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

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 370-377, November-2023
https://doi.org/10.47001/IRJIET/2023.711050

SecureSense: A Network Threat Detection and File Sharing System

[1]K.K.K.P Wickramasinge, [2]G.D.D Ekanayake, [3]P.G.K.S Munasinghe, [4]S.N Hettiwatta, [5]S.M.B Harshanath, [6]S.K Rajapaksha

[1,2,3,4,5,6]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
Authors E-mail: [1]it20231378@my.sliit.lk, [2]it20201814@my.sliit.lk, [3]it20214166@my.sliit.lk, [4]it20246150@my.sliit.lk, [5]harshanath.s@sliit.lk, [6]samantha.r@sliit.lk

***Abstract* - A strong security mechanism designed to protect shared data within corporations is introduced in this document. Our system uses hash checks, modern virus detection, user identification via facial recognition, encryption, and other techniques to guarantee secure data flow and efficiently stop the spread of malware. Our complete strategy strengthens cybersecurity, protects sensitive information, and supports data integrity within document sharing networks by including these measures. This multimodal strategy provides a strong defense, supporting organizations' security postures against new threats. Our technology offers a foundation for seamless document sharing by combining real-time scanning, user authentication, and safe encryption. By placing a high priority on data protection and integrity, we enable companies to reliably communicate sensitive information, establishing safe and effective collaboration environments.**

Keywords: Antivirus, DLP, Encryption, Document, Security, Classification, Access control, Cybersecurity.

I. INTRODUCTION

Organizational document sharing has developed into a crucial element of collaborative work settings in today's connected and digitalized world. This ease of use is accompanied by the persistent threat of virus spread, which poses serious problems for operational continuity, data security, and privacy. Malicious software, including viruses and sophisticated malware, has the ability to infiltrate document repositories, compromise sensitive data, and impair critical operations. An comprehensive library of virus signatures, a reliable virus detection algorithm, and a blocking mechanism are the main elements of the suggested solution. The document virus detection tool will be installed on each endpoint in the organization's network, and a centralized server will enable communication with the viral signature database, synchronization of the database, and overall system control.

We suggest a thorough security mechanism designed specifically for organizational document sharing networks to address this pressing issue. Our solution combines technology to identify, stop, and reduce malware's ability to spread inside the ecosystem of file sharing. Our system creates a strong protection against a range of potential threats by integrating document hashing, virus detection, multi-factor user authentication with facial recognition, centralized administration, intrusion detection, screen capture control, and document encryption. Organizations may protect their networks from potential document-based threats, lower their risk of data breaches, and foster a culture of secure information exchange among their staff by implementing this document virus detection and blocking solution. A basis for future improvements in document protection techniques will be laid by the knowledge gathered from this research, which will also add to the body of knowledge in the field of network security

We describe the major elements, operating procedures, and underlying technologies of our suggested security system in detail in this paper. Our solution intends to strengthen document sharing networks, ensuring data integrity, user privacy, and a robust security posture by tackling both known weaknesses and emerging issues.

We want to give readers a thorough knowledge of the novel strategy we have created to stop malware transmission within organizational document sharing environments by examining the system's architecture, processes, and practical implementations. Our technology aids in the development of safe, effective, and collaborative digital workspaces by reducing security concerns and improving the overall dependability of document sharing.

II. PROBLEM STATEMENT

Endpoint security and network-level defenses are frequently the main priorities of the current malware detection and prevention systems. These steps are necessary, but they typically fall short of tackling the complexity of document sharing ecosystems. With the constantly changing environment of malware, including zero-day exploits and polymorphic strains that can mutate to elude detection,

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

traditional antivirus software and firewalls may find it difficult to stay up. Additionally, corporate document sharing networks cover a variety of hardware, software, and geographical regions, which makes it more difficult to protect against the spread of malware. Users frequently share papers with different collaborators, both inside and outside the company, increasing the danger of malware introduction into the network accidentally [1].

In order to reduce the danger of malware spread within organizational document sharing environments, an innovative method that combines advanced detection algorithms, user authentication, centralized oversight, and robust encryption is required due to the problem's complexity. A comprehensive solution that not only detects and stops malware but also secures user privacy, upholds data integrity, and evolves to counter new threats is necessary to address these issues.

