SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 7 | July 2021 - Peer Reviewed Journal

A STUDY ON THREATS TO MOBILE-LEARNING

[1]Nikhil Pinnamaneni, [2]Sai Charan Muvva, [3]Sumanth Dodda

[1,2,3] *SCOPE, Vellore Institute of Technology, Vellore, 632014, Tamilnadu*

Article DOI: https://doi.org/10.36713/epra7696
DOI No: 10.36713/epra7696

ABSTRACT

Mobile devices are used a lot today and are owned by a huge percentage of the population. Many use mobiles for not just playing games or calling, but also for learning. Mobile learning is a domain that is growing at a very fast rate. Universities are using these devices to target the isolated demographic that has no choice but to rely on mobiles for learning. Some supporters and engineers of mobile learning in colleges are developing and providing infrastructure and content for learning on cell phones totally disregarding the danger of partner knowledge, while using these developments in portable learning is a genuine test. There is a gigantic danger to the privacy, trustworthiness and accessibility of those associated with the creation the substance and conveying the picking up, including the understudies. This paper looks at and presents the security weaknesses and dangers the of mobile learning for the students. This paper distinguishes the security dangers that numerous understudies will confront when utilizing mobiles for learning and analyses the hurtful issues of versatile learning on understudies in situations where a security penetrate happens. This paper presents an argument as to why fixing these issues is important. Ultimately, this goal of this survey is to present the importance of mobile learning security threat and exploring the existing threats and conclude with recommendations for various threats.

KEYWORDS— *M-learning, DDoS, Security Attacks, XSS, CSRF, SQLi.*

I. INTRODUCTION

Mobile learning, or m-learning, is the provision of training or educational material or learning support on any mobile device (smartphone or tablet). Mobile learning facilitates and allows people to learn virtually anywhere, even in remote locations, and anytime as long as they have a smartphone. The usp of m-learing are the massive improvements in mobile technologies facilitating better content and more interactivity, improving the experience for the learners along with the freedom that they can use it at any time and share**[1].** The web is filled with data right now and learners have been using it to learn new things for a long time now. From websites like wikipedia to stack-overflow, all of the web can be accessed from a mobile to facilitate m-learning. Mobile learning is everywhere, easy to use and rich in content , high productivity, usability, interactivity, portability and other scenic spots of sale that can be used to compete with traditional teaching and learning school **[1].**

Mobile learning is without any doubts a new way of learning. It emerged from the need for a versatile alternative to conventional education, and created a versatile learning environment that anyone can use anywhere at any time according to their convenience making education more inclusive than ever **[2]**. The coming of 4G and improvement in video streaming and capacity for a mobile to multimedia have pushed m-learning forward. A long running battery along with affordable rates have made mobiles very accessible and thus mobile learning accessible. The interest for mobile learning has come from a lot of different places or demographics. Advances in technology have come, for eg. 5G will be mainstream soon, and this generation has a higher affinity with mobiles and this interest has made m- learning more popular. No longer would a learner be set in front of a computer desk. Mobile learning lets you study at your leisure in small modules and tasks, be a completely engaged person, and choose when and how much to study in your spare time **[1].** M-learning has the ability to be widespread and completely personalized allowing the learner to choose their subject matter, time and location of study **[2]** Recent times, the pandemic, have shown that the traditional school of teaching can't be done anymore. People have had to switch to mobile learning to facilitate the current situation and with a looming uncertainty as to when things will recover, there has been an increase in the use of mobile learning.

This popularity has however lead to some issues. As observed, the more popular a software or domain gets, the more unwanted attention it receives from hackers and the like **[3].** Case in point being Microsoft Windows and MAC OS with the former being more used and ultimately targeted. The same has been observed in mobile learning. A lot of unwanted attention has exposed a lot of flaws in the existing infrastructure. There is a neglect in security for these apps and the entire domain in general.

The first part of this paper is a review of activities related to mobile learning and the security issues surrounding them. It reviews several studies on m-learning safety and reviews recommendations made in the literature. The second part is a literature survey on mobile learning. The third part deals with research done on security issues and the different types of threats they face. The fourth portion of the paper provides a brief description of the research results analysis, and proposes potential solutions. The final section of the article summarizes the findings and discusses recommendations for dealing with security issues mentioned in previous sections. This paper concludes with the problems encountered during the investigation and instructions for future work to ensure a safe and secure learning environment for students who have no choice but to use mobile learning.

