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

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 329-334, November-2023
https://doi.org/10.47001/IRJIET/2023.711045

Enhancing Security in a Corporate BYOD Environment

[1]Rathnayaka R.P.P.S, [2]Swarnamali I. S, [3]Piyasekara W.D.C, [4]Karunathilaka N.A, [5]Kavinga Yapa Abewardena, [6]Kanishka Yapa

[1,2,3,4,5,6]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
Authors E-mail: [1]poornasujampathi@gmail.com, [2]sadikaswarnamali@gmail.com, [3]dilankachamath1@gmail.com, [4]nimaniashadini@gmail.com, [5]kavinga.y@sliit.lk, [6]kanishka.y@sliit.lk

***Abstract* - Bring your own device (BYOD) is a concept of employees using their personal devices to access the organization's network and resources. While it provides advantages such as increased efficiency and productivity, it also provides security risks to organizations such as data breaches and security issues, if an employee's device is stolen or lost and vulnerable to malware and other security threats since the personal devices are not secure than company-owned devices. To enhance corporate infrastructure security in a BYOD environment, this paper proposes four mechanisms by addressing four issues. The first mechanism is preventing users from accessing the organisation's documents after their termination which helps to protect confidentiality. Second, detecting suspicious user behaviour through location-based anomaly detection helps to identify whether the device is stolen or lost. Third, assigning permissions based on user roles using a Universally Unique Identifier (UUID) prevents unauthorized device access. Furthermore, employing an Application-Aware Virtual Network Adapter solution helps identify data types and ensures secure usage of corporate data simultaneously. By combining these features, a robust security environment can be achieved, effectively mitigating the risks associated with BYOD. Adopting these comprehensive security approaches allows organizations to reduce BYOD-related risks and safeguard their sensitive data effectively.**

Keywords: DLP, AAVNA, Anomaly Detection, UUID, BYOD.

I. INTRODUCTION

Nowadays, Bring Your Own Device (BYOD) has rapid growth since numerous organizations have moved into the Bring Your Own Device (BYOD) with the COVID-19 pandemic. The main concept behind BYOD is to provide employees access to the network, applications, and various information resources of the company using their own devices such as mobile devices, laptops, tablets, and others, whether they are internal or external to the work environment[1].

This approach offers several advantages to the organization, such as cost reduction in device management and increased flexibility for employees, improved efficiency of the work [2].Within these advantages, is driving a greater embrace of the BYOD concept in corporations. BYOD allows employees to utilize corporate information, making productive and efficient options. While corporations are primarily concerned with technology-related issues such as data confidentiality, integrity, and availability (CIA), it is critical to recognize that the BYOD concept creates new security risks and difficulties.

Security issues usually occur with any new technologies. Even though BYOD concepts have been used few years, this concept's security issues have increased[4]. Based on a survey of cybersecurity specialists BYOD Statistics (2023), 62% cited loss of information and breaches as the top security risk with BYOD adoption[5]. BYOD security issues include people installing inappropriate materials or applications (54%), misplaced or stolen machines (53%), unauthorized access to corporate information and systems (51%), malware (51%), and exploits of vulnerabilities (48%).To confirm the complete security of information in the context of BYOD practice, these developing challenges must be properly evaluated[3].

A study concentrating on privacy and security problems in BYOD contexts discovered that the primary causes leading to these issues were technological issues, a lack of policies, a lack of security controls, a shortage of knowledge about security, and inadequate privacy protections [6].

This research proposed a comprehensive solution to the security threats from Bring Your Own Device (BYOD). The primary goal is to detect and prevent unauthorized activities on BYOD devices, protecting the enterprise from potential BYOD security issues and threats. The sub-goals include implementing a Data Loss Prevention (DLP) system to protect confidential data from being used by terminated employees or unauthorized access to the organization documents, establishing a dynamic user behaviour anomaly detection system to detect and thwart unauthorized access attempts based on the location of the employee, introducing an enhanced access control mechanism with role-based permissions to prevent unauthorized device access and services, and proposing an Application-Aware Virtual

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 329-334, November-2023

https://doi.org/10.47001/IRJIET/2023.711045

Network Adapter (AAVNA) to intelligently route traffic, ensuring corporate security.