Our research aims to create and propose a comprehensive security solution that tackles these problems head-on in this setting. Our goal is to offer a comprehensive solution that improves the security and dependability of document sharing networks, allowing businesses to collaborate with confidence while protecting their most important assets from the dangers of malware proliferation. We do this by combining cutting edge technologies and security practices.

A) What we intend to solve

The exchange of digital documents inside organizational settings and their rapid spread have completely changed how firms interact and function. However, this simplicity comes with a significant challenge, the persistent risk of malware spread. The security, confidentiality, and functionality of shared documents are seriously at danger from malicious software, which can range from simple viruses to complex and evasive malware strains.

Modern businesses also transcend physical and geographical boundaries to function inside a complex web of tools, platforms, and user interactions. Because document sharing procedures vary widely, virus prevention must have a sophisticated and flexible stance. Internal and external collaborators unintentionally turn into possible channels for introducing malware into shared repositories, increasing the danger of unintentional infection.

A comprehensive solution that proactively detects, stops, and reduces the spread of malware through organizational document sharing networks is required to address this complicated issue. Along with advanced detection and prevention tools, the system must also easily connect with user processes, protect data privacy, and evolve to counter new threats. Organizations may build a secure and resilient environment for document sharing by addressing these issues, protecting the integrity of their data, upholding user confidence, and maintaining operational continuity.

Our research aims to create a complete security system that effectively solves these problems in this complicated environment. In the context of organizational document sharing, we seek to create a formidable defense against virus dissemination by fusing cutting-edge technology, strong user authentication, watchful monitoring, and strong encryption. Through this project, we hope to equip businesses with the tools they need to take advantage of contemporary cooperation while protecting their digital infrastructure from the enduring threat of malware spread.

III. SYSTEM ARCHITECTURE

Current document sharing practices have security flaws and the potential to expose sensitive data. Our fresh approach confronts these difficulties head-on. Hash checks, virus detection, multi-factor authentication, and encryption are all combined by SecureSense to build a secure framework for effective teamwork while preserving data privacy and integrity.

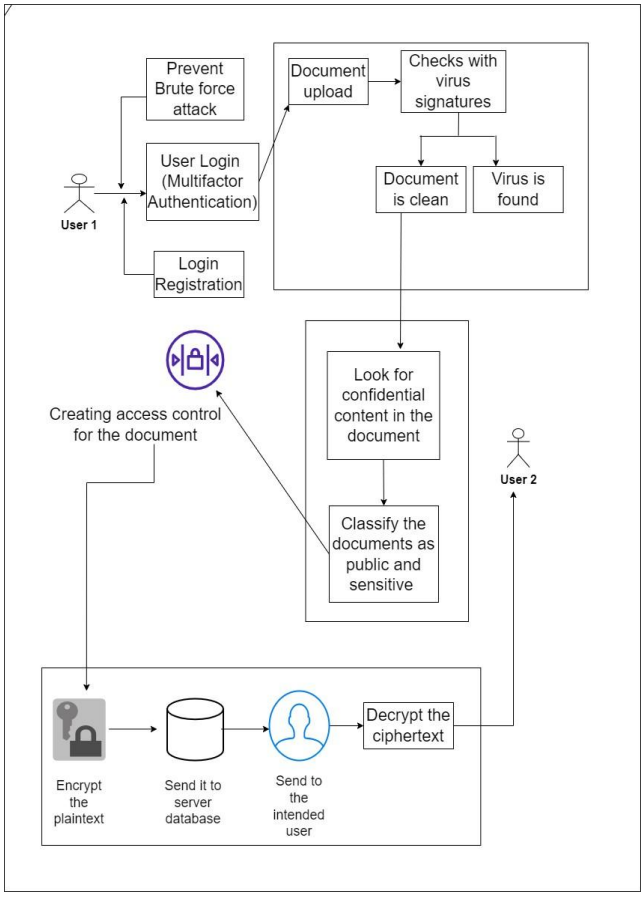


Figure 1: Architecture of SecureSense

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

IV. LITERATURE REVIEW

A new era of cooperation and effectiveness has been ushered in by the widespread use of digital documents and their easy distribution within corporate contexts. The ongoing threat of virus spread, however, casts a shadow over this technological advancement, driving intense study into fortifying document sharing networks. In terms of malware detection, prevention, and safe document sharing, this overview of the literature looks at major developments, trends, and difficulties.

