International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

IAM FOR BRING YOUR OWN DEVICE (BYOD) ENVIRONMENTS: ANALYZING IAM CHALLENGES AND STRATEGIES FOR SECURELY MANAGING USER IDENTITIES AND DEVICES IN BYOD ENVIRONMENTS, INCLUDING CONTAINERIZATION AND MOBILE DEVICE MANAGEMENT (MDM)

Sri Kanth Mandru
Mandrusrikanth9@gmail.com

Abstract

This paper outlines IAM specifically about BYOD protocols. These elements include many devices, probable security threats from unknown devices, and concerns about adherence to regulations. Role-based access control, multi-factor authentication, and integration with mobile device management solutions have been proven viable. Finally, it is stated that under such tangled BYOD policies, the IAM plays an essential role in establishing a safe shield of business information and compliance with the current IT standards and regulations.

Keywords: Authentication, Identity Management, Access Control, Containerization, Mobile Device Management (MDM), Security.

I. INTRODUCTION

Many of today's organizations already have BYOD (Bring Your Own practices), which allow employees to use their company-provided electronic devices at work to accomplish tasks. Although having facility and flexibility is advantageous, it is a significant problem that should not be taken lightly regarding security.

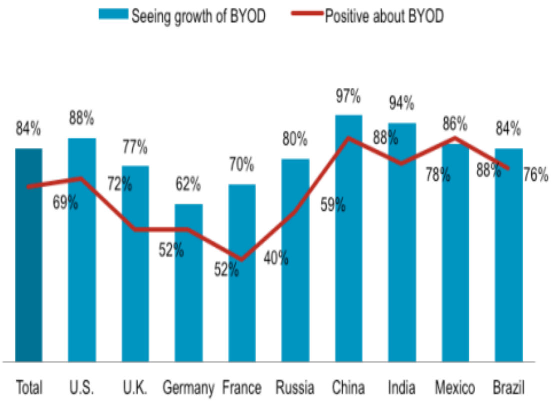

Figure 1: Global perspective on BYOD [1]

Policies defined for using personal devices are usually more or less stringent. Hence, there is a high chance that vital information belonging to the company will leak if individuals have access to such information. The only approach or solution that helps avoid or at least control such risks is

Identity and Access Management, IAM, which deals with access to company resources and some rules or laws to be followed apart from having I&A [1]. IAM frameworks also reduce instances where sensitive information is exposed since the management can dictate what kinds of information should not be accessed by specific tasks, devices, or personnel.

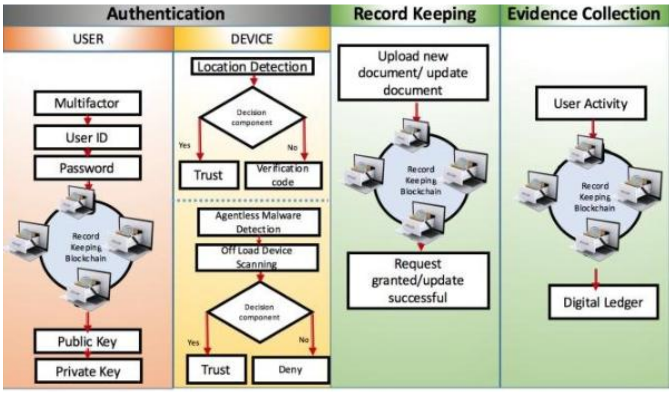

Figure 2: Basic BYOD Architecture [2]

The ever-growing use of BYOD environments, particularly for IAM solutions, forms the core of this research, which focuses on the opportunity of adopting BYOD but with several hurdles, including multiple devices, security, and compliance. This paper aims to help businesses improve security and drive value from BYOD frameworks by analyzing extant approaches to IAM and proposing innovative technologies such as cloud IAM, AI, and advanced access control [2]. Lastly, it will provide specific guidelines for implementing stable and efficient identity and access management systems to capture the characteristics of the contemporary work environments discussed in the paper.

