ISSN No:-2456-2165

Implementing Application in BYOD Environment to Gain Secure Access to Organization Resources

M.Y.A Sankalpa[1]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Perera I.U[2]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Perera M.G.D[3]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Dr. Lakmal Rupasinghe[4]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Dahanayake N.K[5]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Chethana Liyanapathirana[6]
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Abstract:- As remote work has gained significant momentum, many companies are allowing bring-your-own-device (BYOD) environments where employees are allowed to use personal devices to access work-related networks, systems, files and applications. As organizations increasingly embrace bring-your-own-device (BYOD) policies, security concerns are critical. Employees using their personal devices to access sensitive business data under BYOD poses several new concerns. This paper explores how organizations can challenge the overabundance of useless and outdated files, as well as the storage of documents that outlive their usefulness, lack of visibility into file severity, and identification of potential risks. Therefore, organizations must be aware of the location, nature and sensitivity of company collaboration data. Also, random, inconsistent, or unexpected behavior in a system is called anomalous behavior or simply anomaly. Analyzing system activity, defective detection, security scanning, failure, and risk prediction are all helped by ML integrated log analysis. Identification of anomalies align with the security risks not only enough. As a result, the AI-based recommendation system may be utilized to provide consumers individualized recommendations and feedback based on their preferences and areas of interest.

Keywords:- *BYOD, Organization, Application, Detection, user Behavior.*

I. INTRODUCTION

The Bring Your Own Device (BYOD) conception has gained a lot of traction in the modern corporate world, facilitating employees to use their own devices for duties associated to their jobs. [1]Due to the expanding use of mobile devices and the desire to use them for work or school-related purposes, this policy has gained popularity in recent years. BYOD policies can be beneficial for both employees and organizations, as they can increase productivity, reduce costs, and offer flexibility. Data storage has grown in importance as a concern for both consumers and businesses. It has become crucial to effectively manage storage given the rise of personal electronics like smartphones, laptops, and tablets. According to research [2] the average user has over 5,000 files on their device, many of which are duplicates or out of-date. BYOD data hoarding occurs when employees accumulate large amounts of sensitive data on their personal devices without proper security measures in place [3]. Sensitive corporate data is stored on personal devices beyond the control of the organization, which offers significant issues for data security and privacy. Personal devices could not be as secure as those owned by businesses, making them more vulnerable to attacks. As an example, outdated software or files may have security flaws that attackers might use to access private information. Furthermore, keeping confidential information on personal devices increases the risk of data breaches.

In this study present an advanced BYOD application that will enhance data security, provide complete insight into stored data, evaluate user activity, and detect abnormalities while maintaining privacy safeguards in order to mitigate these concerns.

The main goal of our research and development is to produce a comprehensive solution that enables organizations to implement a BYOD policy without affecting the security and privacy of their corporate data. Our solution has four essential components that all work under strict privacy protections: corporate data hoarding, complete visibility into stored data into specific folder, user behavior analysis, and anomaly detection.

Application enables organizations the opportunity to analyze all of the data that is kept on user devices. Administrators can control this functionality to keep monitor of and audit employee access to, modification of, and sharing of data. In application protects company assets and user privacy by utilizing secure protocols and encryption techniques to make sure that only authorized individuals may access to data stored in user devices. To understand and analyze user activity on the user device, this application uses machine learning algorithms, to analyze user behavior analytic algorithms. And application can identify abnormalities or differences from typical behavior by examining patterns, trends, and user interactions. This proactive approach allows for rapid detection of suspicious activity, such as illegal data access, unusual file transfers, or malicious software installs, allowing organizations to take immediate action to reduce possible risks.

In this application has privacy safeguards that ensure that user data is kept private and secure. By abiding by privacy laws and implementing privacy-enhancing technology, application value user privacy. It reduces the potential risk of personal information exposure while still enabling efficient analysis and recommendation features by integrating approaches like differential privacy, data anonymization, and secure computing.