There are several approaches to classify and identify confidential files in organization environments. Here, Conidial file identifying, and classification means use of software tool to identify and analyze confidential files. According to the study confidential files can be categorized as having text of "Social Security numbers, Driver's license numbers, Credit card numbers, Bank account numbers, Patient treatment information" etc [2]. This paragraph mainly focused on previous studies which had used preprocessing techniques to remove unnecessary information from confidential data files, identify the contents and classify them as either sensitive (confidential) or non-sensitive based on the presence of specific keywords or patterns that indicate confidentiality machine learning-based approaches. Following are some studies that had an impact on this study.

Conventional login procedures frequently have flaws since they only use passwords that can be compromised. The absence of multi-factor authentication in these systems makes papers accessible to unauthorized users. SecureSense's login method, in contrast, combines powerful multi-factor authentication with features like brute force protection and facial recognition to create a strong barrier against illegal entry. [3]

SecureSense distinguishes itself with a centralized approach, including hash checks, virus detection, user identification with facial recognition, and encryption. While the Secure document sharing model put forth by Garima Verma and Soumen Kanrar is based on blockchain technology, SecureSense is not. Despite the fact that both solutions seek to improve document sharing security, SecureSense prioritizes real-time malware detection and prevention within a centralized framework, whereas the blockchain-based model makes use of decentralized blockchain attributes for improved data transparency and integrity. [4]

Various dangers linked with BYOD (Bring Your Own Device) are identified in the study research paper "Bring Your Own Device: Organizational Information Security and Privacy" by Abubakar Bello Garba, Jocelyn Armarego, and David Murray. Phishing, social engineering, direct assaults, data transmission interception/spoofing, device loss/theft, and malicious insider acts are among the hazards. [5]

Concerns about security flaws, data privacy, and potential inefficiencies have been highlighted by cloud-based document sharing platforms. While inter network systems are practical, protecting sensitive data from illegal access and data breaches is a frequent concern. SecureSense, on the other hand, is a hopeful solution. Our strategy provides a thorough defense against malware transmission and illegal access by using advanced security features. This approach not only fixes the issues with traditional cloud-based sharing but also guarantees strong security, effective teamwork, and data integrity within corporate document sharing networks. [6]

Direct assaults in BYOD environments often aim to obtain unauthorized access, destroy data, manipulate data, or extract private information. However, it is vital to emphasize that, with the exception of exposing the outstanding ability of hackers, all information about these direct attacks has a negative influence on enterprises. Theft, deletion, or manipulation of sensitive cooperative information, particularly for businesses delivering internet-based services to clients, can have serious consequences for the organization [7].

SecureSense assists users in secure confidential files in organization. The authentication is multi factor and includes access control. Authentication by username and password from the database in hash value, Face Recognition Authentication, Access Control using four tier architecture. ER Weippl, IK Ibrahim, and W Winiwarter's "Contentbased Management of Document Access Control" highlights controlling document access based on its content. SecureSense, in contrast, uses a multi-layered strategy. While the content-based approach concentrates on individual material, SecureSense offers extensive security measures to protect corporate document sharing networks from viruses, unwanted access, and data privacy. [8]

An authorized device is granted access to confidential files and can perform actions commensurate with its assigned privileges. In this system, permissions for authorized employees are structured into four distinct tiers. In contrast, if a device lacks authorization (i.e., not assess the developed biometric check), users will be unable to access the relevant files. In such instances, the system will automatically enforce access restrictions, preventing any unauthorized activity.

Unlike traditional encryption techniques, homomorphic encryption enables computations to be performed directly on encrypted data without the requirement for decryption. This ground-breaking method addresses data privacy issues in situations like outsourced computation by maintaining data

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

private during calculations. While your software includes a number of security measures. [9]

V. METHODOLOGY

SecureSence combines a multi-layered architecture with advanced technologies like automatic file classification and homomorphic encryption to detect and stop virus transmission across organizational document sharing networks. This elaborate architecture is intended to offer all-encompassing security while preserving operational effectiveness and safe teamwork.