II. PROBLEM STATEMENT

Managing policy with IAM is particularly difficult in the BYOD context, as devices might be of different types. Users take their devices to the workplace, including computing devices, personal computers, tablets, and phones for calls and other messages, and others that use various platforms. On the one hand, heterogeneity is problematic for IAM because it is relatively impracticable to implement and ensure compliance with multiple security regimes across this diverse set of devices [3]. Currently, there is no corporate supervision, and while some of the unmanaged devices may have a hard-coded security mechanism, the rest are a significant security concern. These devices are vulnerable to getting infected with malware. They can be attacked frequently as it might take some time before the antivirus program or the security patches of the device can be updated. This worsens compliance issues and data breaches because it affects crucial corporate data that is searchable and saved on those widgets.

As for compliance and data protection, BYOD policies are becoming a headache for data protection laws like the GDPR or CCPA or industry standards such as the Health Insurance Portability and Accountability Act (HIPAA) for medical businesses. Maintaining the company and personal data confidentiality, information security, proper access control, and high levels of authorization policies and standards becomes a necessity but a challenging task if not for the Identity and Access Management solutions. Two risks are possible regarding IDGCO, which could arise due to inadequate IAM concerning BYOD. Due to security incidents and system unavailability, block and control, and other affairs related to the integrity of information, penalties given by regulations and authorities and productivity loss might occur [4]. Second, the other problem could be more general and be related to the proper handling of the identity of the user and their rights across the diverse devices and applications, which may also be another issue that may emerge in this case due to the absence of a unified approach to access control. However, there is a need to develop an IAM strategy that MUST include multi-factor authentication, how the devices can be managed, and the policies that MUST be enforced, especially in BYOD scenarios.

III. SOLUTION

Several strategic approaches may improve the IAM to make it safe and functionally effective on the issues presented by the BYOD situations. Another model for managing permission that corresponds to users and their responsibilities is the RBAC model, which stands for role-based access control model. While it still allows some degree of freedom concerning the use of the workers' owned devices, the RBAC model is helpful in various BYOD cases.

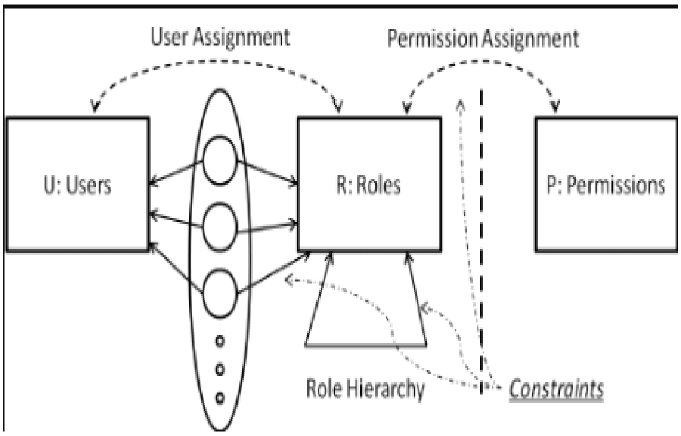

Figure 3: Role-Based Access Control (RBAC) Framework [5]

The RBAC model facilitates the application of strict access restrictions; such restrictions imply that the user has the barest right of access to the resource [5]. Two elements in the authentication of BYOD policies are distinguished: Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

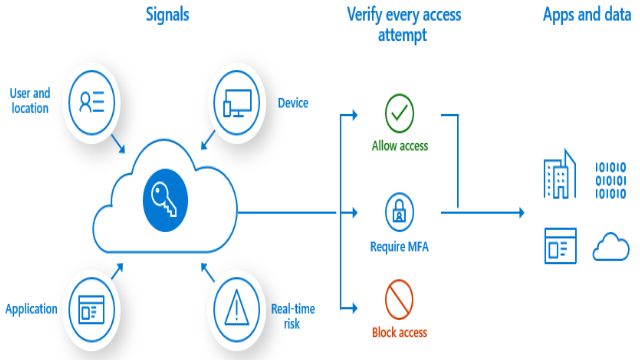

Figure 4: Multi-Factor Authentication (MFA) Process [6]

MFA reduces the likelihood of attackers gaining access because one has to provide at least two identification factors, such as passwords, fingerprints, or OTPs. Single sign-on (SSO) increases security, but it does not necessarily imply that usability is interfered with since users can access several applications using a single identity [6].