II. LITERATURE REVIEW

Studies on duplication detection, identifying out-of-date program files, age-based document deletion, and digital data wiping allow significant insights for the development of effective and secure data hoarding techniques. These strategies enable organizations to effectively organize data in the BYOD setting using machine learning algorithms to provide improved storage management, greater security, and privacy protections. A machine learning-based strategy for duplicate file identification in BYOD contexts was provided by research by Li et al [4]. It achieved great accuracy in duplicate recognition by using a deep learning algorithm to extract information from the file content and metadata. Their study showed how machine learning methods can effectively deal with the problem of data duplication in BYOD storage. Maintaining the Integrity of the Specifications.

A BYOD system's stability and security may be at risk due to outdated application files. In a research Wang et al [5] presented, machine learning methods were used to examine program file versions. They proved the advantages of machine learning in automating the detection and removal of old application files in BYOD environments by detecting outdated files based on version comparison and user behavior analysis.

User devices usually collect a lot of data over time, sometimes including documents that are no longer essential or useful. Automatic deletion systems based on preset parameters, including document age, have been offered as a solution to this problem. The research [6] emphasized the value of automated document management for preserving a structured and effective BYOD environment. When employees leave the company or the devices are put to other uses, it is essential to ensure the secure removal of business data from BYOD devices. By developing a machine learning model on a huge dataset of device usage trends can increase the efficiency of digital data wipe operations by accurately predicting probable data remains.

Data visibility is a critical aspect of data management that refers to the ability to access and view data across an organization. It plays a crucial role in ensuring that data is accessible and usable by authorized personnel while maintaining security and privacy. In the context of implementing an application in a BYOD environment to gain secure access to organization resources, data visibility is an essential consideration to ensure that data can be accessed securely and efficiently [7]. The system will be able to track and examine data flows within the company's BYOD program, identify cooperative sensitive data, and implement the necessary security measures to prevent unauthorized access to the data. It will also be able to spot any unusual activities or changes in the location of the cooperative sensitive data's storage. To assess the degree of sensitivity of the data and implement the required security measures, the system will also employ current organizational security metrics, such as access control regulations and encryption standards.

Automated identification of sensitive data approach was introduced by Ziqi Yang and Zhenkai Liang in 2018. There have been multiple approaches suggested to locate sensitive information in that research report, but they have not used any machine learning, deep learning technologies. System will automatically delete the data with predefined policies. To identify sensitive data, Semantic Understanding and Implicit Specification was the challengers in that research paper [8]. Another research is concerned about the encryption of the data (Check whether the data is encrypted or not). Saudi Arabia introduced a way to check whether the data is encrypted or not by Khalid Almarhabi, Adel Bahaddad, and Ahmed Mohammed Alghamdi in January 2023 [9]. The problems, solutions, and best practices for providing safe access in a BYOD setting are all significant insights provided by these research studies. They cover a range of topics, including security frameworks, MDM tools, user behavior tracking, and location-based security, and serve as a solid foundation for comprehending and putting BYOD security measures into practice.

A random, nonconforming, or unexpected behavior within a system is referred to as an anomalous behavior, or simply an anomaly [10]. The research component aims to develop a system that utilizes Machine Learning to identify anomalies in BYOD activities, focusing on analyzing user behavior, malfunctioning detection, security scanning, and failure and risk prediction and integrating various system-level metrics [11].

Machine Learning has proven to be a powerful tool for anomaly detection, given its ability to analyze complex and dynamic datasets, making it well-suited for addressing security challenges in the BYOD landscape. Previous studies

highlight the significance of machine learning algorithms in identifying anomalies in BYOD activities by analyzing user behavior and detecting abnormal patterns that may indicate security breaches or unauthorized actions.

The literature identifies web traffic as a valuable data source for anomaly detection, as it provides insights into user behavior and activities. Researchers have successfully detected anomalies by monitoring and analyzing web traffic patterns, identifying unusual or suspicious browsing behaviors. Additionally, system-level metrics such as CPU, RAM, and Disk usage have been explored for anomaly detection. Aggregating and analyzing these metrics allows researchers to develop effective models that swiftly and accurately identify deviations from normal behavior.

