International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

Analysis of Vulnerability Issues and Proposed Solution in a Web Based E-learning Platforms

Sanusi Muhammad &Abubakar Sadik Mustapha
Postgraduate School, Department of Computer Science, University of Abuja, FCT, Nigeria

Date of Submission: 01-03-2023 Date of Acceptance: 10-03-2023

ABSTRACT
E-learning is an electronic means of learning, where internet resources and web based platforms are used. The ubiquitous nature of E-learning platform made them vulnerable, hence it is imperative to study their vulnerability features and deduce solution that will make the platforms defensive. This paper investigates the vulnerability nature of E-learning platforms and proposes model solutions. In this study ten web based E-learning platforms are accessed based on their security and vulnerability functions several vulnerability parameters were considered including, Cross site scripting, Broken Authentication and session management, Cross-Site Request Forgery (CSRF), Sensitive Data Exposure, and many others. In line with these Security measures are proposed using two models: I. Cross Site Script (XSS) Vulnerability Interceptor.2.Finger print recognition system3.Token Based Authentication

Key Words : Analysis, Vulnerability, Web based, Solutions

I. INTRODUCTION

The application of E-learning technology in knowledge delivery is receiving great attention because it facilitates teaching and learning activity. According to Almarabeh, (2014), e-learning refers to the "use of Information and Communication Technology e.g. internet, computers, Mobile phone, Learning Management System (LMS), Televisions, Radios and others to enhance teaching and learning activities". Similarly, e-learning has been defined as the use of electronic media, Information and Communication Technologies (ICT) in education (Saidu, 2015). The new technologies including ICT and e-learning have become the driving forces in most tertiary institutions today (Tarus, 2015). It has been adopted globally and to a greater extent in the developed and a few in the developing countries. However, with its application worldwide, e-learning has not been utilized optimally in education in Nigeria (Atsumbe et al 2016). This is likely due to some challenges that tend to militate against the use of this facility in the universities, polytechnics and colleges of education across the country. At the same time whatever technology is introduced in the market, people are concentrating more on the security features of those technologies irrespective of an electronic gadget or a web technology. The society is now conscious on the security features of the technology when it comes to a web source, due to infinite vulnerabilities.The aim of this paper is to analyze the vulnerability issues of web based e-learning platform and propose security measures.

II. LITERATURE REVIEW

In a study by Adebayo &Abdul Hamid (2014) examined the impacts associated with challenges and security lapses of the existing electronic-examination system with aim of upgrading and developing a new e-examination system that takes care of the challenges and security gaps associated with the existing systems. The methodology accepted for the study was interviews and questionnaires. The result exposed that the new system uses data encryption in order to protect the questions sent to e-Examination center through the internet or intranet and a biometric fingerprint authentication to verify the stakeholders.

Researcher (Kamba, 2019) examined and discussed the problems, challenges and benefits of implementing E-learning in Nigerian universities. Survey methodology was adopted for the study. The result found that awareness of e-learning among the universities is very high but investment and commitment to develop an e-learning application is very poor and below expectation. This assertion conforms to Almarabeh (2014) and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

Adewole-Odeshi (2014). Moreover, the research outlined that lack of sufficient trained ICT professional has been a recurring focus in ICT. Also, the study further revealed some factors affecting successful implementation of e-learning in Nigerian Universities such as: (i) Inadequate instructional materials (E-books, CD-ROM), (ii) Lack of tutorial support from instructors, coaches, tutors or technical staff (iii) Poor telecommunication tools like internet facilities, (iv) Lack of collaboration for social communication learning with the instructional demand for active learning, (v) Irregular supply of electricity, (vi) Insufficient fund to upgrade and maintain the equipment and facilities, (vii) Bad policy implementation, and (viii) Lukewarm attitudes towards e-learning process by staff and students. These claims were maintained by (Sife, et al 2007) who further argued in agreement with Tarus et al. (2015) that ICT implementation challenges include (i) lack of awareness and attitudes towards ICTs (ii) inadequate technical support (iii) transforming higher education (iii) lack of staff development and ownership .In depth review of related work was adopted for the review of the paper. Furthermore, the result obtained by (Kamba, 2009) shown that most common encountered problems are unreliable internet connection and mobile lines, slow access to website due to insufficient bandwidth and limited number of computers connected to the internet.

