An Overview Of Security Challenges In BYOD Environment

Rhea Benedicta D'souza
Computer Science Engineering
St. Joseph Engineering College
Mangalore, India
18cs097.rhea@sjec.ac.in

***Abstract*—Bring Your Own Device (BYOD) is a swiftly rising trend in organizations that deal with digital technologies. Businesses that employ BYOD policies face a unique set of security concerns. Despite recent articles indicating a clear understanding of the risks associated with introducing BYOD into the workplace, it remains an underappreciated issue when compared to other IT security concerns. This paper focuses on BYOD security challenge. In addition to this solutions to security challenges are assessed to determine their limitations.**

Keywords— BYOD, BYOD security

I. Introduction

BYOD (Bring Your Own Device) is a developing trend in which employees bring their own gadgets to work. Smartphones are the most common example, but tablets, laptops, USB drives, and even e-readers are often used. BYOD is a result of the IT consumerization trend in which employees are becoming consumers. Many enterprise proprietors and personnel mistakenly trust that every one of the records on their private devices, together with smartphones and tablets, are absolutely safe. This is a risky false impression that would turn out to be costing organizations pretty a piece of money, doubtlessly millions. BYOD creates 3 foremost risks: records leaks, far-flung get right of entry to assaults, and malware infections. Malicious software programs may be used to thieve private records via means of remotely getting access to non-public and private agency information, together with whole database backups, through the employee's private device. Think of a pc virus that could infiltrate and thieve any non-public records saved on an employee's domestic pc, even as they're linked to the net through their cellular device. This isn't always a stretch of the imagination. It's far honestly a developing problem amongst safety experts. Furthermore, malware can infiltrate the BYOD network via an infected smartphone or tablet. Employees bring their smartphones or tablets to work or use them at work for business purposes. They may download malicious applications from untrusted third-party sources that contain viruses and Trojan horses that have the ability to infiltrate vulnerable networks undetected.

II. Related work

BYOD protection is regularly a trouble for agencies. This is because of the truth that, if you want to be effective, agencies should hold a few degree of manage over non-company-owned smartphones, tablets, and computer systems which can be the non-public assets of personnel. BYOD protection rules are turning into greater usually applied and widespread through each companies and their personnel as BYOD has turn out to be greater widespread and information of protection troubles has grown.When considering the risks of BYOD computing, research show that anything from data contamination to user
behaviour to criminal syndicate operations must be considered. Data leakage and virus are examples of unintended effects that emphasise the need to improve enterprise data security. Additionally, businesses must place a high priority on data security in order to safeguard sensitive information such as intellectual property. Organizations must also focus on securing their data rather than distinguishing between devices on the corporate network and those outside of it. Fortunately, recent progress has been made toward three crucial milestones. Instead of device management, Microsoft incorporated APIs into the Office 365 apps to help with mobile app management. The difference in language is modest, yet it has a huge impact. It means you can protect your data without having to manage the devices of your staff. The term User Enrollment was coined by Apple (as opposed to device enrollment). This is a critical realization for millions of businesses who wish to enable their staff to utilize apps on BYOD iPads and iPhones in a secure manner. User enrolment establishes a separate logical area where work data is safe while personal
apps and data are hidden. Work Profiles were designed by Google/Android to keep work data in a distinct container on a personal device.

III. Literature review

The work proposed by Felix. C. Aguboshim and Joy. I. Udobi states that Bring your device (BYOD) may be a system that enables staff to access protected company knowledge from anyplace victimization of their mobile devices. Permitting employees to use their own devices or buying mobile devices for them may be wont to implement BYOD. This paper's author highlights the protection risks and data leaks related to mobile electronic transactions (MET). The study's primary purpose is to show IT and security professionals a way to subsume the foremost frequent BYOD security threats, vulnerabilities, and hazards. To befit any sort of security breach, IT managers responsible for BYOD security should adopt excellent policies that support policy objectives, concepts, norms, and standards, as well as good formulation and communication. Organizations must implement privacy controls and countermeasures to safeguard e-mails sent outside the company, establish and forestall spam, phishing attacks, and malicious links and attachments in e-mails sent outside the company. Unintentional, intentional, and malevolent knowledge leaks are the 3 varieties of data leaks. There are several advantages to this. MET with efficiency implements a Bring Your Device (BYOD) policy, that supports worker satisfaction and will increase job efficiency flexibility. Mobile devices feature business apps that