This anomaly detection component aims to leverage Machine Learning techniques to aggregate and analyze web traffic data, background processes, CPU, RAM, and Disk usage to detect anomalies in BYOD activities. Imposing a consistent and higher-than-expected average task load intensity on the system might indicate an abnormality when it comes to resource consumption. [12]. By incorporating diverse data sources and employing appropriate Machine Learning algorithms, the research component seeks to develop a system that promptly and accurately identifies anomalies in the BYOD environment, enhancing cooperative security measures.

Furthermore, the facts show the significance of Machine Learning-based anomaly detection in the BYOD environment. By utilizing supervised and unsupervised learning techniques and integrating web traffic and system-level metrics, these methods have made notable progress in developing effective models for detecting anomalies in BYOD activities.

Companies that provide Bring Your Own Device (BYOD), which lets employees use their own smartphones and tablets for work, are multiplying in recent years. However, there are potential risks associated with using a private terminal rather than a business terminal, including the possibility of organizational data leaking or private data about employees being disclosed.

These dangers were thoroughly discovered in a prior study; however, they were based on the findings of a qualitative assessment. Additional quantitative evaluation is required to make risk mitigation more realistic. Additionally, new cost risk variables for BYOD were added to the findings of the prior study's risk analysis. Additionally, based on the findings, a quantitative study was carried out to confirm the product's effectiveness [13].

Organizations now frequently allow employees to bring their own devices (BYOD), which poses serious problems when they disregard security regulations. The human behavior in adhering to security policies, which is a major contributing element to security vulnerabilities [14], had not been addressed in previous assessments of the research topic, which had concentrated primarily on the technological challenges surrounding BYOD adoption.

Additionally, the primary goal of another research paper was to comprehend how firm employees felt about the security of the personal gadgets they used for work (BYOD). Prior studies also sought to ascertain the BYOD-related guidance and support that participant received from their employers [15].

III. METHODOLOGY

➢ *Corporate Data Hording in user Device*

Data hoarding comprises three sub modules:

Application will identify duplicate files, out-of-date program files, and automatically delete documents over a certain age to give users an effective and user-friendly way to manage their data storage. Machine learning methods will be used throughout implementation to increase the identification process's rapidity and accuracy.

- *Identification Duplicate Files:*

In this module responsible for detect duplicates saved in the corporate storage. Generated a sample dataset made up of files from user devices to detect duplicate files in storage. Took characteristics from the files that were both content- and metadata-based and trained a machine learning model using methods like deep learning and clustering. This model was then applied to categorize files as unique or duplicates depending on how similar their features were, offering a trustworthy method of handling duplicate data.

- *Identification Out-of-Date Program Files:*

In this module responsible for identify outdated programs. Created a dataset made up of program files from user devices to identify outdated program files. Version numbers, file locations, and timestamps, among other relevant attributes, were retrieved from these files. We developed a model to recognize outdated files by comparing versions and examining use patterns using machine learning methods like decision trees or support vector machines. This method made sure that possibly dangerous application files were found and deleted.

- *Delete Documents Over a Certain Age:*

When determining the maximum permitted age for documents, a pre-defined age parameters is used, this taking organizational policies and needs into effect. In order to avoid data recovery, implemented an automated deletion script, examined the dataset for documents that exceeded the threshold, and safely destroyed them.

In order to fulfill the intention for digital data wipe, use patterns and remaining data remnants were analyzed, and a machine learning model was developed to anticipate likely remains on devices intended for data wipe. Using this approach, we carried out safe data wipe processes to ensure that all critical company data was completely removed. The management of out-of-date software files, duplicate identification, automatic document deletion, and safe data

ISSN No:-2456-2165

wiping difficulties might all be addressed through the use of machine learning techniques and methodical procedures. The general security, effectiveness, and privacy of business data kept on user devices within the BYOD environment are improved by these advances.