1) User Interface Layer: The user interface layer continues to serve as the entrance point for user interactions and enables smooth interaction with security features. Users authenticate themselves using a multi-factor method that combines a face recognition technology with a password protection mechanism. When a user attempts an incorrect password repeatedly, the system temporarily blocks the user and alerts the administrators.

2) Document Hashing and Virus Detection Layer: Incoming documents are hashed, producing one-of-a-kind hash values, and then compared against a database of virus hashes. Any malware matches or discrepancies result in alerts being sent out. Immediate alerts provide users and admins more control.

3) File classification layer: Scope of the research is limited to identify and classify of confidential information files on personal devices. It aims to develop methods and algorithms that can accurately detect and classify various types of sensitive information, such as financial data, personally identifiable information in personal devices.

4) Homomorphic Encryption Layer: The system uses homomorphic encryption to offer the highest level of document confidentiality. Since each document is encrypted using homomorphic methods, encrypted data can be used in computations. Decryption is performed by authorized users using their login credentials, offering an additional degree of security.

A) Key Advantages of the Enhanced Architecture

1) Virus detection and user banning: Alerting system of virus detection to the whole network and blocking out the user that tried to send the virus document give the whole network a confident document sharing and storage.

2) Automated File Classification: Document sharing has been enhanced by the addition of automated file classification, which improves the user experience and security.

3) Homomorphic Encryption: By utilizing homomorphic encryption, you can perform secure computations on encrypted data while preserving document confidentiality.

4) User-Centric Usability: The architecture is always user friendly despite its complexity, giving users easy document exchange and increased security.

B) Virus Detection and Intruder Blocking

The technique takes into account the software's design and architecture, the gathering of necessary information, the carrying out of stringent testing processes, and the construction of assessment metrics to assess the software's efficacy, efficiency, and security. Every workstation in the network receives and installs the Client Software. It includes features like document hashing, comparing MD5 hashes with a continually updated database of virus signatures, and starting alerts when a match is found. This component focuses on real-time document analysis while minimizing overhead and offering a seamless user experience. The network's security infrastructure is orchestrated by the server software. It watches client interactions, maintains an extensive and current database of known virus MD5 hashes, and imposes temporary bans on users who try to send infected files. Additionally, the server keeps thorough records of all communications and actions, which is useful for forensic investigation and ongoing development.

1) Design: A comprehensive architectural plan that highlighted flexibility, scalability, and security laid the groundwork for the program. The client software and the server software are the two key elements of the architecture. Every workstation in the network receives and installs the Client Software. It includes features like document hashing, comparing MD5 hashes with a continually updated database of virus signatures, and starting alerts when a match is found. This component focuses on real-time document analysis while minimizing overhead and offering a seamless user experience. The network's security infrastructure is orchestrated by the server software. It watches client interactions, maintains an extensive and current database of known virus MD5 hashes, and imposes temporary bans on users who try to send infected files. Additionally, the server keeps thorough records of all communications and actions, which is useful for forensic investigation and ongoing development.

C) Automated identification and analysis of confidential files

1) Dataset preparation - company confidential information: SecureSense has to define and classify confidential data patterns due to non-availability of common confederal

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

formats. The following formats sample data formats and contents have been used for sample data.

Employee Personal Information: This category includes files containing personal data of employees, such as names, addresses, contact information, social security numbers, bank account details, or any other personally identifiable information (PII) that is confidential and protected by privacy regulations.

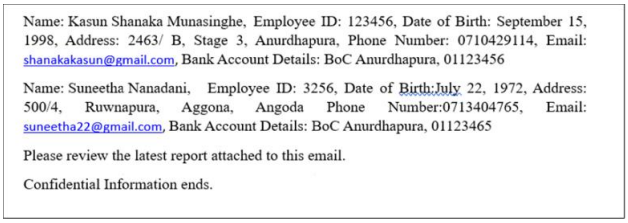
Financial Records: This category includes files containing financial information, such as payroll records, tax documents, financial statements, budget reports, or any other financial data that is confidential and crucial for the company's financial operations.