To analyze the vulnerability issues several number of simulations and analysis were conducted and presented in Table 1to Table4. Table 1presents presents the challenges and vulnerability issues in various E-learning platforms. Table 2 presents Security Measures On Vulnerability Issues In Web Based E-Learning. Table 3 presents E-learning Platforms Scanned to obtained their measure features and vulnerability associated while Table4 presents the Results Of Vulnerability Found from the analysis and online scanning of the E-learning platforms.

Table 1: Web Based ELearning Vulnerability Platform Challenges

NUMBER	PARAMETR NAME	DESCRIPTION
1	Cross-Site Scripting	Taking untrusted data and sending them it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites
2	Injection	Injection flaws, such as SQL, OS, and LDAP injection
3	Security Misconfiguration	Secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Software should be kept up to date.
4	Broken Authentication and Session Management	Application functions related to authentication and session management incorrectly implemented, leading to compromise of passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities
5	Insecure Direct Object References	Exposing a reference to an internal implementation object, such as a

		file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data
6	Missing Function Level Access Control	Verifying function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, access to functionalities without proper authorization is possible
7	Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This makes the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim
8	Invalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, victims can be redirected to phishing or malware sites, or use forwards to access unauthorized pages
9	Sensitive Data Exposure	Sensitive Data Exposure Not properly protecting sensitive data, like credit cards, tax IDs, and authentication credentials. Sensitive data deserves extra protection like encryption at rest or in transit.
10	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities Components, like libraries, frameworks, and other software modules, nearly always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a variety of possible attacks

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

Table 2: Security Measures On Vulnerability Issues In Web Based E-Learning

NUMBER	NAME	SECURITY MEASURES
1	Cross-Site Scripting	**Filter input on arrival**: At the point where user input is received, filter as strictly as possible based on what is expected or valid input. **Encode data on output**: At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding. **Use appropriate response headers**: To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend. **Content Security Policy**: As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.
2	Injection	**Step 1: Train and maintain awareness** To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page **Step 2: Don't trust any user input** Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input. **Step 3: Use whitelists, not blacklists** Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only. **Step 4: Adopt the latest technologies** Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQL
3	Security Misconfiguration	. Developing a repeatable patching schedule . Keeping software up to date . Disabling default accounts . Encrypting data . Enforcing strong access controls . Provide admins with a repeatable process to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

		avoid overlooking items . Set security settings in development frameworks to a secure value . Run security scanners and perform regular system audits
4	Broken Authentication and Session Management	. Credentials should be protected: User authentication credentials should be protected when stored using hashing or encryption. . Do not expose session ID in the URL: Session IDs should not be exposed in the URL (e.g., URL rewriting). . Session IDs should timeout: User sessions or authentication tokens should be properly invalidated during logout. . Recreate session IDs: Session IDs should be recreated after successful login. . Do not send credentials over unencrypted connections: Passwords, session IDs, and other credentials should not be sent over unencrypted connections.
5	Insecure Direct Object References	**1.Logically Validate References** Every web-application should validate all untrusted inputs received with each HTTP Request. At a minimum, the application should perform "whitelist validation" on each input. This means verifying that the incoming value meets the applications expectations for that input, such as: .Minimum or maximum length .Minimum or maximum bounds (for numeric values) .Acceptable characters **2 Use Indirect References** An alternate approach to avoiding Direct Object Reference vulnerabilities involves embracing a design approach in which actual references to application-managed resources (such as ids, names, keys, etc.) are replaced with cryptographically strong random values that "map to" the original values. The mapping between the random values and their actual values is maintained on the server, so the application never exposes direct references. This is a more intrusive remediation than mere logical validation, as it impacts the application design
6	Missing Function Level Access Control	• Use an easy authorization module to invoke rules • Don't hard code, ensure module can allow the admin to update and audit rule easily. • Ensure authorization is enforced in the controller or business logic • Avoid assigning permission on a per user basis
7	Cross-Site Request Forgery	•Implement an Anti-CSRF Token An anti-CSRF token is a type of server-side