II. LITERATURE SURVEY

Mobile devices are the primary targets of digital attacks by the hackers and cyber criminals. In today's world it became so easy for the cyber criminals or hackers to perform cyber-attack as it is more easy and less risky than the physical attacks as it only requires computer and an internet connection. Latest report in security written by Nachenberg states that there has been a rapid increase in the number of mobile device attacks **[11].**

As the usage of internet is growing daily it is occupied with large number of hackers and attackers. And as the mobile devices are limited with amount of resources to support strong measures for security which makes them easily affected by attacks. Various security models suggest the IPSec protocol backtracking and prevention as techniques for reverting the Denial of service (DoS) and Distributed denial of service (DDoS) attacks on the mobile nodes. Nepal and Jang-Jaccard observed that the number of cyber-attacks are increasing and becoming potentially more attractive and destructive than before as the mobile technologies are increasing and the victims of these attacks are also growing rapidly **[12].**

Boyinbode states that m-learning is the access point for digital learning for many graduate students and that is playing an important role in the era of digital learning by bringing it to students in rural areas **[11]**.

Mobile devices provide innovative ways for students by enhancing their experience of learning. But these mobile devices are prone to risks. Educational institutions and as well as all the educators are worried about the rise in threats to the individuals data security and privacy. As the mobile devices allow to share text, video and as well as audio content it becomes more easy and efficient for a student to learn from their own place. But also studies conducted show the various adverse affects of m-learning as it may lead the students to join the negative groups and connect with negative communities on social media which may result in ending up having a great negative impact on their career. As most of the people are unaware of the dangers of cyber threats they can be their own cause for victim of cyber attacks **[12]**.

The people are unaware of the conditions which exploit their privacy. As the technology is developing, hackers and cyber criminals are finding new ways to perform attacks on the mobile devices. There are various concerns about the negative adoption that lead from the usage of technologies for learning. The most important ones are the security risks and the exposed attack issues on various contents used for learning and sensitive data on the devices used. These issues also are transferable as they are widely used for education purpose. There are many risks such as interference of students with the learning content and instructions. The securing of e-learning and mobile learning requires neglecting and preventing modification, fabrication, interception of the learning and to protect privacy, as well as to protect from piracy and changing of the data. Controlling the access modifiers is very important to avoid all the threats and we can use authorization and secure authentication for this.

Issues related to security in m-learning platforms and applications which are exploited and related to attackables in OS and the errors or flaws in the application software or the facilities of the network. The applications are built on three tier architecture. This three tier architecture consists of database layer, application layer and a client layer. Due to the closeness of architectures many security issues in e-learning also occur in m-learning. And among these the most security issues occur at database and at level of application layer and at client level they are dissimilar..

III.SECURITY ATTACKS

There are mainly some specific reasons for attacking a website. Getting Access To Information On The User

As mobile devices become more effective units for storing personal information, they are more attractive to violate user privacy. Today mobiles come with a lot of features, from voice recorders to cameras to 4g. The attackers are attempting to be eventually targeted at both the secrecy be credibility of the encrypted records. A effective attack will allow the attacker to read alot of present user information on the device. In addition the aggressor can catch or send a false SMS, forward emails to other mailboxes, and access p ersonal information and calendar. Additional data can be retrieved by reading instant messaging request files, data stored by software used to access social networks, or browser-

stored data. Any additional data in the computer memory or SD card, such as records, images or videos, may also be affected **[4]** (mobile attack threat paper). Overall, the increase in dependence on phones is a two edged sword that can be problematic.

Additionally, tapping into simple hardware features of the phone offers a chanceto gather extra records from the user's environment. The intruder can transform the infected c ell phone into a listening device, by using the voice recording hardware. Accessing the camera offers an opportunity to take images of the user's surroundings or to film video[5]. Additional leverage can be gained by leveraging the location information to violate the user's privacy. Mobile devices may provide positioning information using the GPS module, or use the service provider's network infrastructure to triangulate the positioning. This can prove to be catastrophic and could be life threatening if the information were to end up in the wrong hands.