Customer Data: This category includes files containing customer information, such as customer names, contact details, purchase history, credit card information, or any other data related to customer interactions that is confidential and protected by privacy regulations.

Intellectual Property: This category includes files containing proprietary information, trade secrets, patents, copyrights, research and development documents, or any other valuable intellectual property that is confidential and critical for the company's competitive advantage.

Legal and Compliance Documents: This category includes files containing legal contracts, non-disclosure agreements, compliance reports, or any other legal an regulatory documents that are confidential and require strict protection to ensure compliance and avoid legal repercussions.

Next, create different types of sample files as shown below.



Name: Kasun Shanaka Munasinghe, Employee ID: 123456, Date of Birth: September 15, 1998, Address: 2463/ B, Stage 3, Anurdhapura, Phone Number: 0710429114, Email: shanakakasun@gmail.com, Bank Account Details: BoC Anurdhapura, 01123456

Name: Suneetha Nanadani, Employee ID: 3256, Date of Birth:July 22, 1972, Address: 500/4, Ruwnapura, Aggona, Angoda Phone Number:0713404765, Email: suneetha22@gmail.com, Bank Account Details: BoC Anurdhapura, 01123465

Please review the latest report attached to this email.

Confidential Information ends.

Figure 2: Sample confidential information in a company file

2) Data preprocessing techniques and algorithms: To identify the valuable information that is there in the raw data so that we can ensure its preservation? is one of the most significant issues with data preparation. Our concept of data preparation may have an impact on this. Some may contend that data preprocessing does not actually occur "pre-" data analysis. It requires input from the primary data analysis process. After preparing sample files, unwanted data are removed by using preprocessing techniques. Naive Bayes Classifier algorithm can be used to classify confidential files in an organization as follows.

- Load the document.
- Tokenize the text content of the document into individual words or tokens.
- Remove stopwords (common words like "the", "is", etc.) from the tokens to reduce noise.
- Create a frequency distribution of the remaining tokens to determine the likelihood of each word occurring.
- Prepare a dataset for the classifier by labeling each token as either sensitive (confidential) or non-sensitive based on the presence of specific keywords or patterns that indicate confidentiality.
- Split the dataset into training and testing sets.
- Train a Naive Bayes classifier on the training set, using the features (tokens) and their corresponding labels (sensitive or non-sensitive).
- Test the trained classifier on the testing set to evaluate its performance.
- Use the trained classifier to classify the tokens in the MS Word file as either sensitive or non-sensitive.
- Output the classified tokens, highlighting, or extracting the confidential information identified by the classifier.

D) Login Mechanism and Document Access Control

When compared to password-based methods, the use of biometrics such as fingerprints, face recognition, voice recognition, or retina scans is a more reliable way of accessing information. Biometrics are more secure than passwords since they are harder to steal from a database, and they save time by removing the need to learn or retrieve passwords. Continued biometric authentication and/or multi-factor authentication (MFA) can be utilized to offer an extra layer of protection. It is also worth noting that biometrics can be used to prevent illegal access to sensitive papers.

A biometric check will be introduced to the system to identify authorized devices and restrict access to secret data to those devices exclusively. The biometric technique of choice will be Face recognition scanning. Biometric technology is becoming increasingly used in the workplace as a simple and efficient security solution. The expanding usage of biometric data for personal purposes has also aided its adoption in work environments.

Only approved devices are permitted access to confidential data based on their status. For approved personnel, the system has a four-tiered authorization structure. If a device is not allowed, that is, it fails the biometric check, the user is unable to access necessary data, and the system automatically terminates the activity. In addition, the system contains a mitigation mode that prevents any unexpected

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

behavior identified until it is properly evaluated. Suspicious user activity requires response since it may signal an intrusion or an insider danger. While the investigation is ongoing, the system locks any suspicious user accounts and suspicious login person photo captured by the system. This strategy is extremely useful when dealing with lost or stolen devices.