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

	(CSRF)	CSRF protection. It is a random string that is only known to the user's browser and the web application. The anti-CSRF token is usually stored inside a session variable. On a page, it is typically in a hidden field that is sent with the request. •Use the SameSite Flag in Cookies The SameSite flag in cookies is a relatively new method of preventing CSRF attacks and improving web application security. In the above scenario, we saw that https://attacker.com/ could send a POST request to https://example.com/ together with a session cookie. This session cookie is unique for every user, so the web application uses it to distinguish users and to determine if they are logged in
8	Unvalidated Redirects and Forwards	Simply removing the redirection mechanisms? If you can do without it, then just get rid of this kind of behavior. The simpler, the better. • verifying the "referrer" during the redirection process, to make sure external websites do not send Potential victims to your redirection page. It should come from your website. deactivating redirections to domains you don't manage. •using a destinations whitelist • signing redirections with a hash, in order to validate the authenticity of the URL the user will be redirected to.
9	Sensitive Data Exposure	1.The first step is to avoid dealing with data you don't really need to collect on the website, and avoid storing data that does not need to be stored. That sounds quite easy, and it is. During the functional and technical design of the web application, take enough time to evaluate the need to collect/store. 2. Identify sensitive data, and ensure it is encrypted with the appropriate algorithm, when transmitted, and when stored. 3. Ensure strong and non-deprecated algorithms are used. The OWASP and many other sources of information will tell you which on is good and for which purpose. 4. Run a web application penetration test, to make sure you did not miss anything. Running a security audit periodically will also help you ensuring that your web application remains strong over time

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

10	Using Components with Known Vulnerabilities	Disabling unused components is also important. If you don't use a component in your web application, remove it. That's one potential security flaw solved quite easily.

Table 3: E-learning Platforms Scanned

NUMBER	ELEARNING PLATFORMS SCANNED
1	A Tutor (http://atutor.ca/atutor/)
2	U Lesson (https://www.ulesson.com)
3	Edufirst (https://www.edufirst.ng)
4	Noun (https://www.Nouonline.net)
5	Ubongo (https://www.ubongo.org)
6	Learncora (http://www.learncora.org)
7	Udemy (https://www.udemy.com)
8	Prepclass (https://www.prepclass.com.ng)
9	Myafrilearn (https//myafrilearn.com)
10	Class notes (https://classnote.ng)

Table 1 Results Of Vulnerability Found

ELearning Platform	A Tutor	U Lesson	Edufirst	Noun	Ubongo	Learncora	Udemy	Prepclass	Myafrilearn
Software Security					√	√		√	
Vulnerable JavaScript library	√	√				:			
SQL Injection of any kind					√	√		√	
Cross Site Scripting of any kind	√								
Directory traversal				√					
Headers Security Check	√	√			√			√	
Content Security policy Test	√				√			√	
CRLF injection/ HTTP response splitting								√	
File inclusion								√	√
HTTP parameter pollution			√		√	√		√	

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

III. PROPOSED SOLUTIONS

Several number of solutions are proposed to counteract the vulnerability issues understood from the analysis in section 2. The solutions include the finger print model, Cross Site Script model and token based authentication system all presented in Figure1, Figure 2, and Figure 3 respectively.