maintain cloud property with knowledge services like Dropbox, yet as devices that may hook up with any offered network, despite whether or not or not it's trusty by the enterprise. A rise in price savings, resembling the initial device purchase, continuous device usage, and IT help desk support, as staff brings their own devices to work. Among the downsides are: permitting employees to access company data on their own devices creates data protection requirements. The foremost troublesome facet of BYOD is keeping work data secure and breaking away consumers' personal information. Infosystems is exploited by an increase in human vulnerabilities. Confidentiality, integrity, and accessibility are all troublesome to maintain. knowledge discharge can occur as a result of lost devices, which might be caused by an absence of understanding that ends up in an employee's operative in an exceedingly dangerous manner.[1]

The work proposed by MD Iman Ali, Sukhkirandeep Kaur, Aditya Khamparia, Deepak Gupta, Sachin Kumar, Ashish Khanna and Fadi Al-Turjman shows that a complete start to finish eco-framework is required to complete the legal examination cycle for the cybercrime system and the regulation of noxious exercises. During the investigation, they used a hazard extraction instrument that used specified spot sandblast and Cisco ISE for AAA, as well as Palo Alto. Using these devices, they were able to build a BYOD basis where harmful actions could be identified and investigated. In the principal period of this examination, BYOD clients were kept in a remote put over the web to interface with the corporate organization without a VPN where noxious action was distinguished utilizing Cloud Security. During the second phase of the study, BYOD customers were retained inside the corporate network and connected through remote, where spiteful behaviour was detected using on-premise security. In the third stage, BYOD clients are kept remote over the web without VPN and cloud administrations where the vindictive movement was identified utilizing on-prem 3-layer security. benefits incorporate Detection of cyberattack in BYOD climate was identified utilizing designated spot innovation. Observing and identification of dangers was directed utilizing cloud outer security incorporation utilizing GCP (Google Cloud Platform) that improved the security. DOS assault in rush hour gridlock location in BYOD security was distinguished. The HIP boundary has utilized that need to run and deal with different security applications to ensure PCs, like anti-virus, against spyware, and firewalls. Among the drawbacks is the digital assault was positioned as a worldwide danger and because of COVID-19 pandemic circumstances defenseless and assailants were focusing on associations because of changing traffic designs during WFH. PC and information robbery of workers leaving their PCs open is a significant danger for malevolent assaults. With cutting-edge level security set up, building a digital legal BYOD got foundation might be investigated further.[2]

The work proposed by Akeju, O., Butakov, S. and Aghili, S is about the data security and protection hazard related to utilizing versatile and implanted gadgets for learning in the K-12 setting was distinguished in this study report. This study centers around two parts of BYOD and IoT risks. The NIST security hazard the executive's model (NIST-8062) was utilized to feature the protection worries of K-12 biological system players that were considered when BYOD/IoT innovations were created. Pride costs, direct business costs, and rebelliousness costs are exceptionally significant contemplations. Proposed hazard examination to recognize explicitly accepted procedures in light of ISACA, IIA, SANS, and NIST proposals. BYOD's handbook for the K-12 programme in two Canadian jurisdictions (Alberta and Manitoba) adopted the recommended recognised norms with the purpose of further developing its goods.The benefits are NIST Privacy system has a bunch of controls that can assist an association with recognizing security hazards inside their handling environment. The National Institute of Standards and Technology (NIST) provides information on core procedures, as well as hazard assessments and a detailed examination of the BYOD structure's flaws. K-12 biological system gives adequate opportunity to the dominance of ideas and abilities, creates deep-rooted learning. drawbacks are Log documents and frameworks reviews are kept uniquely for 30 days in certain organizations that can be deceived by the NIST system. Many (if not most) organizations today don't oversee or get their cloud foundation. Executing K-12 in schools and universities will be troublesome as numerous understudies will not have the option to utilize their gadgets[3]

