NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 7, ISSUE 3, Mar.-2020

USABILITY AND PRIVACY IN ACADEMIC LIBRARIES: REGAINING A FOOTHOLD THROUGH IDENTITY AND ACCESS MANAGEMENT

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology, Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT
This paper discussed how identity and access management is applied to libraries to improve their usability and protect the privacy of the users. The gains from efforts to simplify the academic experience of the students can be weighed based on the quality of academic materials that they get access to daily [1]. However, there are many data security precautions that institutions must take to safeguard the private information of their users. Using an example of a University Library's involvement in single sign-on initiatives in cooperation with the IT department as well as a third-party software provider, a strategy for academic libraries to more solidly integrate privacy and security in their systems is important. One element of cooperation where the librarian's standard devotion to patron or user privacy may be maintained is identity and access management. The idea that technology is a driver for 'disruptive innovation' in the libraries field has been widely explored in academic and broader print publications [2]. Furthermore, the difficulties and possibilities posed by technical advancements like e-books and cable Internet connectivity in homes, along with the additional constraints imposed by public-sector cutbacks, are well documented. Most of these advancements questioned the significance (or should be) of library collections in the 21st century.

Keywords: University Library, usability, identity management, access management, cybersecurity

INTRODUCTION
In recent years, our social system has been more concerned about the conflicts between internet freedom and security. The debate swings around usability, security, and privacy principles. It is necessary to strike a balance since placing a greater focus on one may result in trade-offs in the other. It is conceivable, and even essential, for an institution or a business to take a stance in this interplay [1]. For instance, Apple and Google appear to bet that e-books users will proceed to quantify the impact of usability of their online services, balance this freedom with the awareness (and perhaps discomfort) that the massive quantity of personal information they choose to provide in exchange for online resources is easy. However, when security matters in involved due to the increase in security breaches, the ebook customers will want assurance of their protection when accessing these services. However, Apple appears to be confident that its customers will continue paying for its services that provide more privacy guarantees, among other advantages [2].
Maintaining a customer's right to privacy has historically been seen as a professional obligation by librarians and information professionals. Nonetheless, in the context of school libraries, the library's responsibility in maintaining collections has largely shifted away from the custodianship of locally available materials and more towards brokering access to subscription content housed elsewhere. Moreover, the access management system – to the extent that it is administered on-site – relies at minimum as much on IT as on library personnel. Additionally, it is reliant on additional access brokers and IT personnel employed by a variety of publishers and data brokers [3]. This activity is essentially consultative and is predicated on the sharing of information about the library, resources stored, the users, and its services. As a result, because a great deal of information regarding library users' behavior is no longer directly within the library's control, the difficulties associated with maintaining the organizational commitment to privacy have shifted dramatically [3,4]. The issue of authentication and authorization is frequently neglected when usability-security conflicts become a business problem for public libraries: controlling the way users connect to the material offered by the library. This paper will therefore explore how identity and access management can change these practices and help libraries to maintain a high standard of professionalism when it comes to the usability and privacy of library resources.

PROBLEM STATEMENT

The main problem that this paper will try to solve is an assessment of how identity and access management works in improving usability and privacy in academic libraries. There is a potential problem when users access library resources. Their details can be accessed by unauthorized people if there are no robust planforms to protect their identities. Identity and access management come in hand with protocols and algorithms which will control who accesses and uses the stored information in a library database. An evaluation of how identity and access management work to improve accessibility and privacy in academic libraries is the principal issue that this paper will attempt to resolve. Identity management (IdM) includes maintenance activities related to electronic identity lifecycles: provisioning, de-provisioning, and intermediate handling of modifications. Moreover, the IdM systems can make individual identities, along with a set of associated characteristics, accessible through published directories, which may be used by adjacent solutions to verify a person's credentials and get associated attributes in return. Access Management is a broad term that refers to the duties involved in granting access to resources once a user's credentials have been verified. The identity management system does not make any judgments regarding access to surrounding apps; it simply verifies the validity of the credentials provided. IAM is mainly concerned with enhancing and simplifying the technology and business procedures that enable authorized people to access the appropriate library services at the appropriate time.

LITERATURE REVIEW

A. The development of the academic library

Academic libraries have an illustrious history and tradition, and they have long played a crucial role in academic studies, teaching, as well as intellectual interaction. University libraries have grown over the years in lockstep with the institutions of higher education to which they belong, and have established a reputation for being robust hubs capable of adapting to changing cultural, social, and technological factors [5]. Several distinct academic library systems have been recently introduced to universities like Yale, Harvard, Cambridge, and other regions with distributed federal campuses, like the University of the West Indies [4,5]. At such a period where many discussions are focusing on physical stocks reduced in library services, it is fascinating to see that the oldest public libraries had no had a vast collection of books and appeared to ask for donations of writings and other manuscripts, like the Bodleian at Oxford University with a core of legacy materials.

