Real-Time Verification: The system continually analyses the typing styles of active users with their associated typing profiles while it is operating in real time. The system assesses whether users' keyboard interactions are consistent with their pre-established typing profiles as they type. Unexpected variations in typing rhythm or dwell lengths, for example, might cause deviations from the usual to raise an alarm about a possible security problem [10].

Impostor Detection: Keystroke Dynamics' main goal is to identify imposters who are seeking to get unauthorized access. The typing patterns of unauthorized users are compared to the authorized profiles that have been stored when they attempt to access a device. The system can recognize the user as a forger and initiate the necessary security procedures if the user's typing behaviour dramatically deviates from the usual patterns.

Evaluation of Accuracy and Robustness: Strict testing and validation are used to assess the accuracy and robustness of the keystroke dynamics technology. To replicate a range of user behaviors, including those of real users and imposters, synthetic situations are constructed. Performance indicators such as accuracy, precision, recall, and false positive rates are

© 2023-2017 IRJIET All Rights Reserved

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 9, pp 137-144, September-2023

https://doi.org/10.47001/IRJIET/2023.709016

computed to assess the system's capability to accurately identify authorized users and identify pretenders.

E) Mouse Dynamics Integration and Assessment

The key component of this research work, mouse dynamics adds a further layer of behavioral biometrics to improve user authentication and device security. The capture, analysis, and evaluation of users' unique mouse movement patterns in real time are all part of the integration and evaluation of mouse dynamics.

Data Capture: As users interact with the device's mouse, data about mouse movement is first captured. The speed, direction, acceleration, and trajectory of user motions are all tracked as they move the mouse around the screen. These mouse movement patterns serve as the foundation for analysis and verification since they are continually recorded and verified in real-time [11].

Feature Extraction: After the mouse movement data has been recorded, feature extraction techniques are used to draw conclusions from the motion characteristics' raw data. Relevant parameters including speed variance, movement route curvature, and consistency of direction shifts are computed using sophisticated statistical methods and signal processing techniques.

Machine Learning Model: Based on the retrieved mouse movement data, a machine learning model is built to distinguish between authorized users and prospective attackers. Techniques like principal component analysis (PCA) and the deep learning 1D-CNN model are frequently used for this purpose, much like other biometric approaches. The model picks up on the minute variations in mouse movement styles that separate authorized users from legitimate users.

Development of User Profiles: The system develops user-specific mouse movement profiles for each authorized user using the learned machine learning model. These profiles record the unique traits of each user's mouse behavior, serving as a guide for upcoming confirmation.

Real-Time Verification: As the system operates in real-time, it continually compares the mouse movement patterns of the present users to the corresponding profiles. The system assesses whether users' mouse movements are consistent with their pre-established profiles as they manipulate the mouse. A possible security danger might be indicated by deviations from the norm, such as odd movement trajectories or unexpected acceleration patterns.

Impostor Detection: Mouse dynamics technology looks for unauthorized access attempts by impostors. The mouse movement patterns of unauthorized users are compared to the authorized profiles that have been stored when they attempt to use the device. When a user significantly deviates from the typical mouse behavior, the individual may be recognized as a fraud [12].

Evaluation of Accuracy and Performance: Through extensive testing and validation, the accuracy and performance of mouse dynamics integration are assessed. To mimic different user behaviors, including those of authorized users and imposters, synthetic scenarios are created. Performance indicators including accuracy, false positive rates, and false negative rates are computed to evaluate the system's capability to accurately identify authorized users and identify importers.

Comparative Analysis: The effectiveness of mouse dynamics authentication is evaluated against that of other authentication techniques, including keystroke dynamics and conventional password-based authentication. The usefulness of mouse dynamics as an extra layer of security and its capacity to support current authentication systems are determined through a comparative study.

V. CONCLUSION

This research work is a significant improvement in how educational institutions and other settings are handling the growing problems of device security and unauthorized access. This system offers a thorough and proactive approach to protecting electronic assets and sensitive data through the careful integration of cutting-edge technologies, such as visual image processing, keyboard dynamics, and mouse dynamics. The solution offers a strong defense against the growing tide of device theft and possible breaches by integrating real-time threat detection, user authentication, and upgraded security capabilities.