The purpose of Hai Vu Nguyn's proposed research was to look into the tactics used by software development (IT) network of thousands in a university setting to protect a BYOD-friendly environment. IT security experts from the California state University institutions conducted several investigations after controlling the network location where BYOD was implemented for at least two years. The research idea was built around the principle of defensive promotion. Data gathered through chats. PMT was utilized to analyze the ethical context of IT workers and gave extra information on conflicting viewpoints, KAP, and TPB through the conceptual framework. According to how the research operates in professional practice and promotes societal change, the study was presented in the way the data was acquired, analyzed, and verified. By enhancing student credentials through cyber security, with appropriate security measures accessible. Unauthorized access to the network and data is prevented. The PMT framework was utilized to decipher the replies of the grades that examine persons who may pose a hazard. There are dangers. The interview site differed depending on the location of each institution or location. The relevance of cybersecurity is not understood by the faculty. There is no network address translation (NAT). Security regulations, training requirements, and access control mechanisms are all unfamiliar to the participants. [4]

The work proposed by Fara Jamal , Mohd. Taufik Abdullah, Azizol Abdullah and Zurina Mohd. Hanapi examines the Bring Your Device (BYOD) authentication method in depth. The review's major goal is to identify prevailing BYOD authentication methods, distinguish BYOD security thresholds, and evaluate the threshold strategy. According to the findings of the assessment, there are 25 verification methodologies proposed by industry and educational

institutions that are appropriate for use by BYOD to increase security by avoiding and detecting data leaks in the enterprise. Data Source, Search Strategy, Research Selection, and Terms of Installation and Release are all part of the search process for these tactics. Organizations can keep their networks safe by restricting access to protected resources to only authorised users or processes. Protects the company by ensuring that only authorized users have access to the network and apps. The method is based on the patterns of user activity. It may take longer to learn user routines and discover unexpected activity, Only concerned with user authentication. There is no additional control after the user has verified authentication. The server stores user and device verification information. The user may not be able to be authenticated if the server is hacked. [5]

The work proposed by Mohammed Ketel examines the many ways and solutions that businesses can employ to address the security risks connected with BYOD. Software- Defined Networking (SDN), Enterprise Mobile Management (EMM) solutions and Network Function Virtualization (NFV) are some of the concepts discussed. Any EMM system must start with mobile device management (MDM). The primary goal of MDM is to manage, deploy, secure, and monitor BYOD devices in the workplace. IT administrators can remotely configure and control devices after enrolling them in the MDM server. Alternatively, because it provides intelligent orchestration, granular network control, and provisioning, SDN is touted as a viable approach to manage the entire network. Network Function Virtualization is another important new technological advancement that will enable BYOD to reach its full potential (NFV). SDN and NFV are not mutually exclusive, rather they are complementary. Through virtualization, SDN can help NFV perform better, and NFV can help SDN perform better. A range of solutions, including policies and technology controls, can be used to manage and secure BYOD. This article discussed the technological methods that businesses may utilise to safeguard BYOD. These systems could make use of a variety of network technologies. The SDN strategy has several advantages, including its simplicity and capacity to evolve, allowing it to adapt to changing needs. The SDN paradigm also provides a simple, highly scalable design as well as an extremely simple setting, which can help with BYOD issues. Different network functions can efficiently share the same processing resources (processors, networks, and storage) by employing NFV. NFV also improves network service provisioning agility by allowing network functions to be instantiated on demand. Some of MDM, MAM, and MCM's flaws include their inability to manage network functions such as Network Access Control (NAC). They also lack the ability to enforce network security policies, which is critical to the business. [6]

The paper offered by Bashayer Alotaibi and Haya Almagwashi is a literature review that illustrates contemporary BYOD security concerns and issues, security solutions, and policy best practises from an organisational stance. A complete security policy model is also given and discussed. In a case study that looked into security and privacy difficulties in BYOD contexts, technical dangers, the absence of policies, the lack of security controls, the lack of security awareness, and the loss of privacy were all factors. BYOD regulations, security mechanisms, and device monitoring systems were all found to be insufficient in the study. The need for BYOD connectivity to supervise numerous handsets various application software is discussed in this report. Certain free public cloud may use information for personal gain that might be used by external parties for device backups, posing protection and legal concerns. Employee devices that were already lost or stolen constitute a serious security concern since critical corporate data can be accessed and disclosed immediately. It can be tough to put together a crisis management plan following a data breach. Network approach, enterprise mobility technique (MDM), mobile application organisational strategy (MAM), digital information systematic approach (MIM), and integrated mobility management strategy are some management options to consider (EMM). [7]