During the late nineteenth and early twentieth centuries, academic library resources started growing in size and value, and a sense of competition began to develop between institutions in terms of the size and worth of their holdings. The post-war era saw a dramatic rise in academic production, which, when coupled with the advent of early computer technologies in the 1970s, resulted in the creation of novel methods for storing, classifying, and retrieving knowledge [6]. While these advancements supported public libraries management in developing digital programs and coping with the wealth of information, there have already been worries that online technologies and automation might well result in the collapse of library services and the involvement of librarians becoming obsolete, as well as an acknowledgment that the existence of academic library science needed to be changed. Even by the mid-80s, it was apparent that "the whole research communication company evolved in ways that threatened to de-institutionalize information [6]. Libraries could not and can not be expected to maintain a monopolize the information, as they did in the past. Nonetheless, these views have not always taken sufficient account of the reality that libraries have continuously changed and the function of the librarian has also altered per the change process [6].

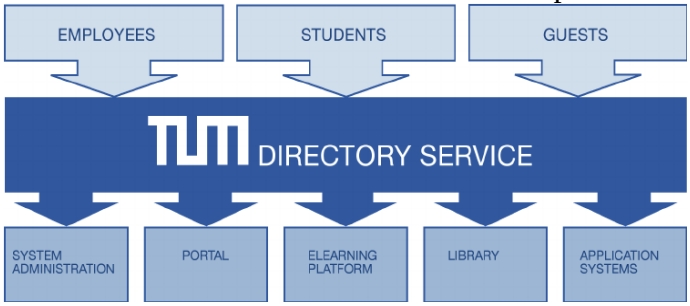

Fig i: Directory service for IAM

B. Identity and access management

Library personnel typically contribute to the field of identity and access management via a variety of means. First and foremost, they will see to it that the conditions of the licenses agreed with publishers of academic material are adhered to in actuality. Secondly, support will be requested if the user gets notice of error or denial of access for a material that has been obtained and connected through the university portal or its library [5]. In a third instance, a librarian may be involved in the library domain when they are involved in the negotiation of agreements with a publisher or aggregator about a user's ethical and legal right to privacy and the university's proper regulatory adherence to information security [6,7]. Beyond legal understanding, the library needs employees who are familiar with their institution's identity provider (IdP) services and understand how it functions as an intermediate between both the university, publishers, and users or readers to have a meaningful voice in this area [8]. An IdP decides what details about a student to disclose to other parties, based on the student's consent [8].

Users' data is compiled into categories called "attributes" in the IdP. These are centralized data structures that can include details such as which educational establishment they belong to, the nature of their association with the institution (for instance, if they're a student, an employee, an associate, or a combination of the above), a unique and personal identifier (normally, an institutional username), among other details [8,9]. If a third-party service or program, such as a publishing platform, requires varying proportions of this data, it will ask the university (IdP) for it. A simple statement that they are from the university that provides for the publisher's services is typically sufficient for access, although more comprehensive or granular (or personal) details may be required.

Considering that striking a balance between accessibility and privacy is a strategic choice that every web-based institution must undertake, it implies that the specific characteristics that a provider requests from an institution may reveal much about its core business practice. For example, SAGE, Wiley-Blackwell, and JSTOR all need a single attribute to show that the client is affiliated with the host university to allow entry to their journal collections [9]. However, to be granted institutional access to LinkedIn a user requires the IdP to start releasing a personal token that will be used to remember the user whenever they visit the website. LinkedIn also requires that the user's institutional e-mail address be automatically released, in addition, to strongly designed to encourage users to align their use of such a learning system with a pre-existing LinkedIn account. Essentially, in exchange for a monthly membership fee, the first three platforms fulfill their agreements with the school by giving students access to a collection of materials that are presented in the same manner by each user from the institution [10. As part of its mission to customize the experience for users and expand the user base of LinkedIn Learning, a data-driven networking site, the management hopes to establish an identity that is entrenched in the user's life beyond the limits of their institutional affiliation. While both need a yearly academic subscription, LinkedIn Learning has the potential to generate extra, if not larger, profits as a result of the institution's desire to "pay" for offerings with the credentials of its users [10,11]. This attribute disclosure may not always be following the principles or long-term preferences of the libraries, the institution, or even the user in question.