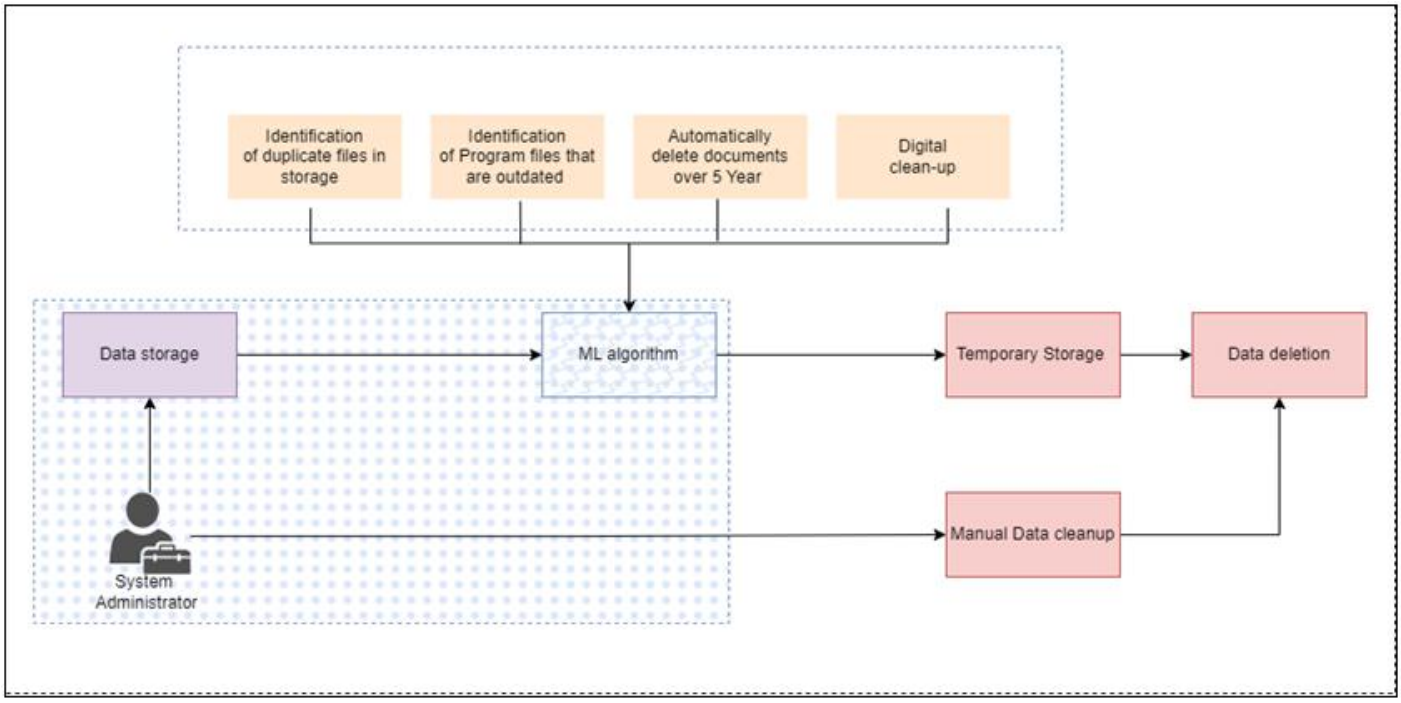

Fig 1 System Diagram

➢ *Corporate Data Visibility in user Device*

The implementation methodology for an application in a Bring Your Own Device (BYOD) environment, aimed at achieving secure access to organizational resources, comprises several essential steps.

The primary objective of this project is to deliver a web solution that enables organizations to effectively manage devices in a BYOD setting. The system empowers system administrators to capture data and filter out sensitive corporate information. It also allows them to pinpoint the exact location of these sensitive data, ascertain their nature, and determine their level of sensitivity. Moreover, the system focuses on detecting any suspicious activities, such as manual file renaming or changes in file location, triggering alerts for the administrators.

- *This Component of the System Possesses the following Capabilities:*

✓ Data Capture and Filtering: The system captures data and identifies and filters out sensitive corporate information.
✓ Location Identification: The system determines the precise location of the sensitive data within the organizational resources.
✓ Nature Identification: The system identifies the nature or characteristics of the sensitive data.
✓ Sensitivity Identification: The system determines the level of sensitivity associated with the corporate data.
✓ Furthermore, the system allows the system administrator to detect suspicious activities related to corporate files, such as changes in the file location of sensitive data.