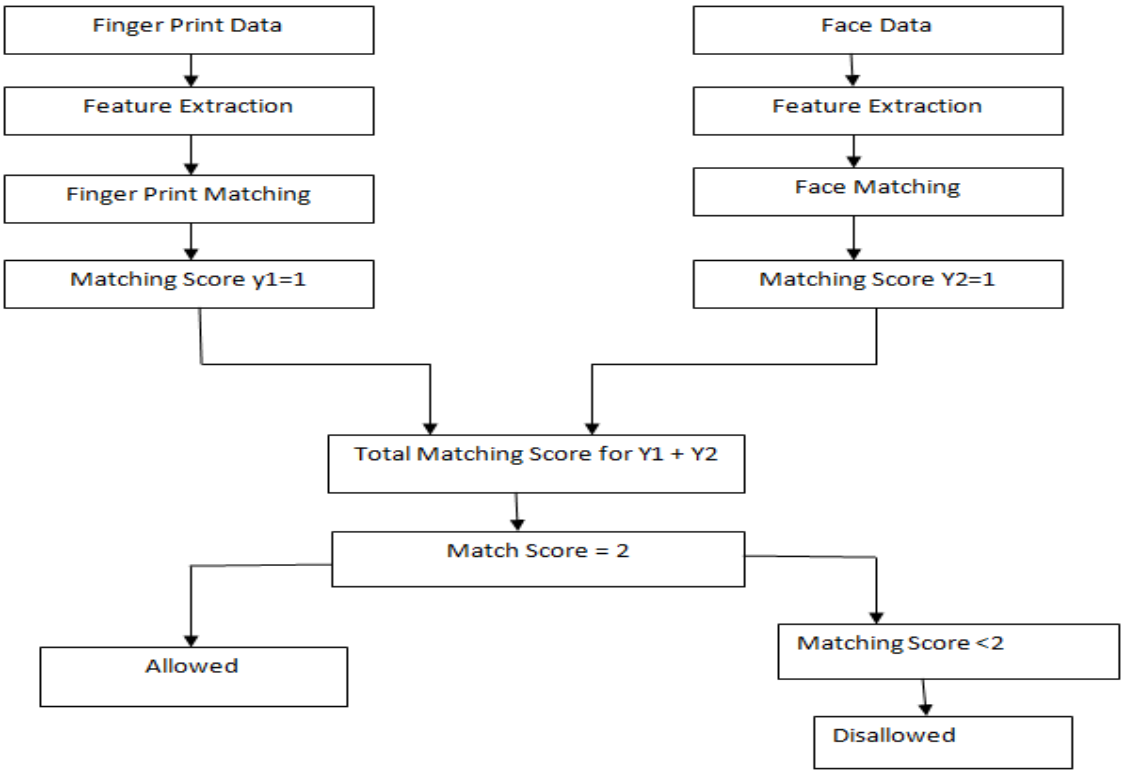

Figure 1 :Proposed model- The Finger Print Recognition system

The finger print recognition system is responsible for the recognition and matching the input fingerprint against the fingerprint template store in the database to obtain fingerprint matching scores. And also the face recognition system is responsible for matching the input face against the template stored in the database.

The score level will integrate the matching scores (score y1 and y2) in other to make the matching score.Matching Score will be computed as follows:Y1 =1 + Y2 = 1 and Y1 +Y2 = 2Where y1 and y2 are finger print and face matching score such that it is constant y1 + y2 = 2, else Disallowed

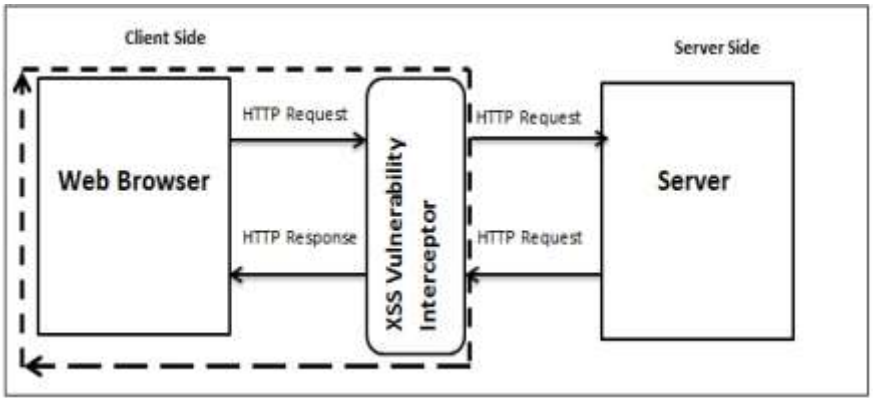

Figure 2 :Cross Site Script (XSS) Vulnerability Interceptor

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 650-659 www.ijaem.net ISSN: 2395-5252

The propose approach consists of an interceptor between browser and server for detection of XSS. In this approach all the HTTP traffic between client and server is exchanged through interceptor which employs filtering to check for possible attacks in source code to be executed by browser. There are no direct communication channels between browser and server. Normally, when a client intents to visit a website by typing the URL into the address bar. The URL is send to the web server for lookup and if found response is generated and cookie is setup in browser. In this approach the generated request from the browser is intercepted by interceptor which performs the scanning of the website on the server to get all the URL's of the possible web pages of that website.

The web pages are the divided into two categories: the form based web page and non-form based web page. Special designed payload will be injected into the input field of the form based web pages and changes in the values of the parameters will be noted. If any change of values found, the page will be considered as suspicious. The address of the suspicious page will be maintained by the interceptor. The list of address of all non-suspicious pages of the website will also be mentioned in separated file by interceptor. The source code of the suspected code will then be passed to the white list filter to find any attack. The non-suspicious pages will be passed through black list filter for any malicious script.

3.3 Token-Based Authentication: Token-Based Authentication (TBA) is an authentication mechanism mostly used for authentication of API requests. In this mechanism, the user is issued an API access token upon successful authentication, which will be used while invoking any API request. In this process, a cookie will never be issued by the server. Once a user inserts the token and provides a PIN, their system is authenticated and can reach a protected E-learning website or platform.