The paper is structured as follows. A literature review of this suggested solution is presented in Section II.The methodologyis presented in Section III. Results and discussion of this solution are presented in Section IV. Section V provides concluding notes at the end.

II. LITERATURE REVIEW

The growing BYOD concept is involved in security issues, including data loss, leaking, device theft, and unauthorized access. This review aims to contextualize the suggested framework, assess its effectiveness, and provide an understanding of its comparative advantages over typical strategies by examining previous research and approaches which are implemented for BYOD working environments.

The authors in this research paper[7] evaluates how BYOD security solutions were implemented in an Oman-based higher education facility. BYOD is the practice of allowing employees to use their own mobile devices for work-related activities. The risks of BYOD are highlighted in the study, including the possibility of data loss due to mobile device loss or theft. The research collects qualitative and quantitative data to analyze the usage of the network and the services accessed by users. The paper proposes using authentication processes such as 802.1x, CA, and Radius to control user access and secure the network.

The authors in this research paper [8]introduces security mechanism of Bring Your Own Device (BYOD) security in corporate environments, primarily focusing on the potential risks and the development of an adaptive security policy model. The paper acknowledges the advantages of BYOD, including enhanced employee satisfaction and efficiency, but also underscores the significant security concerns like data theft and unauthorized access. To address these challenges, the paper proposes the creation of an adaptive security technique and an intelligent filter that leverages user behaviour and context for access control. This approach aims to detect unusual behaviours, protect against advanced threats like phishing, and ultimately enhance the security of both devices and data in BYOD environments. The research methodology involves quantitative methods and experimental analysis to validate these concepts and potentially bridge the access control gap in BYOD settings.

The research's suggested solution[9]introduces a context-based dynamic access control scheme. A Collection System, a Detection System, and a Control System are the three main parts of this system that make it function. The Collection System gathers context data from devices without agents, using methods like network packet analysis and DHCP fingerprinting. If abnormal behaviour is detected, an agent can be installed for more precise data collection. The Detection System profiles users' normal activities, storing this data in a database and creating behaviour profiles. Abnormal behaviours are then identified in real-time by comparing against these profiles. The Control System enforces access control based on detection results and predefined policies, utilizing both existing solutions like MDM and NAC and innovative methods like dynamic access privilege adjustments. This comprehensive approach enhances security in BYOD and smart work environments by swiftly identifying and mitigating abnormal and malicious behaviours.

The proposed solution of [10] framework utilizes dynamic adaptive context and machine learning techniques to mitigate the risks of infiltration, exfiltration, or tampering of sensitive information on BYOD devices. This approach addresses three types of intruders, including those who mimic the behaviour of legitimate users to gain unauthorized access to an organization's IT infrastructure and data.

III. METHODOLOGY

Implemented a security solution for BYOD issues using four main components. It consists(Fig.1) of a confidential data retrieval policy manipulation, dynamic user behaviour anomaly detection, enhanced access control mechanism, and application-aware virtual network adaptation.

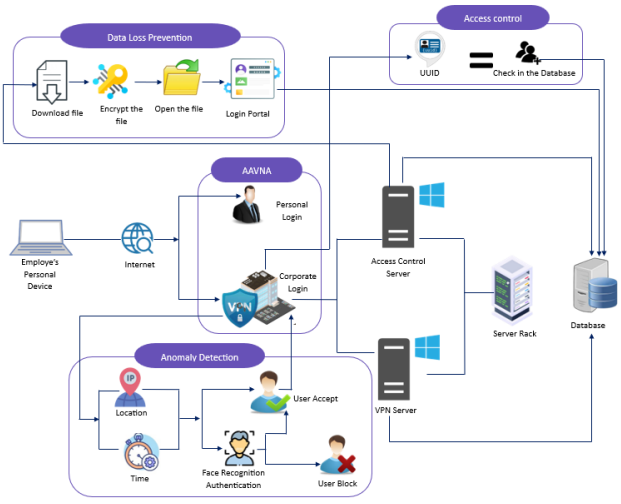

Figure 1: System diagram of the proposed solution

A) Confidential data retrieval policy manipulation

The phrase "Data Loss Prevention" refers to a collection of tactics, technologies, and procedures designed to prevent sensitive information from being leaked, lost, or exposed to unauthorized parties. After the employee’s termination from

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 329-334, November-2023

https://doi.org/10.47001/IRJIET/2023.711045

the organization, this solution prevents access and modification of critical documents.