Noxious Or Damaging Malicious Acts The increase in computing capacity focuses on contemporary mobile devices for malicious at tacks with the goal of covertly leveraging the power of raw computing in conjunction with ac cess to broadband networks. Top of the line cell phones , for instance, have CPU working frequencies more prominent than 1GHz, and physical memory far over 512 MB. Moreover, parallel processing processors for mobile devices are under development. Mobile devices, together with high-speed Internet connectivity, will become attractive in case of malicious attacks, such as botnet deployment **[6]**.

Detrimental hacker acts are intended to generate frustration for the owner of the software, rather than perform beneficial assignments for the attacker and this is something developers tend to ignore. While such acts of noxiousness are usually readily available, they are done to cause as much harm to the user and create as many problems as possible and it is important to understand this. Especially in the context of a people who use mobile learning, the attacks can be in very regressive and are usually things like data loss to battery depletion of devices and other resources, overall creating a bad experience for uses who just want to learn and gain knowledge. **[3]**. Also, by gaining access to sensitive systems the attacker can cause permanent damage and disable the device.

Attacks or security issues in M-learning systems are Cross site scripting (XSS):

Cross site scripting (XSS) assaults are one of the most well-known types of security assaults. It is a standard vector assault that introduces pernicious code on a weak web application. It changes in a manner that doesn't straightforwardly distinguish the framework yet rather the clients of the web application are the most powerless.

An effective normal content assault can have genuine ramifications for the notoriety of an online business and its associations with its clients.

Contingent upon the result of the assault on clients' records that can be hacked or diminished, deception projects and page substance might be adjusted, which will lead clients to deliberately give their data **[15]** Finally, meeting treats might be shown, empowered by the culprit to mimic clients and bargain their records.

Cross-site scripting (XSS) assaults can be isolated into two kinds:

I) Saved

ii) Demonstrated

The very much kept Cross site content, otherwise called site cross-site, is the most harming of the two. Happens when a noxious content is introduced legitimately into the introduced web application.

Cross-demonstrated content feeds noxious content presentation from a web application, client or customer program. The content is installed in the connection, and possibly works when that connection is clicked.

Cross-cutting is a danger presented by digital protection accidents, Javascript and Html as the fundamental driver of this misuse. In 2008 Symantec Corporation detailed that cross webpage scripting assaults on sites represented around 84% of all security hazards **[15]**. Cross site content as a rule alludes to page sections made on the customer worker side. The possibility of a cross webpage content is to make web customer records do what the noxious client needs. Such misrepresentation can install the content on an unstructured page each time a page is stacked, or at whatever point a related occasion is held **[12].** Content assaults can be utilized to accomplish the accompanying results:

I) Access touchy data

ii) burglary of your own data

iii) change the usefulness of the program

iv) expulsion of web application

v) Refusal Attack (DoS) Attack.

In any case, alternate routes to site contents can be limited by making sure about HTML passages, by putting treat security in the program, by utilizing a substance security strategy, by utilizing JavaScript sandbox instruments, and by utilizing different break techniques.

Application for fake site (CSRF)

A fake application (CSRF) otherwise called XSRF, Session riding or seaward, is a kind of assault that fools an internet browser into making an undesirable program when a client or customer is signed in. deceitful assaults can be incredibly hazardous for both the client and the business. Client business connections will be seriously harmed as business foundations may not recover the trust of clients. It can likewise prompt unapproved moves, secret word changes and the burglary of significant data that may incorporate meeting treat subtleties.