Docker and Kubernetes are containerization technologies that provide a safe environment for employees to deploy applications when they bring their devices to the workplace. It makes the management and updates of the app and its dependencies easier since interfering with other apps is minimized since it has been put in a container, limiting its interaction with private data and with company data [7].

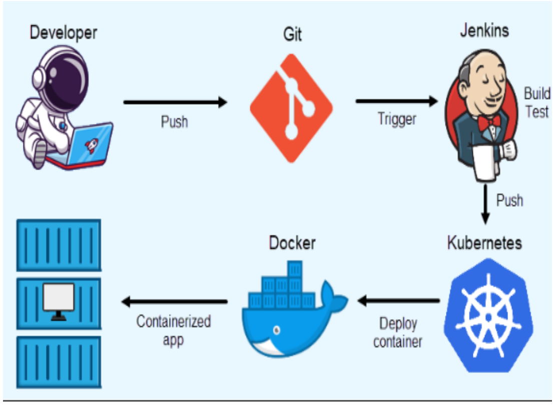

Figure 5: Containerization Technology: Docker, Kubernetes [7]

Due to this, mobile device management (MDM) solutions are crucial for any industry to enforce safe Bring Your Device (BYOD) policies. The benefits mentioned are better device security and additional data protection.

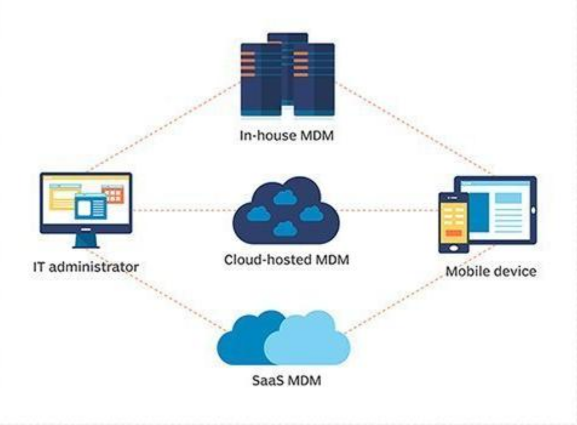

Figure 6: Mobile Device Management (MDM) Solutions [7]

As such, MDM systems enable the management and monitoring of enterprise devices remotely and enforce security configuration and business policies.

Other preventive techniques that can be implemented to enhance the security of BYOD security data are the isolation of the network and the use of encryption protocols. Segmentation, where a network is divided into smaller parts that are more accessible to process, assists in handling potential risks, especially in a breach. To give access only to the intended people, there are secure channels like a virtual private network (VPN) where the information is encrypted from the user's device to the business network [7]. Such tactics may be developed alongside one another to construct an enveloping IAM architecture in organizations within the context of BYOD. It also increases a system's protection and assists business enterprises in staying compliant with the law, improving workflows, and giving users greater control of their devices at work.

These assumptions, in fact, embrace future development of IAM for BYOD scenarios addressing such issues as RBAC, MFA, SSO, containerization, MDM, and network segregation and, by implication, the roll-out of cognitive computing enhanced by machine learning across every level of IAM. These will contribute further improvements to the security and the application of the IAM systems to toggle their access policies in accordance with the context and actions of the user. This can then be measured statistically by the artificial intelligence models. If the statistics seem to indicate that there might very well be something dangerous, then that is how it will perceive it. This may cause preventive measures such as better means of authentication or restrictions on privileges for access to some sections. As such, the proactivity leads to creating barriers to sophisticated cyber schemes, holding targets on the systems of BYOD in a more effective way [7]. However, there are newer and clearly simpler protocols and standards, such as OpenID Connect and OAuth, which are relatively recent crises that have clearly defined structures for authorizing applications and authenticating users on different devices and systems. These standards offer fixed security states and strict user access patterns incorporated within IAM configurations, further enabling integration and hastening the IAM releases within BYOD settings.