The following paper proposed through Poorva Tiwari, C S Skanda, U Sanjana, S Aruna, Prasad Honnavalli rates approximately one of the number one demanding situations in BYOD, that's securely deleting agency records whilst an worker leaves an organization. In addition to this, present paintings associated with steady deletion, and steady and selective deletion strategies that delete best the specified documents or directories with out tampering with non-public records also are discussed. Two per-record deletion strategies also are presented, specifically Overwriting records and Encryption primarily based totally deletion which erases precise documents securely. Erasure of records in maximum record structures in recent times effects in unlinking the record region and staining records blocks as unused because of overall performance and deletion latency. The per-record deletion strategies proposed on this paper lessen latency and overall performance overheads caused through overwriting a whole disk. Per-record deletion answer in a BYOD surroundings can assist securely delete best the focused documents. The set of rules exact for per-record deletion is used for overwriting a unmarried record. On the opposite hand, in encryption-primarily based totally deletion, the records in a record is encrypted earlier than deletion to make sure that deleted records upon healing isn't readable. AES encryption set of rules with a 128-bit key became used to encrypt the record earlier than deletion. The desire of set of rules is primarily based totally on ultimate protection and overall performance. A unmarried overwrite is all this is required to safely smash the record, making sure that no significant records is retrieved. In a BYOD context, selective documents may be thoroughly deleted the use of per-record deletion on a record-through-record basis. When in comparison to absolutely erasing a disc, this approach is faster. The AES encryption approach is used for encryption-primarily based totally deletion, which affords the satisfactory protection and overall performance. After overwriting a layout record which include a PDF, it became now no longer readable through pdf visitors which include Preview on macOS and became now no longer recoverable in each record structures. The destroyed pdf documents that had been recovered the use of Stellar Data Recovery Tool had been unreadable through any pdf viewer for the reason that formatted content material apart from the flat textual content have been overwritten. Handling the keys is one of the risks of encryption-primarily based totally deletion because of its

inconvenient nature. Future paintings will cognizance on growing a manner to tune documents as a way to be securely wiped from the time they may be created, in addition to figuring out record-machine sports like updating and deletion.[8]

MD Iman Ali and DR. Sukhkirandeep Kaur provide a novel approach for comment of unauthorized harmful activity in the BYOD setting, as well as a consequent defense algorithm to build a secure BYOD environment, in this research work. Finally, the findings of the study led to the development of a cyber-defense BYOD setting and a computer crimes BYOD ecosystem to protect the key infrastructure of businesses that use BYOD services. A two-phase technique is used in the newly designed model. The first phase is to assess and identify fraudulent BYOD transmission, while the next safeguards the vital infrastructure that helped to establish the BYOD computer forensic system. A concentrated investigation was done to find a flaw in a secure certificate-based authentication process, which led to the invention of the innovative Protection approach. This strategy can be implemented by any firm to secure infrastructure, resulting in a security control cyber forensic environment. When adopting BYOD infrastructure, the "Protect" protocol is recommended. The method for detecting malicious BYOD traffic is useful in preventing an ex-employee from gaining illegal access to an organization's network. The "PROTECT" module in this algorithm safeguards the infrastructure against unauthorized users. In addition, activity logs are recorded so that forensic analysis can be performed. The "PROTECT" algorithm for dropping traffic includes a mechanism that removes traffic while also capturing all logs for forensic inquiry.The algorithm used to detect harmful BYOD traffic has a flaw that allows a threat path to be opened. In the second example of the algorithm, illegal access occurs when the date on which the granted certificate expires is later than the date of disband. This is a situation in which a BYOD user is no longer a genuine legalized user yet can still access essential infrastructure. Future studies in this area will focus on cloud traffic analysis in conjunction with BYOD infrastructure. [9]