Figure 2: File Explorer Panel

First, the employee's identity is verified using a File Explorer panel (Fig 2.). This panel shows all the files that employees have access to download. Then the employee can select the file and download it to their local machine. The cryptographic algorithm used for encryption and decryption is AES-265. When the file is downloaded, the file is in the encrypted format. Employees can only decrypt the file using the file explore panel. Without the file explore panel, employees cannot access the files in the organization.

B) Dynamic user behaviour anomaly detection

This component suggests a method based on dynamic user behaviour anomaly detection to strengthen the BYOD concept. The approach uses a methodical series of procedures to find abnormal access patterns based on the temporal and spatial details of user interactions.

Data preprocessing is an essential phase in ensuring that the raw input data is turned into a structured format suitable for further analysis and modelling. It plays a crucial role in enabling accurate and effective anomaly identification. The procedure consists of a number of phases. To extract important attributes the hour of access and the day of the week, feature engineering is used. These characteristics enhance the anomaly identification process by providing useful temporal insights. Geographic coordinates—latitude and longitude—are normalized, aligning them with other features, to reduce the impact of various scales. Latitude, longitude, hour, and day of the week are the parameters that are ultimately identified during the feature selection step and are crucial for training the subsequent anomaly detection model. The dataset is then split into separate training and testing subsets, allowing the model to pick up on existing patterns while still ensuring that it can evaluate previously unobserved data.

The methodology uses the Isolation Forest algorithm as the foundation of the anomaly detection system, building on the processed dataset. By separating anomalies into separate branches of a randomized binary tree, the Isolation Forest algorithm excels at finding anomalies within multidimensional data[11][12]. The model is trained on the chosen attributes, including latitude, longitude, hour, and day of the week, enabling it to spot changes from typical patterns of activity. In order to improve model generalization, an anomaly proportion hyperparameter must be calibrated to provide balanced sensitivity to both normal and anomalous events.

By identifying incoming user access attempts as normal or anomalous based on departures from established patterns, the trained Isolation Forest model is used for anomaly prediction. In addition to identifying potential risks, face recognition mechanisms to authenticate the user. This two-layered strategy also imposes strict authentication rules to deter unauthorized access attempts.

After detecting the anomaly, the system does not know this is legitimate action or not. For example, Ann is work from home regularly, but she visits his mothers house in work day. According to the system, when she visit her mother's house, she will get a error message of anomly detection. Since it is a legitimate action, there should be a strong mechanism for validate the user. Face recognition comes in to play for addressing that problem.

Face recognition is done by using multi person face recognition CNN model. The process of face recognition is capturing user face images, save that it to the folder and trained the model using the muti person face recognition CNN model.

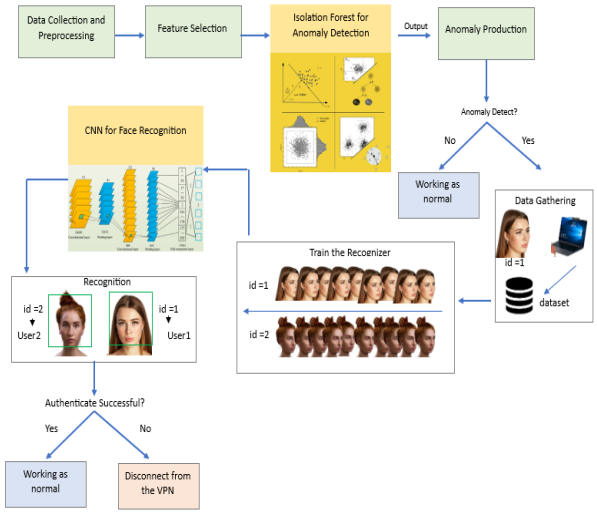

Figure 3: System diagram for user behavior anomaly detection

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 329-334, November-2023

https://doi.org/10.47001/IRJIET/2023.711045

C) Enhanced access control mechanism

UUIDs are used as a safe and scalable authentication technique in the approach to UUID-based access management in a BYOD website. A UUID is a digital identification that is given to each individual user or piece of hardware [13]. The online portal, known as an access control web portal, is used to store and retrieve users' UUIDs. An administrator is the primary user with the most privileges in this portal. The web portal's admin user may generate new users and provide them with UUIDs. This procedure guarantees that the portal's resources and services are only accessible to approved devices and users who possess valid UUIDs. In addition, UUIDs provide an increased degree of security in comparison to conventional passwords due to the fact that it is substantially more difficult to guess or break them[14]. This strategy offers a solution that is both flexible and efficient for managing access control in a BYOD environment. As a result, it promotes a smooth and secure user experience.