Cross site imitation (CSRF) application assaults are frequently done utilizing risky social designing strategies, for example, utilizing a connection or email that fools a client into sending a false solicitation to a worker from their side which eventually prompts an assault **[16].**

Cross-Site Request Forgery (CSRF) assaults that stunt the casualty into downloading a page containing a pernicious solicitation. It is hazardous as in we utilize the casualty's character and rights to perform pointless obligations for the person in question, for example, changing the casualty's email id, home or private location, or secret phrase, or utilizing individual data to buy a thing. Struggle Request Attack (CSRF) normally recognizes exercises that cause state change on a worker yet can likewise be utilized to get to private information. On most sites, programs will naturally introduce those applications with any site-related treats, for example, client meeting treats, their confirmation subtleties, their IP address, Windows area qualifications and that's just the beginning. Hence, if a client has now signed in to the site, the site won't stray from this current client's authentic solicitation. Along these lines, the aggressor may make the casualty do things the individual didn't expect to do, for example, login, buy any things, change account subtleties, access account data, or different administrations gave by those weak web applications **[16].**

Cross webpage phony (CSRF) application alleviation procedures work by adding extra check information to applications that permit web applications to get applications from unapproved destinations. Notwithstanding this there are numerous approaches to diminish CSRF assaults. Obviously:

I) Sign out of web apps when you are not utilizing them
ii) Verification of login subtleties
iii) By not permitting programs to recollect passwords
iv) To abstain from perusing all the while when you sign into a web application

In web applications, there are numerous answers for forestall a great deal of vindictive traffic and forestall risky assaults. Among the most widely recognized approaches to forestall the creation of arbitrary tokens for all meetings or ID demands. This was later tried and confirmed byworker. Meeting demands for copy tokens or missing qualities can be restricted. On the other hand, an application that is certifiably not a substantial ID token for its time is confined from getting to the application.

Moving treats twice is another known strategy for forestalling cross-demand extortion (CSRF). Like utilizing various tokens, irregular tokens are appointed to both the treat and application boundaries. The worker at that point confirms that the tokens are the equivalent before conceding admittance to the framework **[11].**

While running these tokens can be shown in numerous areas, including program history, in HTTP login documents,

SQL injection attack

SQL injection is an injection of malicious code technique which is used to attack the applications which are data driven. In those data driven applications malicious SQL statements are inserted in the entries for their execution. The SQLi must exploit the vulnerabilities in applications. SQLi is known by the websites as an attack vector which can be used to attack any type of SQL database **[14]**. These SQL injections allows the hackers or attackers to spoof the identity of the person and tamper with existing data, they can also cause repudiation issues like nullifying the transactions and changing of the balances, they also allow for complete exposure of the data present in the system, they can even destroy the entire data or can make it unavailable and unidentifiable and can become administrators of the database. It is considered as one of the top most application vulnerabilities of 2007 and 2010 by OWASP **[13].**

There are four main types of SQL injection.

They are:

i Classic or normal SQLi
ii Blind SQLi
iii Database system specific SQLi
iv Compunded SQLi

SQLi is the short form of Structured Query Language injection which is used in the website address and performs various searches using the search engines like (google, yahoo, bing etc.) to hack personal information of the users like passwords, usernames etc. This method can be used by the hackers to pass input as a string which contains malicious code to run some unexpected activity which acts in a malicious way. These kind of queries access unauthorised data, they can bypass the user authentication or even shutdown the entire database of the web application even if it is present in some different server. These SQLi's can also be applied on URLs. These URLs are modified and changed in a manner to access important information of the user. This SQL injection attack can be prevented by following some austere rules and best practises of security.

The methods used to mitigate this SQL injection attacks are:

i Checking the input from user for dangerous characters like ';'
ii Using statements which are well prepared

iii Encrypt the sensitive information

iv Check whether the errors are saying anything about the architecture of the database.

v Maintain a limit of access to the database in order to avoid the SQL injection attacks from unwanted or unknown users.

Session Hijacking:

The commandeering of the meeting is tied in with exploiting the client's online control of the framework that is ordinarily held by a meeting token. As the http convention utilizes different TCP associations the different web application workers require an approach to distinguish all association demands made by the client. The best strategy is only sending a symbolic sent by a web worker to a customer program after a fruitful customer check. The meeting token contains a wide scope of links and can be utilized in an assortment of ways, for example, a URL, or in a HTTP call header, for example, a treat, or in the header or body of a HTTP demand body **[17].**

This assault takes or predicts a substantial meeting token and utilizations it to increase unapproved admittance to a web application worker.