The methodology for implementing an application in a BYOD environment to ensure secure access to organizational resources adopts a comprehensive approach to risk management and security controls, with the aim of safeguarding organizational assets.

In order to fulfill the intention for data visibility, location, nature, and sensitivity were analyzed, and a machine learning model was developed to identify any unusual activities or changes in the storage location of cooperate in organization. Application continuously keeps track of all files and checks for any unauthorized modifications or deletions.

➢ *ML Integrated Anomaly Detection System*

When developing an anomaly detection system that can analyze user behavior and detect anomalies in a BYOD context, certain essential steps must be taken as follows:

- Data Collection should be done to gather relevant data from the BYOD environment, including web traffic logs, system-level metrics (CPU, RAM, Disk usage), and information on background processes. This data will serve as the foundation for training and evaluating the anomaly detection system.

- Preprocessing is initiating to clean and preprocess the collected data to ensure consistency and compatibility. This step may involve removing outliers, normalizing data, and handling missing values, if any.

ISSN No:-2456-2165

- Feature Extraction is done to extract meaningful features from the collected data. This includes extracting relevant information from web traffic logs (e.g., URLs, timestamps, source/destination IP addresses) and deriving statistical features from system-level metrics (e.g., average CPU usage, maximum RAM usage).

- Machine Learning Model Development means developing a machine learning model, such as a supervised or unsupervised algorithm, to detect anomalies based on the extracted features. Think about using SVM, Random Forests, or clustering methods like K-means or Local Outlier Factor (LOF) to your data. Fine-tune and optimize the model parameters to improve its accuracy.
- Training and Evaluation is performed to split the dataset into training and testing subsets. Train the machine learning model on the training set and evaluate its performance using appropriate metrics (e.g., accuracy, precision, recall) on the testing set. Iterate this process to enhance model accuracy.

- Improvement and Adaptation is vital component of this task chain, because it continuously monitors the BYOD environment and collect new data over time. Regularly update and retrain the machine learning model to adapt to the evolving environment, incorporating new anomalies and ensuring ongoing accuracy improvement.

- Finally, the Performance Assessment should be done. It Assess the performance of the developed anomaly detection system by conducting experiments and comparative analysis with existing approaches. Evaluate the system's ability to accurately identify anomalies while minimizing false positives and false negatives.

➢ *AI based recommendation system*

Artificial intelligence (AI) is a contemporary technical technique for teaching computers to think or use their intelligence like humans do by copying traits, teaching them to make wise judgments, and teaching them to carry out tasks as directed. The demand for creating intelligent recommendation systems is currently enormous. A recommender system may be developed using a wide variety of tactics and techniques [13]. According to our research, content-based recommendation systems are utilized in BYOD due to their ability to target user behavior.

There are many different types of strategies and approaches that can be used to develop a recommendation system. One method is the content-based recommendation system. This indicates that under the content-based recommender technique, the products that are comparable to the former items picked by a certain user are recommended. The following are the fundamental ideas behind content-based recommender systems: The user-preferred items' descriptions are examined to identify the key characteristics that distinguish them from one another, and those choices are then recorded to user profiles [14].

With access control in BYOD environment and propose a dynamic access control framework based on the gathered context information. When a user attempts to connect his device to corporate network, device's context information is collected and forwarded to detection system. The accumulated information is analyzed and compared with user's normal behavior stored in the database, to identify normal and malicious users [15]. The user profile is compared to the attributes of each item to determine which goods to recommend, depending on how comparable they are. The result is sent to recommendation system that enforces access control based on these results and corresponding security policies. Finally, user can generate a recommendation log report.

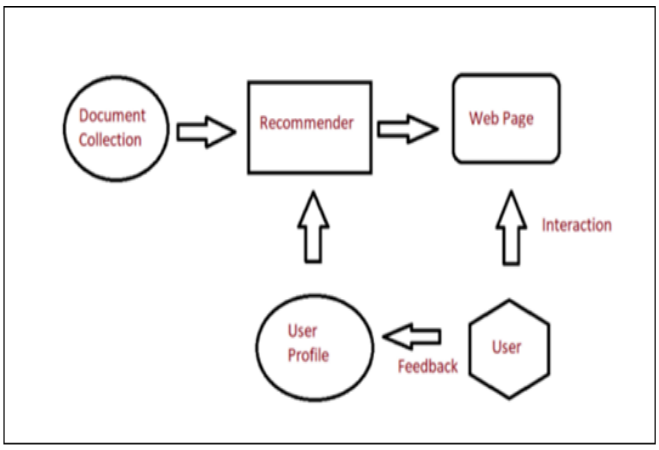

Fig 2 Data Analyzing to Detect Risks

As shown in the figure above, the data is first analyzed to see if there are any risks, if so, they are classified and then a recommendation is shown.