Within the domain of computer systems, the use of installed agents has considerable importance, enabling us to explore the distinctive characteristics that delineate individual machines. One notable component is the UUID linked to a particular personal computer, which serves as a distinctive digital fingerprint distinguishing it from the extensive array of devices. Upon the extraction of the UUID by the deployed agent on a specific computer, a multitude of potential outcomes are made accessible, including the ability to establish a connection between such UUID and an assigned user. Mongo DB is a suitable NoSQL database management system for storing UUIDs and user information pertaining to the use of organizational resources. By using the features of MongoDB, it is possible to easily cross-reference the obtained UUID with stored records, quickly revealing the associated UUIDs linked to a particular user.

The potential to enhance human comprehension and manipulation of digital environments is held by this method, which is supported by the symbiotic relationship between deployed agents and MongoDB. This potential is evident in several aspects such as customized user experiences, targeted assistance, and security measures.

D) Application-Aware Virtual Network Adapter (AAVNA)

The proposed research methodology involves the development and evaluation of a comprehensive network management solution comprised of a network adapter web application and a network simulator prototype. This solution aims to provide efficient network administration, VPN creation, device allocation, and IP address collection. The network adapter application is constructed using fundamental web technologies.

Concurrently, a network simulator prototype is being developed due to the unavailability of existing simulators and server configurations. This web-based application will emulate network scenarios akin to established tools like GNS3 or Cisco Packet Tracer[15][16]. The goal is to visually showcase the functionalities of the network adapter application, emphasizing the network administrator's role and interactions. This prototype will be linked to the primary network adapter application.

The research methodology revolves around constructing a self-contained network environment that adheres to industry standards and regulations, including IEEE guidelines. By creating a coding-based ecosystem, the need for third-party software or external servers is obviated, streamlining the network processes. Devices and users are dynamically registered within the system as they access the network application.

To evaluate the proposed solution, a multi-step approach will be followed. Firstly, the network adapter's efficacy in network administration, VPN allocation, and device management will be examined through real-world scenarios. Secondly, the network simulator's accuracy in emulating complex network interactions will be assessed. User feedback and system performance metrics will inform the evaluation. Ultimately, the research aims to demonstrate the viability of an integrated coding-based network management solution that facilitates streamlined administration, ensuring adherence to standards and efficient user interaction.

IV. RESULTS AND DISCUSSIONS

Tokyo check-ins are included in the Four Squre dataset, which was compiled from 12 April 2012 to 16 February 2013 over a period of around 10 months [17]. 573,703 check-ins in Tokyo are included. Each check-in is linked to a time stamp, a set of locations, and a set of venue classifications. Initially, this dataset was used for studying the spatial-temporal regularity of user behaviour in LBSNs [18].

As presented anomaly score(Fig 4), the obtained anomaly scores from our dataset were subjected to analysis using the Isolation Forest algorithm, aligning with the methodology described earlier. The algorithm effectively assigned higher anomaly scores to instances that exhibited substantial deviations from normal behaviour. Notably, the anomaly scores indicated a notably higher likelihood of anomalies, with a range of scores between -0.541 and -0.624. The lowest anomaly scores, approaching -0.453, were associated with instances displaying behaviour more consistent with the established norms of the system.