The face recognition check and access control are intended to protect sensitive data from any harm and threats by allowing employees to access private files using their own devices while reducing any potential threats. The system validates the user's unique face recognition authentication and confirms the employee's tier-based status before giving access to the appropriate file categories. The following advantages may be acquired through implementing this technology, which can improve the security of confidential information within the organization.

1) User loggin procedure: When a user attempts to access their account, they must provide their username and password. When the user enters this information, the system authenticates it to ensure that it is correct. In addition, the system will do a facial recognition scan to confirm the user's identification. After being input, the user's password is kept in the database as a hash value to increase security.

Consider the following scenario: you keep all user passwords in your database in plain text, with no alteration. If an attacker obtains access to your database, they will be able to simply see and change any user credentials stored there, putting all user data at danger. Hashing, on the other hand, gives a one-way encryption solution to this problem. Hashing converts a password into another string known as the hashed password, which cannot be readily reversed back to its original form. As a result, hashing is known as a one-way procedure that adds security to user passwords

2) Biometric data identification and analysis: This approach adds into the system a "Face recognition" (biometric check) mechanism. The biometric check assists in the identification of authorized devices, guaranteeing that confidential files may only be accessed on devices that have been identified. The biometric authentication procedure is invisible to the user, and the screen does not show whether or not it is being confirmed. A face recognition algorithm is required in any software or system to enable facial detection and recognition. Experts often divide these algorithms into two broad types. The geometric method identifies face characteristics, whereas the photometric statistical approach extracts values from photos. These values are then compared to templates to eliminate variances. Two further major classes into which the algorithms can be separated are feature-based and holistic models. While holistic approaches examine the entire human face, the former focuses on facial landmarks and evaluates their spatial characteristics and relationships to other features. Biometrics are biological measurements or physical features that are used to identify individuals. Common biometrics include facial biometrics, retinal scanning, and fingerprint mapping. Facial biometrics works by:

The process of collecting and analyzing an image of a person's face is referred to as facial analysis. Most facial biometric systems use 2D images rather than 3D ones. The program determines a person's facial structure, such as the distance between the eyes, as well as the distance between the forehead and chin. Furthermore, the system recognizes facial landmarks to differentiate between a face in a database and a real person.

3) Unauthorized user/ device activity blocking: Based on their permissions, the system allows authorized devices to view secret files. The system divides the permissions of authorized personnel into two tiers. Unauthorized devices that have not been biometrically verified are unable to access the required data since the system automatically prevents the activity. If unusual activity is detected, the system enters mitigation mode, disabling the questionable behavior until it is thoroughly investigated. Suspicious user activity triggers action since it might signal an intrusion or insider danger, and their accounts are frozen while the system investigates. Even if the gadget is lost or stolen, this procedure is straightforward. If the user enters wrong information, he or she will be unable to access files or accounts. There are only five opportunities to try again. Even if the username and password are correct, the user is still unable to access the account since the biometric check fails. The account has been terminated. Only the administrator has the ability to retrieve the account.

VI. CONCLUTION

The growth of the personal device culture in the workplace has created a need to protect company documents holding critical information from potential dangers. These threats take advantage of flaws in user devices and behaviors by deploying techniques like as brute force attacks, phishing, malware, and device theft. To address this important problem, there is a need for a system capable of recognizing and preserving essential information, especially in light of the growing number of occurrences of device compromises both locally and worldwide. Security is one of the most concerning risks related with the usage of personal devices for work. Allowing workers to use their own devices to access a company's assets brings apparent concerns. Many businesses have been hesitant to embrace the personal device concept due to concerns about dangerous apps and viruses. Because business owners are fully aware of the very real threat