The following paper that was proposed by Khoula Al Harthy, Nazaraf Shah, Dr. Arun N.S. Shankarappa stated that To effectively deal with privacy contravention, loss of corporate data, and data leakage in the BOYD environment, an appropriate risk management system is required. Using the MDM log file, this article presents a new approach for proactively identifying potential vulnerabilities in the BYOD context and commitment and mitigation measures in actual environments. Security auditing, security compliance, and policy compliance are all made possible by log file analysis, which also aids in determining user activity. It also aids in the detection of vulnerabilities by tracking changes in rules or traffic load. The goal of the study was to classify log records into two categories: normal and malevolent behavior. To detect the two types of events, a support vector machine was chosen. This approach can be used to classify a dataset with 100 features. It also has a high rate of accuracy in both short and lengthy training times. In terms of accuracy, the SVM algorithm was compared to other algorithms such as Naves Bayes and the random forest algorithm. The experiment's findings revealed that classifications with higher percentages of true positive and false negative had fewer errors. However, because the number of false positives and true negatives was lower, there was an encouraging sign of fewer errors. When compared to the other three algorithms, SVM has the best accuracy percentage. As a result, SVM can be used to predict irrational behaviour. As a result, in the BYOD scenario, the proposed intelligent risk management performs better overall. The ability of the proposed system to make precise and timely assessments for optimal response based on two inputs is its distinguishing feature. The MDM server logs are the first input, and the present risk management system is the second. Due to a higher false-positive rate, the MLP and BN have a high error rate. This report is the second stage of a two-stage research. As a result, the first level, evaluation and analysis, is represented by this paper. In a future article, the implementation stage will be discussed. [10]

The paper proposed by Melva Ratchford, Omar El-Gayar, Cherie Noteboom, and Yong Wang describes the purpose of the study which was to conduct a comprehensive evaluation of the literature on security issues and considerations linked to the BYOD phenomenon in organisations. We presented a classification approach based on existing research to achieve this goal. Management, IT, User, and Mobile Device are the four organisational domains that make up the scheme. The classification scheme's goal is to create a foundation for recognising and discussing the security risks and obligations connected with each domain when it comes to securing BYOD situations. It also gives you a better grasp of the BYOD issue, which is gaining traction as businesses try to protect their corporate data. [11]

The paper proposed by Jiunn-Woei Lian Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah depicts that, when discussing information security management, they emphasised the importance of the human element. The research mentioned above, on the other hand, do not provide empirical results. As a result, an empirical study on the protection of BYOD information security is required. In this study, the statistical findings are used to verify the integrative framework. The factors impacting how valuable BYOD network security protection is viewed have been found. We also demonstrated how varied knowledge and awareness and self-efficacy influence a person's protective behaviour. The information also shows how past investigations are similar and different. These findings can be used as guidelines in scientific education and long-term implementation. [12]

The work proposed by Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah investigates an issue that has received little attention: the behavioural study in a BYOD context. Recognizing that there are risks associated with the BYOD practise, the findings of this study are both essential and pertinent. Second, security is examined from a management standpoint, as opposed to prior BYOD study, which was conducted from a technological standpoint. This research will create a theoretical model to discover characteristics that influence employee compliance with BYOD security standards, which is still a rare occurrence. It applies the SCT and OCT to new situations of BYOD security policy compliance, as well as providing a new perspective on

a distinct security culture. It goes beyond the typical PMT to investigate compliance behaviour in a BYOD environment.[13]

This study included work on scoring systems proposed by Priscilla M Boadi, Dr Shikun Zhou, and Dr Ioannis K. Dynamic soundness threats are data collected particularly on BYOD security risks, whilst Static security threats are data collected on all mobile security threats. On the other hand, gathering enough and pertinent data to coerce informed decisions about BYOD infirmity rating is a striking challenge. The approaches for grading vulnerabilities include CVSS, CWE, and CWSS; however, while CVSS is the most extensively utilised of the three, it lacks real-time vulnerability scoring for BYOD systems.[14]

The paper proposed via way of means of Fara Jamal, Mohd. Taufik Abdullah, Azizol Abdullah, Zurina Mohd. Hanap states that the use of blockchain with extra protection functions will assist to stumble on facts leakage cases. The use of consumer authentication combining with tool believe version will assist to resolve facts leakage due to loss or stolen tool, malware and save you unauthorized man or woman to get entry to the information. Record preserving will assist corporation to stable their touchy facts and save you legal consumer to leak the facts. Digital ledger in blockchain will offer proof of each consumer transaction that may be used as proof whilst facts leakage occurs. It's additionally may be utilized by virtual forensic group to locate proof of protection attack. The blockchain generation that incorporates cryptography will permit the corporation to shield their touchy facts and save you from leaking even if an worker brings his or her personal tool to the corporation.[15]