C. Change of identity, loss of personalization: single sign-on provider

Many library subscription services need the usage of a personal user token that recalls return visitors as well – in particular reference monitoring systems and e-book resources that depend on the implementation of electronic copyrights [12]. In such instances, the connection to a personal email address on the site is critical to the provision of the services. It allows the user of referencing management software such as EndNote and RefWorks to build customized catalogs of sources for certain coursework and citation styles; in e-book collection, it affirms the publisher's and writer's legal right to determine copyrighted content [12,13]. The design of the data protection access arrangements and the management of them may profit many institutions substantially from a user-centered service, such as the contemporary academic library [13]. An initiative to transition from an on-premises institutional identification supplier to a centralized entity will help a learning institution resulted in expanding and protecting the millions of credentials from its users. The IdP platform had previously been implemented by libraries in streamlining the log-in process in Library databases. In the past, IT operations have progressively started using applications to enable single sign-ups to other programs and services, including the VLE and student/staff intranet [14].

The disparities in professional cultures amongst the organizations engaged were brought to light as a result of this. Example: Information Technology (IT) emphasizes a systematic and rule-based solution to technological problems following its mandate, and it takes justifiable pleasure in the knowledge of its employees to offer beautiful solutions that are suitable for the vast majority of use applications [14]. Scholarly library staff, on the other hand, have a far more narrowly defined mission: to link groups of readers to pertinent study material in the most efficient manner possible way. Even technical and operational librarians engage in active contact with the front-line touch-points of this endeavor. In an academic environment, librarians also maintain a long-standing history of communication with members of the scholarly and current teachers [14]. Since this emphasizes emphasis on the end-user experience of the person as well as the main business of the institution, with its potential complexity, this emphasis may run the danger of paying a lot of attention to the minor aspects of the university's operations [15]. There's also a risk that consulting services employees might rule themselves out of the dilemma in IT or web-based initiatives because they think it's too difficult or that they're not technically inclined. Library professionals run the danger of being shut out of an important arena for making decisions in this manner.

IT staff may be startled to discover that there is a likelihood of third-party users contribute to a loss of private information, especially concerning e-book notes or sources used for the preparation of coursework. It would cause a significant amount of disruption [15,16]. A system project management plan provides the essential link between the two worlds. It was possible to have frequent meetings of the implementation team, which include members from information technology departments, the library, and the new IdP software provider [16]. Also emphasized is a development of a user-centered quality assurance test strategy that emerges from documented user stories, allowing problems to be discovered and addressed at an earlier stage.

D. Institutional ID over Social ID

The provision of individual members of a platform or site is a major source of large web-based data companies and all their problems. In essence, any online participant – including colleges and their libraries - must react to a propensity or preference to monitor and maximize the use of their web-based services by monitoring and aggregating unique IDs for their users. It is often firmly believed that student activities are always tracked via all the facilities offered by the University, especially library catalogs. It may be argued that user information must be utilized to enhancing the quality of life and relieve the efforts to raise the learning environment and validate tuition costs. Moreover, additional services offered by universities, particularly externally hosted VLEs, may be designed such that batch imports from new subscribers are received and extended to a digital version of the university's user community [16]. Like many other websites, the percentage and respective statistical data of third-party service providers can reflect the number of registered users, and time spent on the platform. In reality, the exercise can be facilitated in the guidelines of a technical team that is required to customize the tools on behalf of students or librarians.

The General Data Protection Regulation (GDPR) requires that 'privacy by default and design' be implemented, and our industry is expected to become more aware of this need as a counterweight to the current prevalent tendency of making liberal use of student’s implicit permission [16,17]. It is feasible to provide and maintain customized memberships on third-party websites while maintaining the privacy of users' personal information. The institution's communication with the third-party provider — in this case, the librarian – is the primary participant in that dialogue. That's only one tiny illustration of how an organization may determine, as Google and Apple have done, how much and in what manner it wants to interact with the demands to maximize use via data-driven business strategies, and how it intends to deal with them [17].

IAM TECHNOLOGY SCOPE IN US

IAM technologies will be used more extensively by the United States Library Services to safeguard its resources against identity theft and other kinds of fraudulent activity. To capture the wider university education setting of evaluation, the ACRL conducts an environmental scan continuously for developments in higher learning [17,18]. Academic Libraries trends reflect these sectors, with the significance of the library in enabling digital research being a notable standout among them [18]. As was the case with the previous resources discussed in the literature study, the highlighted regions were taken into consideration

throughout the creation of the first codebooks. Safeguarding the authenticity and protection of this material, as well as the data systems in which it is kept, is a critical role performed by the library. Policies on data protection in the U.S are a cornerstone of the majority of the University's policies and interventions for Identity and Access Management, which covers access, authentication, and audit controls, among other things.