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 370-377, November-2023
https://doi.org/10.47001/IRJIET/2023.711050

presented by cyberattacks, implementing personal device regulations may be a difficult task. Companies who are serious to implementing the personal device idea must recognize that people are the weakest link in the security chain. They must rapidly seek solutions that will either entirely resolve or considerably alleviate these challenges. Our research addresses these issues front on by using a hash check mechanism and a intruder banning technique to detect viral assaults and possibly harmful files, hence improving overall security. Many ordinary users may lack a thorough awareness of the possible threats posed by critical information within an organization. misplacing critical files, deletion, destruction, change data while losing integrity, etc. that jeopardize data integrity are all possibilities. It is crucial to be able to identify these key files and determine the amount of harm they pose to the company. It enables users to understand the importance of certain files and take charge of their administration. Our research approach tackles the issue of user awareness and workspace disorder by offering a technique for automatically identify critical and sensitive files that uses machine learning technology. A reliable option for safe file uploading and downloading in cloud environments is homomorphic encryption. It efficiently protects data secrecy and integrity by allowing computations on encrypted data without needing to decrypt it. This method allays security worries by enabling cloud storage and file manipulation without disclosing the contents of the files. Additionally, local file decryption provides anonymity even from the cloud service provider for downloaded files. Even though there might be some performance issues, ongoing developments will probably reduce these restrictions. Homomorphic encryption essentially has the ability to change how cloud data operations are conducted by boosting security while maintaining functionality.

Despite the strict implementation of numerous security measures to protect online accounts and personal data, vulnerabilities exist that might possibly expose this information within the data management systems of others, resulting in data theft or leaking. While promising, facial recognition technology has traditionally been used for user identification in conjunction with expensive and constrained hardware developments. The goal of this project is to make face recognition logins more accessible to website and software developers. We do this by employing a variety of machine learning techniques to consistently identify user accounts while depending on low cost cameras. To demonstrate the viability of this approach, we created a web API that allows users to authenticate into their accounts using face recognition. Furthermore, we plan to create a user-friendly website to test the robustness of our system. Organizations may use this technology to improve personal device security, enhancing the security of important data. In addition to hashing techniques to improve data security, our system includes a multifactor authentication mechanism to protect confidential information. In the event of an unauthorized attempt to access the system through brute force attacks, the system takes a photo of the attacker and sends it to the admin database, blocking access to the confidential files. Such suspicious actions are automatically blocked by the system.

REFERENCES

[1] I.A. Saeed, A. Selamat, and A. M. Abuagoub, “A survey on malware and malware detection systems,” International Journal of Computer Applications, vol. 67, no. 16, 2013.

[2] N. Nissim, A. Cohen, C. Glezer, and Y. Elovici, “Detection of malicious pdf files and directions for enhancements: A state-of-the art survey,” Computers & Security, vol. 48, pp. 246–266, 2015.

[3] Z. Imran and R. Nizami, “Advance secure login,” International Journal of Scientific and Research Publications, vol. 1, no. 1, pp. 1–4, 2011.

[4] G. Verma and S. Kanrar, “Secure document sharing model based on blockchain technology and attribute-based encryption,” Multimedia Tools and Applications, pp. 1–18, 2023.

[5] A.B. Garba, J. Armarego, D. Murray, and W. Kenworthy, “Review of the information security and privacy challenges in bring your own device (byod) environments,” Journal of Information privacy and security, vol. 11, no. 1, pp. 38–54, 2015.

[6] C. H. Wu, R. K. Chiu, H. M. Yeh et al., “Implementation of a cloudbased electronic medical record exchange system in compliance with the integrating healthcare enterprise’s cross-enterprise document sharing integration profile,” International Journal of Medical Informatics, vol. 107, pp. 30–39, 2017.

[7] H. V. Nguyen, “Cybersecurity strategies for universities with bring your own device programs,” Ph.D. dissertation, Walden University, 2019.

[8] E. R. Weippl, I. K. Ibrahim, and W. Winiwarter, “Content-based management of document access control.” in INAP. Citeseer, 2001, pp. 78–86.

[9] M. L. Gaid and S. A. Salloum, “Homomorphic encryption,” in The International Conference on Artificial Intelligence and Computer Vision. Springer, 2021, pp. 634–642.

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 370-377, November-2023

https://doi.org/10.47001/IRJIET/2023.711050

Citation of this Article:

K.K.K.P Wickramasinge, G.D.D Ekanayake, P.G.K.S Munasinghe, S.N Hettiwatta, S.M.B Harshanath, S.K Rajapaksha, "SecureSense: A Network Threat Detection and File Sharing System" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 370-377, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711050

****