Moreover, there are new trends that are moving IAM systems to the cloud, which changes organizations' identities in the context of BYOD. Some of the benefits of cloud IAM solutions include flexibility, which enables them to be easily enlarged or adapted to the growing needs originating from modern business environments and newly introduced technologies. It minimizes document activities and routine use since IAM functions can be configured and maintained geographically in various regions of the enterprise [8]. It is noteworthy that through the use and integration of these innovations in IAM strategy, there could be a possibility of having a positive impact on the new rising challenges such as managing BYOD propagated risk in organizations, protection of networks and systems from cyber threats, the compliance of the current policies, standards, and regulations as well as enhancing and developing a sustainable and adaptable force that is ready to counter future and unknown complexity in technology requirements and needs.

IV. USES

The effect of sector-specific techniques can be witnessed with examples of Identity and Access Management (IAM) integrations in 'bring your device' (BYOD) scenarios in different industries. Regulation requirements and the security of patients' records are demanding in healthcare, so IAM solutions are crucial. For instance, to ensure that only authorized employees can access information regarding patients, RBAC frameworks have been adopted by healthcare companies to keep such information away from the employees' handheld devices [8]. EHR has also made record access easy while retaining a strict security measure, primarily through implementing MFA and SSO.

IAM in banking is rated a high priority when working with financial data and keeping an eye on security standards such as PCI-DSS or GDPR. For example, examples demonstrate how MDM solutions could integrate with IAM systems to mitigate unauthorized publication or disappearance of case information [9]. This assists the users in obtaining permission to use mobile applications in business.

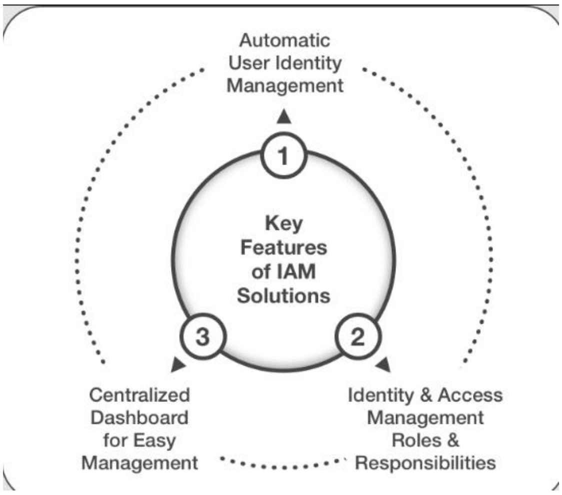

Figure 7: Key Features of IAM [9]

IAM solutions currently widespread in the IT services sector involve using secure tunnels and network separation to protect client information as employees in this industry directly or indirectly log into different client networks and data [10]. This is made possible by implementing the contained technology that ensures security while deploying and running the programs for data integrity as they are laid down.

To be sure, RBAC, MFA, and SSO form the basis of IAM. Yet the fine print of implementing these principles is vastly different in the various industries due to differences in data sensitivity, legal requirements, and business environments [11]. Examples of successful IAM implementations in several areas are worth noting to illustrate how IAM can be applied to solve multiple problems in the field and enhance security, performance, and adherence to regulatory standards in environments where BYOD technologies are used.

However, it is also evident that there is progress in IAM for BYOD environments across fields that are not IT services, healthcare, and, to some degree, the financial domain, such as education and retail. For example, regulating access rights to the limited information regarding the students as well as the various course materials that are available or should be made available to the diverse personal gadgets the faculty along with the students utilizes is a menace to academic institutions. Other features such as biometric authentication and access control policies are often incorporated in IAM systems to harness safe access to the databases charged with research and educational information as well as to avoid compromising the students' data and piracy of the content. Likewise, retail businesses depend only on IAM to secure customer details collected from multiple interfaces such as web and mobile applications [11]. Here, IAM frameworks facilitate the defense of the transactional data and comply with the PCI-DSS and CCPA regulatory bodies, as well as guarantee operational efficiency and SSO features. The following discusses how IAM makes it possible to prevent the occurrence of data breaches and unauthorized access to customers' private data while at the same time permitting convenience. This will help boost customer confidence and security, which are vital for the success of any business.