IV. Comprehensive Analysis

Work Conducted by	Work Proposed on	Advantages	Disadvantages
Felix.C. Aguboshim and Joy. I . Udobi	Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD)	MET employs BYOD policy effectively, that encourages job satisfaction among employees, cause better job efficiency indexability.	Maintaining confidentiality, integrity, and availability are quite complex.
MD Iman Ali, Sukhkirandeep Kaur, Aditya Khamparia, Deepak Gupta, Sachin Kumar, Ashish Khanna and Fadi Al-Turjman	Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment	Perception of cyberattack in BYOD environment was detected using checkpoint technology.	Cyber-attacks were rated as a global peril, and the situation was vulnerable owing to the COVID-19 pandemic, with attackers earmarking enterprises due to forewarn traffic motif during WFH.
Akeju O, Butakov S and Aghili S	Main factors and good practices for managing BYOD and IoT risks in a K-12 environment	The NIST Privacy Framework includes a set of rules that can assist a company in identifying privacy issues in its processing environment.	Implementing K-12 in schools and colleges will be difficult as many students won't be able to use their own devices.
Hai Vu Nguyen	Cybersecurity Strategies for Universities With Bring Your Own Device Programs	By cyber security, it enhances student credentials with appropriate security controls available. Protects network and data from unauthorized access.	There is no network address translation (NAT). Security regulations, training requirements, and access control mechanisms are all unfamiliar to the participants.
Fara Jamal, Mohd. Taufik abdullah, Azizol Abdullah and Zurina Mohd. Hanapi	A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique	Corporations can garner their networks safe by blocking access to their protected resources to just certified users or processes.	Focused on user authentication only. Once the user has already verified authentication, no further control is performed.
Mohammed Ketel	Enhancing BYOD security through SDN	The SDN approach offers a straightforward, flexible network model and a convenient environment, which can aid in overcoming BYOD issues.	Reconfiguring an SDN network is not a simple task since it involves a lot of expenses
Bashayer Alotaibi, Haya Almagwashi	A Review of BYOD security challenges, solutions and policy best practices	Virtual LANs are used to decrease network traffic and categorise users according to access control policies and functions.	Using data separation methods exposes firm data to security threats.
Poorva Tiwari, C S Skanda, U Sanjana, S Aruna, Prasad Honnavalli	Secure wipe out in BYOD environment	The AES encryption method is used for encryption-based deletion, which provides the best security and performance.	Because of its inconvenient nature, handling the keys is one of the downsides of encryption-based deletion.
MD Iman Ali, DR.Sukhkirandeep Kaur	BYOD cyber threat detection and protection model	The "PROTECT" module in the algorithm proposed, safeguards the infrastructure against unauthorized users	The algorithm used to detect harmful BYOD traffic has a flaw that allows a threat path to be opened.
Khoula Al Harthy, Nazaraf Shah, Dr. Arun N.S. Shankarappa	Intelligent risk management framework for BYOD	In terms of accuracy, SVM trumps the other methods. The suggested system's differentiating characteristic is its capacity to combine effective and accurate appraisals for effective response basis of two inputs.	Owing to a tremendous false-positive percentage, MLP and BN have a huge aberration.

Melva Ratchford, Omar El-Gayar, Cherie Noteboom, and Yong Wang	BYOD security issues: a systematic literature review	Provides a deeper understanding of the BYOD phenomenon as organizations aim to protect their corporate information.	There are too many risks when a corporation implements BYOD. Even after having a strong technical security there might any mistake in the management end.
Jiunn-Woei Lian	Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value	Provides a deeper understanding of the BYOD phenomenon as organizations aim to protect their corporate information.	There are too many risks when a corporation implements BYOD. Even after having a strong technical security there might any mistake in the management end.
Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah	BYOD Security Policy Compliance Framework	The study investigates an area that has received little attention that is the behavioural study in a BYOD setting.	New issues arise as a result of education and practice. The distinction between conventional IT leading acquisition and BYOD underside inverted adoption was brought up.
Priscilla M Boadi*, Dr Shikun Zhou and Dr Ioannis K	Current BYOD Security Evaluation System: Future Direction	The score system has been established in this evaluation to measure the threat level in BYOD.	Acquiring pertinent data to make informed BYOD susceptibility assessment judgements is a huge challenge.
Fara Jamal, Mohd. Taufik Abdullah, Azizol Abdullah, Zurina Mohd. Hanap	Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology.	The use of blockchain in conjunction with extra security features will aid in the detection of data leakage incidents.	Developing distributed ledgers to function in a highly distributed, heterogeneous network would require considerable effort.