ECONOMIC BENEFITS

The implementation of IAM in academic libraries will elevate the majority of U.S. libraries to the status of worldwide brands. Nike, Virgin, and Harvard are just a few of the well-known brands on the globe. Universities, like other companies, are increasingly competing and cooperating on a worldwide level [18,19]. As industrialized nations cannot compete on manufacturing costs, they compete on knowledge-based sectors where 'know-how' and identity are essential. With the advancement of interconnectivity and networking, new and significantly improved goods may complement and replace current products while also reaching market opportunities via electronic distribution and existing products can be made available to a much larger market through the Internet [19].

CONCLUSION

This paper provides an analysis of IAM's usability and privacy in academic libraries. The findings from this analysis show that libraries play a unique role in the systematic examination and limitation of data supplied to third-party providers – as both actors of technological partnership and in managing memberships and renewals. Being knowledge managers, librarians must take an active part in knowledge sharing by identifying our position and taking advantage of opportunities. This agreement allows the Library to test advanced functionality important to its operations while being cognizant of the privacy and security concerns of using that data. To put it another way, libraries have an impact on nearly every aspect in the development of new, privacy-oriented standards and access control systems that are being developed. The ability to actively participate will place libraries in a position to significantly factor in adherence to licensing agreements, providing us a more powerful stance on issues ranging from economic and operational concerns to ethical concerns. Given that Apple and Google are placing their futures on whatever philosophy wins the usability vs. privacy argument, it seems to reason that colleges as a whole, and their libraries, in particular, should be able to play a leadership role in the conversation.

REFERENCES

1) N. Bakar and A. Selamat, "Agent systems verification: systematic literature review and mapping", Applied Intelligence, vol. 48, no. 5, pp. 1251-1274, 2018.
2) J. Brady, "Artificial intelligence and natural man", Artificial Intelligence, vol. 11, no. 3, pp. 267-269, 1978.
3) C. Oancea, "Artificial Intelligence Role in Cybersecurity Infrastructures", International Journal of Information Security and Cybercrime, vol. 4, no. 1, pp. 59-62, 2015.
4) S. Rubin, "Knowledge-Based Programming for the Cybersecurity Solution", The Open Artificial Intelligence Journal, vol. 5, no. 1, pp. 1-13, 2018.
5) T. Tagarev, "Intelligence, Crime and Cybersecurity", Information & Security: An International Journal, vol. 31, pp. 05-06, 2014.
6) C. Tschider, "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", SSRN Electronic Journal, 2018.
7) S. Chraa, "Network Centric Warfare and Defence Industrial Implications", Journal of Defense Studies & Resource Management, vol. 01, no. 02, 2012.
8) S. Chraa, "Network Centric Warfare and Defence Industrial Implications", Journal of Defense Studies & Resource Management, vol. 01, no. 02, 2012.
9) D. Dasgupta, "Computational Intelligence in Cyber Security", 2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2006.
10) A. Ghanemi, "Toward overcoming the challenges facing biomedical analyses", Alexandria Journal of Medicine, vol. 51, no. 3, pp. 277-278, 2015.

11) E. Padilla, "Tips to Prevent, Detect & Respond to Cyberattacks: How Safe Is Your Firmware?", IESE Insight, no. 33, pp. 31-37, 2017.
12) Xing Fang, N. Koceja, J. Zhan, G. Dozier and D. Dipankar, "An artificial immune system for phishing detection", 2012 IEEE Congress on Evolutionary Computation, 2012.
13) C. Bitter, D. Elizondo and T. Watson, "Application of artificial neural networks and related techniques to intrusion detection", The 2010 International Joint Conference on Neural Networks (IJCNN), 2010.
14) P. Andrews and J. Timmis, On Diversity and Artificial Immune Systems: Incoporating a Diversity Operator into aiNet, Neural Nets, LNCS 3931, Apolloni et al. (Eds.), Springer, 2005.
15) S. Forrest, A. Perelson, L. Allen, and R. Cherukuri, Self-nonself Discrimination in a Computer, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Los Alamos, CA, USA, 1994.
16) S. Hofmeyr and S. Forrest, Immunity by Design: An Artificial Immune System, In Proceedings of the Genetic and Evolutionary Computation Conference, vol. 2, 1999, pp. 1289-1296.
17) 8.S. Hofmeyr and S. Forrest, Architecture for an Artificial Immune System, Journal of Evolutionary Computation, vol. 8(4), December 2000.
18) H. Hou and G. Dozier, Immunity-based Intrusion Detection System Design, Vulerability Analysis, and GENERTIA's Genetic Arms Race, the ACM Symposium on Applied Computing, Santa Fe, NM, USA, March 13-17, 2005, pp. 952-956.
19) 20.J. Zhan and L. Thomas, Phishing Detection using Stochastic Learning-based Weak Estimators, In Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security, Paris, France, April 2011.