V. IMPACT

These systems improve numerous factors that accompany the usage of 'mobile' in business, including security, user interface, and regulatory aspects. Consequently, BYOD is likely to improve the level of protection of organizations that implement BYOD through the effective adoption of a good IAM architecture [12]. This implies that practices such as RBAC and MFA help reduce the levels of unauthorized access and data breach incidents. Consequently, by applying technical options such as the remote management features of an MDM system, the corporation can manage and secure the personal device when it is integrated into the organization's network by the administration of the individual device.

IAM is relevant in that aspect because it contributes to improving the usability of systems because of the roles they play in the negligence of SSO access to many resources and applications. This is especially so if a person is in a situation where he has to log in repeatedly to gain access to resources and materials, which is evidence of improved productivity and user satisfaction [12]. The company can address the requirements of legal norms, which are essential to the application's functionality, including GDPR or HIPAA, with a robust IAM solution. The two main objectives of IAM are accessing and securing client/employee data and avoiding high-risk fines [13]. The last two advantages are more related to sustaining constant expectations for further optimization of costs and enhancement of productivity in IAM processes. Other benefits of numerous and simplified audits, generated reports, and advantages of centralized IAM systems include better IT control and a short time to contain a security breach.

Besides, IAM solutions for enterprises that implement BYOD also provide the techniques to manage the identified threats and adapt to new threats and technologies. Real-time and large data may be analyzed by IAM frameworks involving AI and machine learning that help to look for the anomaly and probable security hazards [15]. By itself, this feature helps guard the organization against intricate attacks on a BYOD structure by admitting automatic responses like adaptive access control or real-time threat termination. However, there are a few parameters, such as scalability and flexibility that are indispensable to the implementation of the BYOD that are supported by the cloud-based IAM solutions. They can also expand and develop their identity management solutions and satisfy business requirements by expanding into other geographic regions and leveraging cloud IAM services that already don’t possess security issues. Firms with multiple workforce demographics and varying legal requirements in various areas of the globe will benefit from it more than others, for instance.

Furthermore, when integrating IAM into BYOD arrangements, the application of sophisticated technologies like blockchain could improve the security and credibility of verification processes. Since the ledger is dispersed in the blockchain, the risk of identity theft is relatively low, and everyone can be confident that they are interacting with real and verified users through records of identification transactions in the system. The organizations may attempt to build forward IAM strategies that include fast and creative solutions that assist them in mitigating the emergent threats and, at the same time, implementing compliance with the new regulative rules and requirements while bearing in mind the BYOD policy in the workplace.

VI. SCOPE

- The new developments in IAM concerning BYOD include the augmentations that utilize current innovative technology to include innovative technology to integrate modern threats.
- Another factor that cannot be missed is the extent and nature of how both ML and AI are incorporated into the IAM systems.