IV. CONCLUSION

To summarize, our research focuses on creating a comprehensive system that effectively tackles the challenges encountered in the Bring Your Own Device (BYOD) environment, ensuring secure access to organizational resources. This system consists of four key components that address different aspects of security and data management within the BYOD landscape.

Our research findings demonstrate the effectiveness of our system in enhancing security and privacy in BYOD environments, specifically for small to medium-sized companies. Given the rapid growth of BYOD practices, the system's scalability allows for future improvements and updates.

As the BYOD landscape continues to evolve, our system provides a solid foundation for organizations seeking to maintain secure resource access. By implementing our comprehensive solution, businesses can embrace the advantages of BYOD while minimizing risks, ultimately creating a productive and secure work environment.

In conclusion, our research contributes to the development of a flexible and robust system that effectively addresses security challenges in the BYOD environment. This system facilitates secure access to organizational resources while upholding privacy and data protection.

REFERENCES

[1]. F. S. ,. P. Hudan Studiawan, "Anomaly Detection in Operating System Logs with Deep Learning-Based Sentiment Analysis," Dependable and Secure Computing, vol. 18, pp. 2136-2148, 2021.
[2]. "Forcepoint," [Online]. Available: https://www.forcepoint.com/cyber%02edu/bring-your-own-device-byod.
[3]. R. Siciliano, "Best practices for BYOD data storage," Finextra, Boston, 2015.
[4]. Y. Z. S. C. W. &. W. L. Li, "Deep learning-based duplicate file identification in BYOD environments," Journal of Information Security, vol. 15, no. 4, pp. 345-359, 2017.
[5]. J. L. Q. S. T. &. J. M. Wang, "Machine learning approach for detecting outdated program files in BYOD devices.," in Proceedings of the International Conference on Mobile Computing and Security, Boston, 2019.
[6]. H. K. Y. P. J. &. L. S. Chen, "An intelligent document management system for BYOD using machine learning techniques.," Journal of Mobile Information Systems, vol. 25, no. 3, pp. 187-202, 2018.
[7]. F. L. M. L. S. L. A. Dedeche, "Emergent BYOD Security Challenges and Mitigation Strategy," Citeseer, Melbourne, 2013.
[8]. Z. L. Z. Yang, "Automated identification of sensitive data from implicit user specification," Springer, 2018.
[9]. A. M. A. K. A. A. B., "Security management of BYOD and cloud environment in Saudi Arabia," ELSEVIER, vol. 63, pp. 103-114, 2023.
[10]. A. M. M. M. S. Al-Haj Baddar, "Anomaly Detection in Computer Networks: A State-of-the-Art Review," University of Genova, Italy.
[11]. A. B. A. M. A. K. Almarhabi, "Security management of BYOD and cloud environment in Saudi Arabia," ScienceDirect, 2023.
[12]. D. A. M. R. D. a. M. S. I. Kohyarnejadfard, "A Framework for Detecting System Performance Anomalies Using Tracing Data Analysis," 3 August 2021. [Online].
[13]. M. I. T. K. H. S. A. K. T. E. S. T., "Risk Assessment Quantification for Bring Your Own Device Based on Practical Viewpoints," International Institute of Applied Informatics, 2022.
[14]. A. M. K. G. F. S. T. A. Wani, "BYOD usage and security behaviour of hospital clinical staff: An Australian survey," International Journal of Medical Informatics, 2022.
[15]. A. A. N. M. L. M. K. R. Palanisamy, "BYOD Policy Compliance: Risks and Strategies in Organizations," 2020.