The system's effectiveness in spotting and preventing possible security breaches was made clear by its implementation and assessment. The visual image processing component, which is supported by powerful algorithms, demonstrates its brilliance by quickly and precisely detecting unauthorised users and questionable behaviours through real-time picture analysis. As a result, there is an ever-vigilant sentinel that may sound the alarm at the first indication of a security risk. The use of behavioural biometrics, namely mouse and keyboard dynamics, adds a degree of individuality to user identification. The technology records the unique typing and mouse-movement patterns of authorised users, making it possible to distinguish between real people and prospective impostors. The strong defence mechanism that

© 2023-2017 IRJIET All Rights Reserved

ISSN (online): 2581-3048
Volume 7, Issue 9, pp 137-144, September-2023
https://doi.org/10.47001/IRJIET/2023.709016

results from this multi-layered strategy considerably reduces the danger of unauthorised access and device theft.

In the end least, this research project represents a significant paradigm change in the field of device security. By fusing technology advancement with a painstakingly designed operational architecture, it not only offers an efficient defence against the rising tide of gadget theft but also establishes a standard for all-encompassing security measures. The ramifications go beyond educational institutions and apply to corporations and organisations as well, supporting the cause of lower risks, more security, and a more robust digital ecosystem. Our linked world's basis has been strengthened by the incorporation of contemporary technology, securing not just physical assets but also the data that powers our digital life. Through this study, a roadmap for a safer, more secure digital future is being developed.

REFERENCES

[1] A Communications, "Arrowhead General Insurance Agency, Inc.," Back-to-school laptop and mobile device security measures, 2023.

[2] "SoSafe," What Are Brute-Force Attacks?: Examples & Prevention Tips, 2023.

[3] "Common (and uncommon) approaches to preventing the theft of computers, laptops and tablets in schools," [Online]. Available: https://blogs.worldbank.org/edutech/computer-theft-schools. [Accessed 12 08 2023].

[4] "Image processing in the context of a visual model - university of utah," [Online]. Available: https://www.math.utah.edu/~gustafso/s2013/3150/pdeNotes/Artigo_Stockham_01450712.pdf. [Accessed 12 08 2023].

[5] "Cybersecurity Guide: Fundamentals of Cybersecurity Topics," [Online]. Available: https://www.xcitium.com/cybersecurity/. [Accessed 12 08 2023].

[6] H. Dhaduk, "Support Vector Machine and Principal Component Analysis Tutorial for beginners," [Online]. Available: https://www.analyticsvidhya.com/blog/2021/07/svm-and-pca-tutorial-for-beginners/. [Accessed 12 08 2023].

[7] T. Contributor, "What is CCTV (closed circuit television)?: Definition from TechTarget," [Online]. Available: https://www.techtarget.com/whatis/definition/CCTV-closed-circuit-television. [Accessed 13 08 2023].

[8] P. Vennam, "Attacks and preventive measures on video surveillance systems: A Review," Applied Sciences, 2021.

[9] "Keylogger: How they work and how to detect them," Knowledge Hut, 2023.

[10] Y. Muliono, "Keystroke Dynamic Classification Using Machine Learning for password authorization," Procedia Computer Science, 2018.

[11] "Mouse Dynamics," Typing DNA, 2023.

[12] M. Antal, "Intrusion detection using Mouse Dynamics," IET Biometrics, 2019.

[13] "Laptop theft prevention and recovery," Department of Public Safety, 18-May-2015. [Online]. Available: https://dps.usc.edu/services/laptops/. [Accessed: 27-Aug-2023].

[14] "Laptop theft prevention," Public Safety | Brown University. [Online]. Available: https://dps.brown.edu/crime-prevention/safety-tips/laptop-theft-prevention. [Accessed: 27-Aug-2023].

[15] "Laptop theft prevention," Harvard.edu. [Online]. Available: https://www.hupd.harvard.edu/laptop-theft-prevention. [Accessed: 27-Aug-2023].

[16] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics overview," in Biometrics, In Tech, 2011.

[17] Researchgate.net. [Online]. Available: https://www.researchgate.net/publication/221912833_Keystroke_Dynamics_Overview. [Accessed: 27-Aug-2023].

[18] Researchgate.net. [Online]. Available: https://www.researchgate.net/publication/306062718_Enhanced_keystroke_dynamics_authentication_utilizing_pressure_detection. [Accessed: 27-Aug-2023].

Citation of this Article:

Basnayake B.M.N.K., Pinto N.V.C., Bulugammana B.M.P.P., Wijerathne W.N.D., Ms. Thamali Dassanayake, Mr. Uditha Dharmakeerthi, "Enhanced Enterprise Device Theft Detection System" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 9, pp 137-144, September-2023. Article DOI https://doi.org/10.47001/IRJIET/2023.709016

****

© 2023-2017 IRJIET All Rights Reserved