- It is possible to suppose to some extent that in the case of real-time risk assessment of AI, the parameters of limitation of access can be altered with regards to the patterns of user participation and other related information patterns [16].
- Thus, the IAM controlled by artificial intelligence can identify such pre-odd behavioral patterns that suggest possible threats and contribute toward minimizing these threats; in that case, the changes in access control can be made less stringent to address the challenges associated with the BYOD model effectively.
- Besides this, some emerging protocols and standards on the IAM path, like OpenID Connect and OAuth, are also present. Adopting such standards improves user and application experience in the BYOD setting due to secure authentication/authorization between the service and the app and enhanced integration [17].
- The standard authentication approach is helpful in the sense that it allows organizations to have reasonable efficiency in security while, on the other hand, adding third-party apps without much strain.
- The reliability of identity and access management systems resident in the cloud heavily depends on BYOD's security policy.
- The cloud IAM solution is ideal in the BYOD situation, which necessitates central identity and access management across different geographical locations, as it offers scalability and flexibility with the required features.
- A lot of precautions have to be taken while selecting a cloud IAM solution to ensure that the company's information is not compromised and that the solution deployed by the firm does not lead to a violation of the law.
- According to the evaluation of the discussed evolutionary and revolutionary trends, some observations can be made on how further IAM development for BYOD implementation would affect security, work efficiency, and adaptability of the digital work environment in the following ways [18].
- Machine-learned adaptive access controls are more advanced and can be viewed as an evolution of identity and access management.
- Regarding correlated risk estimates, real-time user data in context and behavioral patterns might be leveraged through machine learning techniques to modulate IAM system access.
- This is a precautionary measure that assists in avoiding situations where threats that might be out there get worse, hence making security stronger by the time the possible risks have been recognized.
- In the BYOD arrangements, standard IAM protocols such as OpenID Connect and OAuth start to emerge where necessary.
- The Modern Bring Your Device settings can also have to be both flexible and growing and cloud-based Identity and Access
- Management Solutions will continue to be needed to respond to these [16].
- The cloud IAM solutions can be implemented in a very short time, and they can also be expanded for the expansion of the scale of users as well as the regional scale expansion with a feature of centralized management.
- This is helpful for organizations with many employees because it means that identity can be managed centrally and change can happen quickly in a timely manner to accommodate for innovation and global compliance [19].
- To address these changes, organizations are required to invest a large sum in cloud-based solutions, standard IAM processes, and artificial intelligence savvy.

VII. CONCLUSION

- Identity and access management (IAM) is the subject of this research because it is essential to define the perimeters of BYOD.
- One of the most relevant findings is identity and access management, which should be addressed by various tools and solutions, mobile device management, multi-factor authentication, and access based on roles.
- Sound IAM practices enhance user productivity as well as adherence to some laws and acts.
- Organizations must introduce a powerful but efficient IAM to offset BYOD to the extent that the guidelines or rules of the organization allow its employees.
- These solutions should utilize cloud computing technology and have flexible, AI-enabled controls.

REFERENCES

1. R. O. Ouko, "Identity management and user authentication approach for the implementation of bring your device in organizations," 2017. Available: http://hdl.handle.net/11071/5678
2. D. Kyriazis, “BYOS: Bring Your Own Security in Clouds and Service Oriented Infrastructures,” May 2018, doi: 10.1109/waina.2018.00114. Available: https://doi.org/10.1109/waina.2018.00114
3. R. O. Ouko, “Identity management and user authentication approach for the implementation of bring your own device in organizations,” Jun. 2017. Available: https://core.ac.uk/download/pdf/132627775.pdf
4. P. Saa, O. Moscoso-Zea, and S. Lujan-Mora, “Bring your own device (BYOD): Students perception — Privacy issues: A new trend in education?,” Jul. 2017, doi: 10.1109/ithet.2017.8067824. Available: https://doi.org/10.1109/ithet.2017.8067824
5. N. Vithanwattana, G. Mapp, and C. George, “Developing a comprehensive information security framework for mHealth: a detailed analysis,” Journal of Reliable Intelligent Environments, vol. 3, no. 1, pp. 21–39, Apr. 2017, doi: 10.1007/s40860-017-0038-x. Available: https://doi.org/10.1007/s40860-017-0038-x
6. D. Peraković, S. Husnjak, and I. Cvitić, “Comparative analysis of enterprise mobility management systems in BYOD environment,” 2014. Available: https://www.fpz.unizg.hr/ikp/upload/perakovic_husnjak_cvitic.pdf
7. T. Oktavia, N. Yanti, H. Prabowo, and N. Meyliana, “Security and privacy challenge in Bring Your Own Device environment: A Systematic Literature Review,” Nov. 2016, doi: 10.1109/icimtech.2016.7930328. Available: https://doi.org/10.1109/icimtech.2016.7930328
8. S. T. Ng, F. J. Xu, Y. Yang, and M. Lu, “A Master Data Management Solution to Unlock the Value of Big Infrastructure Data for Smart, Sustainable and Resilient City Planning,” Procedia Engineering, vol. 196, pp. 939–947, Jan. 2017, doi: 10.1016/j.proeng.2017.08.034. Available: https://doi.org/10.1016/j.proeng.2017.08.034
9. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196–248, Jan. 2019, doi: 10.1109/comst.2019.2933899. Available: https://doi.org/10.1109/comst.2019.2933899