The most widely recognized approaches to seize a meeting token are:

i Use a predictable session token

ii Session sniffing

iii Perform client-side attacks like (Trojans, harmful javascript codes, Cross site scripting etc.)

iv Perform Man-in-the-middle attack (MIM)

v Perform Man-in-the-browser attack

vi Using tools for session hijacking Like:

- Wire shark
- T-SightS
- Hunt
- Hamster and ferret

The session hijacking is possible when the ID of the session is encrypted weakly or too short or can be predicted easily. Usually sessions which do not expre on the HTTP server may allow an attacker or hacker to peform unlimited guesses in order to brute force the valid and authenticated session id. In addition to that a session id can be loged in and cached in some proxy servers. When the user requests are tranmitted via URL, the requests can potentially kept in history of the browser, may be in cache or even in the bookmarks **[11]**. This data can be viewed afterwards also.

Methods to mitigate session hijacking are:

I. Set a secure session link via HTTPS

II. Encrypt user’s browser and the web server using end to- end encryption method by secure HTTP or SSL.

III. VPNs can be used for encryption

IV. Generating long and random session cookies by the web servers which reduces the chances of predicting or guessing of the session cookie.

V. Session ID monitors can be used to monitor if these IDs are used and tools like Blacksheep can be used to send fake IDs of the session in order to check if an intruder is trying to hack the session ID.

VI. Once a session ends there should be an automatic log out and the client must use different session ID inorder to re-authenticate

VII. A server can be given instructions to delete a session cookie which is exposed or disclosed in the network.

DDoS Attack:

DDoS Attack A DDoS (distributed denial-of - service) attack is a kind of attempt to interrupt general targeted server traffic and introduce additional flooding to the network. About traffic. Mobile and computer programmes can be used to hack computers. A DDoS assault is a a sort of tourist jam that obstructs the highway, protecting ordinary travellers from arriving at their ideal holiday location.

[18] A distributed denial-of-service attack wants an attacker to control network of mobile learning application to carry out an attack. Mobile application are contaminated with malware, converting each one into a bot. The attacker can have the remote control over a bunch of bots which is known as botnet. If the botnet is settled, via

the method of remote control can directly control the mobile application by sending updated instruction to each bot. When the ip address of targeted user is attacked by the botnet,

each bot will send a packet known as request packets to the target, thus causing overflow of the targeted mobile learning server, resulting in denial of service to general traffic.

Denial of service in mobile learning can be prevented by maintaining decent security procedures that can help to protect application from hacking activities. A scheduled renovation policy for m-learning servers and network infrastructure, in addition to an uninterruptible

energy deliver, can also prevent provider denial by means of offering a constant strength deliver. DoS occured from the network breach can be avoided by using prevention technique such as reverse proxies spread across multiple hosting locations**.[19]** Various step to prevent DDoS attacks are :-

A DDoS (distributed denial-of-service) attack is a type of attempt to disrupt general traffic of targeted server and netwwork are introduced by additional flood of traffic. Exploited machines can be mobile and computer application. A DDoS attack is a type of visitor jam clogging up with highway, protecting normal visitors from arriving at its desired vacation spot.**[18]** Various step to prevent DDoS attacks are :-

A. Buy more Bandwidth :-
One of the most masic way to protect from DDoS attack is to increase enough bandwidth so that it can handle spikes in network traffic that can be caused by malicious activity.

B. Configure your network hardware against DDoS attacks :-
Many various hardware configuration changes are available to prevent mobile learning application from DDoS attacks.
For example - Configure your system firewall to ignore various ICMP packets from external network, which can help us to prevent certain ping based volumetric attacks.

C. Protect your DNS servers :-
Always remember that most of the malicious actor aims to bring your Mobile learning servers offline by DDoSing your DNS server. So due to this reason your DNS server should have redundancy and placing them in specific data centres at the back of load balancers is also a good concept. A better solution may also also be to move to a cloud-based DNS server that could offer large bandwidth and a couple of points-of-presence in information facilities around the world.[20]

Man in Middle Attack

A man-in-the-centre assault (MITM) is an assault wherein the assailant covertly sends and can modify correspondence between two gatherings that trust it is immediate correspondence. One case of a MITM assault is the utilization of dynamic eavesdropping, in which the assailant connects with the people in question and passes on messages between them to cause them to accept that they are talking straightforwardly to one another through private correspondence, and in reality the entire discussion is constrained by the aggressor. The aggressor must have the option to take all the proper messages that go between the people in question and infuse new ones. This is valid as a rule; for instance, an aggressor inside the scope of getting an unlisted Wi-Fi hotspot can go about as an arbiter. **[21]**