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

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 329-334, November-2023

https://doi.org/10.47001/IRJIET/2023.711045

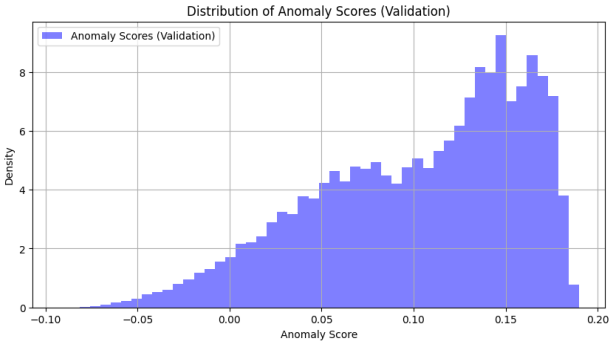

Figure 4: The distribution of anomaly scores

In our anomaly detection model, we achieved an accuracy of 80% (Fig 5.). The percentage of accurate predictions the model made is indicated by accuracy matric. Furthermore, our model archives a 100% accuracy rate in detecting anomalies, demonstrating exceptional precision. This shows that our model consistently identified an instance as an anomaly when classifying it. Our accuracy for typical occurrences was slightly lower at 67%, indicating that some instances were misclassified as anomalies. Despite this, our model performed exceptionally well in recall, especially for normal instances (100%), making sure that it properly identified all normal instances. The recall rate for anomalies was 67%, indicating that the majority of anomalies in the dataset were correctly identified by our model. For both the anomalous and normal classes, the F1 scores, which balance precision and recall, were excellent at 80%. Two real positives, one false positive, and two true negatives were identified by our confusion matrix. In conclusion, our model displays a great capacity to spot anomalies while keeping a respectable level of overall accuracy.

```
Accuracy: 80%
Precision (Anomaly): 100%
Precision (Normal): 67%
Recall (Anomaly): 67%
Recall (Normal): 100%
F1 Score (Anomaly): 80%
F1 Score (Normal): 80%

Confusion Matrix:
[[2 1]
 [0 2]]

Classification Report:
              precision    recall  f1-score   support

      Normal       1.00      0.67      0.80         3
     Anomaly       0.67      1.00      0.80         2

    accuracy                           0.80         5
   macro avg       0.83      0.83      0.80         5
weighted avg       0.87      0.80      0.80         5


Macro Average Precision: 0.83
Weighted Average Precision: 0.80
Macro Average Recall: 0.83
Weighted Average Recall: 0.87
Macro Average F1 Score: 0.80
Weighted Average F1 Score: 0.80
```

Figure 5: Model Confusion Matrix

The graph (Fig.5) shows the training accuracy and training loss curves for face detection model. As the number of epochs increases, both curves decrease. This suggests the model is improving its ability to fist the training set of data.

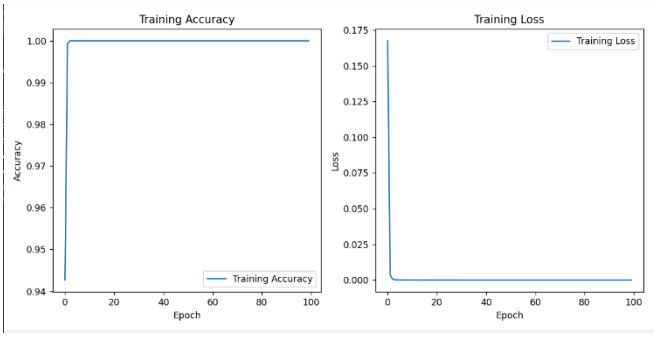

Figure 6: Training accuracy and loss

V. CONCLUSION

In conclusion, our comprehensive look into numerous aspects of protecting Bring Your Own Device (BYOD) environments has produced impressive results that collectively contribute to improving the overall security and effectiveness of such systems. By utilizing encryption, validation checks, and user association protocols, the development of a Confidential Data Retrieval Policy Manipulation approach has shown enormous promise in protecting both corporate and user data. Additionally, the Dynamic User Behavior Anomaly Detection technique, applying the FourSquare dataset, has successfully identified anomalous behavioural patterns through intuitive visualizations and Isolation Forest-based anomaly ratings, providing a key step towards proactive threat identification. The implementation of an Enhanced Access Control Mechanism, powered by Universally Unique Identifiers (UUIDs), has led to increased safety measures, faster onboarding and offboarding processes, and a more reliable access control framework. By making network administration, VPN allocation, and IP address management user-friendly, the Application-Aware Virtual Network Adapter (AAVNA) has demonstrated its value. Network robustness is further increased by the use of in-app security mechanisms. In conclusion, our research reveals a thorough strategy that not only closes existing security vulnerabilities but also lays the groundwork for revolutionary improvements in BYOD network administration, promising operational effectiveness, adherence to industry standards, and improved security measures.