10. G. F. Belete et al., “Exploring Low-Carbon Futures: A Web Service Approach to Linking Diverse Climate-Energy-Economy Models,” Energies, vol. 12, no. 15, p. 2880, Jul. 2019, doi: 10.3390/en12152880. Available: https://doi.org/10.3390/en12152880
11. X.-L. Hoang and A. Fay, “A Capability Model for the Adaptation of Manufacturing Systems,” Sep. 2019, doi: 10.1109/etfa.2019.8869142. Available: https://doi.org/10.1109/etfa.2019.8869142
12. O. G. Otti, “Bring Your Own Device (BYOD): Risks to Adopters and Users,” The Repository at St. Cloud State. Available: https://repository.stcloudstate.edu/msia_etds/73/
13. T. Sommestad, H. Karlzén, and J. Hallberg, “The Theory of Planned Behavior and Information Security Policy Compliance,” □the □Journal of Computer Information Systems/□the □Journal of Computer Information Systems, vol. 59, no. 4, pp. 344–353, Sep. 2017, doi: 10.1080/08874417.2017.1368421. Available: https://doi.org/10.1080/08874417.2017.1368421
14. K. Downer and M. Bhattacharya, “BYOD Security: A New Business Challenge,” Dec. 2015, doi: 10.1109/smartcity.2015.221. Available: https://doi.org/10.1109/smartcity.2015.221
15. M. R. Spruit and R. S. Batenburg, “Enterprise Mobile Security: The development of a Mobile Risk Assessment Method (M-RAM),” Oct. 02, 2018. Available: https://studenttheses.uu.nl/handle/20.500.12932/32966
16. F. Osimani, B. Stecanella, G. Capdehourat, L. Etcheverry, and E. Grampín, “Managing Devices of a One-to-One Computing Educational Program Using an IoT Infrastructure,” Sensors, vol. 19, no. 1, p. 70, Dec. 2018, doi: 10.3390/s19010070. Available: https://doi.org/10.3390/s19010070
17. H. Okonofua and S. S. M. Rahman, “Cybersecurity: An Analysis of the Protection Mechanisms in a Cloud-centered Environment,” Aug. 2018, doi: 10.1109/trustcom/bigdatase.2018.00299. Available: https://doi.org/10.1109/trustcom/bigdatase.2018.00299
18. C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, “Recent challenges, trends, and concerns related to IoT security: An evolutionary study,” 2018 20th International Conference on Advanced Communication Technology (ICACT), Feb. 2018, doi: 10.23919/icact.2018.8323774. Available: https://doi.org/10.23919/icact.2018.8323774
19. “BYOD Security: A New Business Challenge,” IEEE Conference Publication | IEEE Xplore, Dec. 01, 2015. Available: https://ieeexplore.ieee.org/abstract/document/7463876/
20. A. S. Omar and O. Basir, “Identity Management in IoT Networks Using Blockchain and Smart Contracts,” Jul. 2018, doi: 10.1109/cybermatics_2018.2018.00187. Available: https://doi.org/10.1109/cybermatics_2018.2018.00187
21. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey," Computer Science Review, vol. 33, pp. 1–48, Aug. 2019, doi 10.1016/j.cosrev.2019.05.002. Available: https://doi.org/10.1016/j.cosrev.2019.05.002
22. A. D. Giwah, “User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory,” Apr. 2018, doi: 10.1109/secon.2018.8479178. Available: https://doi.org/10.1109/secon.2018.8479178