V. Conclusion

By perusing through these research papers, we understand that BYOD is a method that allows employees to access protected business data from anywhere using their mobile devices. Securing BYOD is a critical aspect in avoiding the security risks and data leakages associated with MET. Based on the (NIST-8062) model, the risk of BYOD and IoT was identified, as well as privacy concerns in the K-12 ecosystem. The PMT was utilized to gain access to IT professionals' ethical framework as well as supplementary information on conflicting viewpoints. They discovered 25 verification strategies across industries and educational institutions that might be used by BYOD to improve security by avoiding and detecting data leaks. The various research papers provide information on the different security threats faced in a BYOD environment. Potential mechanisms to prevent attacks were also discussed. These papers make us aware of what an organization must take into account while the study's main goal is to teach IT and security professionals how to deal with the most quotidian security threats, vulnerabilities, and risks connected with BYOD systems. To complete the forensic investigation process, a full end-to-end eco-system must be built. The cyberattack was classified as a global threat, and attackers were targeting organisations because of the COVID-19 pandemic situation. BYOD users were maintained at a distance over the internet in order to access to the corporate network without using a VPN or cloud services, where malicious activity was discovered using on-premise 3-layer security.

References

[1] Felix. C. Aguboshim and Joy. I. Udobi, “Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD)”,10th October 2019 in Journal of Information Engineering and Applications.

[2] MD Iman Ali, Sukhkirandeep Kaur, Aditya Khamparia, “Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment”,18th September 2020, Digital Object Identifier 10.1109/ACCESS.2020.3024784 by IEEE.

[3] Oluwaseun Akeju*, Sergey Butakov and Shaun Aghili “Main factors and good practices for managing BYOD and IoT risks in a K-12 environment” 1st January 2018 by Concordia University of Edmonton, 7128 Ada Boulevard, Edmonton AB, Canada.

[4] Hai Vu Nguyn “Cybersecurity Strategies for Universities With Bring Your Own Device Programs”, 10th December 2019 by Walden University,Minneapolis, Minnesota.

[5] Fara Jamal , Mohd. Taufik Abdullah,Azizol Abdullah and Zurina Mohd. Hanapi “A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique”, 1st April 2020 by Journal of Physics: Conference Series.

[6] Mohammed Ketel “Enhancing BYOD security through SDN”, 19th April 2018 at the Southeast Conference in St. Petersburg, Florida, USA

[7] Bashayer Alotaibi, Haya Almagwashi “A Review of BYOD security challenges, solutions and policy best practices”, 4th April 2018 at the 1st International Conference on Computer Applications and Information security (ICCAIS) held in Riyadh, Saudi Arabia.

[8] Poorva Tiwari, C S Skanda, U Sanjana, S Aruna, Prasad Honnavalli "Secure wipe out in BYOD environment", 17th October 2020 at the International Workshop on Big Data and Information in Depok, Indonesia.

[9] MD Iman Ali, DR.Sukhkirandeep Kaur "BYOD cyber threat detection and protection model", 19th February 2021 at the International Conference On Computing, communication and intelligent systems.

[10] Khoula Al Harthy, Nazaraf Shah, Dr. Arun N.S. Shankarappa "Intelligent risk management framework for BYOD", 12th October 2018 at the IEEE 15th International Conference on e-Business Engineering (ICEBE).

[11] Melva Ratchford, Omar El-Gayar, Cherie Noteboom, and Yong Wang "BYOD security issues: a systematic literature review", 22nd July 2021 by the Dakota State University, Madison, United States

[12] Jiunn-Woei Lian "Understanding cloud-based BYOD information security", 14th July 2020 by the Department of Information Management, National Taichung,University of Science and Technology, Taichung, Taiwan

[13] Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah "BYOD Security Policy Compliance Framework", 8th July 2019 at the Pacific Asia Conference on Information Systems in China.

[14] Priscilla M Boadi*, Dr Shikun Zhou and Dr Ioannis K "Current BYOD Security Evaluation System: Future Direction", 1st January 2018 in the Journal of Information Technology and software engineering.

[15] Fara Jamal, Mohd. Taufik Abdullah, Azizol Abdullah, Zurina Mohd. Hanap "Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology", 1st November 2018 in the Journal of Information Technology and software engineering.