ACKNOWLEDGEMENT

Our sincere appreciation also goes to the research panel for their insightful feedback. We are grateful to SLIIT for providing a supportive platform for our successful research.

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 329-334, November-2023
https://doi.org/10.47001/IRJIET/2023.711045

REFERENCES

[1] H. A. B. Alotaibi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," Saudi Arabia.

[2] Y. H. P. M. T. Oktavia, "Security and Privacy Challenge in Bring Your Own Device Environment: A Systematic Literature Review," in International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 2016.

[3] M. M. R. a. Y. Wang, "BYOD-Insure: A Security Assessment Model for Enterprise BYOD," in 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ) pp. 1-10, doi: 10.1109/MOBISECSERV.2019.8686551., Miami Beach, FL, USA, 2019.

[4] R. M. P. a. P. R. B. N. M. C. Galego, "BYOD : Impact in Architecture and Information Security Corporate Policy," in 17th Iberian Conference on Information Systems and Technologies (CISTI) pp. 1-2, doi: 10.23919/CISTI54924.2022.9820043., Madrid, Spain, 2022.

[5] J. Howarth, "24+ Fascinating BYOD Statistics (2023)," 1 December 2022. [Online]. Available: https://explodingtopics.com/blog/byod-stats.

A. G. a. M. D. a. A. J. Bello, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments," in Information \& Computer Security, pp. 475--492, 2017.

[6] W. S. Khoula AlHarthy, "Implement Network Security Control Solutions in BYOD Environment," in 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 29 Nov. - 1 Dec. 2013.

[7] A.A. &. P. B. Z. Musa Abubakar Muhammad, "Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access".

[8] J. O. a. C. I. Eun Byol Koh, "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment," in Proceedings of the International MultiConference of Engineers and Computer Scientists 2014 Vol II, IMECS 2014, Hong Kong, March 12 - 14, 2014.

[9] T. Z. Daniel Petrov, "Context-Aware Deep Learning-Driven Framework for Mitigation of Security Risks in BYOD-Enabled Environments," in IEEE 4th International Conference on Collaboration and Internet Computing, 2018.

[10] W. Z. Z. Dong Xu, "An Improved Data Anomaly Detection Method Based on Isolation Forest," in 10th International Symposium on Computational Intelligence and Design, 2017.

[11] K. M. T. Z.-H. Z. Fei Tony Liu, "Isolation Forest," in Eighth IEEE International Conference on Data Mining, 2008.

[12] M. M. Paul J. Leach, "A Universally Unique IDentifier (UUID) URN Namespace," 2014.

[13] "Management of UUID and version number of data sets," in International Reference Life Cycle Data System (ILCD) Data Network, EUR 25198, 2012.

[14] G. J. G. A. D. R. M. M. A. C. a. P. M. P. Gil, "Computer networks virtualization with GNS3: Evaluating a solution to optimize resources and achieve a distance learning," in IEEE Frontiers in Education Conference (FIE) Proceedings, Madrid, Spain, 2014, pp. 1-4, doi: 10.1109/FIE.2014.7044343., 2014.

[15] F. J. a. K. K. J. Janitor, "Visual Learning Tools for Teaching/Learning Computer Networks: Cisco Networking Academy and Packet Tracer," in Sixth International Conference on Networking and Services, Cancun, Mexico, pp. 351-355, doi: 10.1109/ICNS.2010.55., 2010.

[16] Kaggle, "FourSquare - NYC and Tokyo Check-ins," Kaggle, [Online]. Available: https://www.kaggle.com/datasets/chetanism/foursquare-nyc-and-tokyo-checkin-dataset.

[17] D. Z. V. W. Z. Z. Y. Dingqi Yang, "Modeling User Activity Preference by Leveraging User Spatial Temporal Characteristics in LBSNs.," in IEEE Trans. on Systems, Man, and Cybernetics: Systems, (TSMC), 45(1), 129-142, 2015.

Citation of this Article:

Rathnayaka R.P.P.S, Swarnamali I. S, Piyasekara W.D.C, Karunathilaka N.A, Kavinga Yapa Abewardena, Kanishka Yapa, "Enhancing Security in a Corporate BYOD Environment" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 329-334, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711045

****