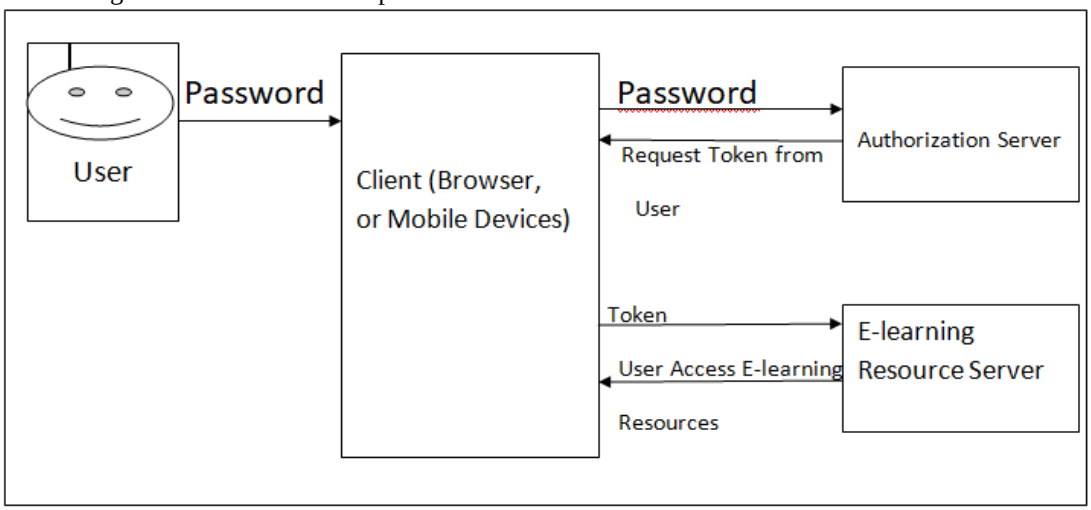

Figure 3 :Token Based Authentication to access E-learning Platform

The Token-Based Authentication works as Follows:

1. The user enters his credentials (i.e. the username and password) into the client (here client means the browser or mobile devices, etc).
2. The client then sends these credentials (i.e. username and password) to the Authorization Server.
3. Then the Authorization Server authenticates the client credentials (i.e. username and password) and generates and returns an access token. This Access Token contains enough information to identify a user and also contains the token expiry time.
4. The client application then includes the Access Token in the Authorization header of the HTTP request to access the restricted resources from the Resource Server until the token is expired.

IV. CONCLUSION

The study fully focused on the Vulnerability issues in Web based e-learning technology. So people may continue to work on my research limitations presented. That kind of research will imply to bring more powerful and effective products. Apart from this, my research will found to be useful in mobile e-learning

technology as there are Vulnerability issues in mobile technologies too.

REFRENCES

[1]. Hussain S., Wang Z., and Sun C. (2011) 'A comparative study of open-source learning management systems in Open-Source Software for Scientific Computation (OSSC), 2011 International Workshop on (pp. 86–93).

[2]. Jamil D., Zakih.,(2017), 'Vulnerability Security'. International Journal of EngineeringScience and Technology (IJEST) (pp. 126-127).

[3]. Jensen, Schwenk, (2009); On technical security issues in cloud computing. In, Ieee, (pp109-116)

[4]. Kumar a., Pakalar.,(1998); The virtual learning environment system. In, IEEE, (pp711-716)

[5]. Laisheng X, Zhengxia 'Web based E-learning: A New Business Paradigm for E-learning. In, 2011. IEEE, (pp716-719);

[6]. Strauss, Corbin Jm(1990) Basics of qualitative research: Grounded theory procedures andtechniques, Sage Publications, Inc. (pp 127-129);

[7]. Swenson M (2011) 'E-Learning standards and technical specifications. Disponibleon-line: http://www. luvit. com (pp123-127);.

[8]. Van Harmelen, (2006) 'Personal learning environments. In,.Citeseer,(pp 815-816)

[9]. Vaquero L, Roderp -Merino (2019); A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer CommunicationsReview,Vol 39 (1),(p50-55)

[10]. Adebayo O; and Abdulhamid S; (2014); E-Exams System for Nigerian Universities with Emphasis on Security and Result Integrity (p0921-1402);

[11]. Adewole-Odeshi, E. (2014); Attitude of Students Towards E-learning in South-West Nigerian Universities: An Application of Technology Acceptance Model. Library Philosophy and Practice, 0_1(p45-50);