While utilizing other security calculations, for example, Deffie Hellman, an outsider can get to and change the message when it is moved from understudy to framework for versatile perusing. Mobile phone perusing is perhaps the greatest concern. **[21]**

There are four key highlights of the MiTM assault procedure:

Mindfulness and Education:

Human blunder is related with a higher level of digital assaults, for example, MiTM assaults. Individuals coincidentally click an awful connection or utilize their login information on a degenerate site, giving programmers admittance to the entirety of their information. To evade this, instruction is basic, particularly in business. Guaranteeing that workers know about the fundamental standards of forestalling digital assaults when all is said in done, and MiTM assaults specifically can spare a great deal of time and cash.

Straightforward things like training representatives to keep away from public wifi organizations or instructing individuals what an email to take delicate data looks like can go far in forestalling these assaults. Holding customary security times to stay up with the latest and requiring secret key changes is typically a couple of basic advances you can take to remain safe from MiTM assaults.

Encryption and VPNs

Utilizing encryption on all gadgets that contain touchy data and utilizing private organizations (VPNs) when associating with informal communities includes an additional layer of security against MiTM assaults.

VPNs make a protected and encoded channel for information sent over the Internet from a gadget or organization. Utilized for a long time, VPNs distantly worked as pipelines secured by all information going through them, making them powerful against MiTM assaults.

Firmware and Software Update Policy : One of the manners in which MiTM programmers access frameworks is to utilize obsolete programming and firmware in the framework. Having an arrangement that stays up with the latest keeps likely focuses from MiTM access. Ideal projects have all the current security highlights of known issues and make it hard for programmers to get entrance. The equivalent ought to be finished with switches, IoT gadgets, and other equipment and programming associated with your organization. Indeed, even a solitary purpose of disappointment as a bulb associated with an obsolete firmware variant could put your whole organization in danger. **[22]**

Portable Connection Security

Keeping gadgets associated with secure PDAs can be a test, particularly with the full number of changes happening in the business consistently. With 5G innovation increasing boundless acknowledgment, the capacity to ensure against dangers, for example, Torpedo assaults and Stingray gadgets is basic. Actualizing the security of IMSI proprietors lessens the danger to the whole association by giving total inclusion to every associated gadget, regardless of where they are associated with the organization.

Password attack

Encryption in adaptable learning is one of the noteworthy issues with respect to the endorsement of encryption which is a key factor in protecting compact picking up from external effects. Mystery key attacks are comparatively as the name construes, an untouchable endeavoring to enter the mystery key erroneously and endeavoring to get to and use a versatile learning framework in the off base way. A particular kind of system can't hinder this sort of attack **[23].**

Mystery state attacks appear generally with Dictionary Attack. Attacker uses an overview of words in word reference attacks completely expecting the customer's mystery key being the most extensively used enunciation. For passwords reliant on a singular stipulation, the word reference attack is dynamic. Glossaries are not confined to English words; they also contain ordinary passwords. Regardless, current structures shield their customers from getting to certain principal passwords, convincing customers to make complex passwords that can't be recorded. **[24]**

Used gadget (Hydra): - Hydra is a simultaneous saltine wafer that considers attack by various shows. Quick and adaptable, and easy to add to new modules. This methodology empowers analysts and security pros to explain that it is so normal to remotely get to unapproved permission to a device. It supports various courses of action including HTTPS.

Preventive Measures

1. Slow down repeated login: That's the least requesting way to deal with challenge. The end customer will doubtlessly not notice a 0.1 second delay when marking in, anyway that concede will augment immediately for the aggressor, especially in case they can't advance similar endeavors.
2. passwords. Any working structure licenses customers to reset passwords predictably, or even at standard spans. The reason behind this is it will require some investment for an assailant to emphatically attack a many-sided mystery word in order to succeed. If the mystery expression changes after some time, by then the aggressor must restart. **[25]**

Acquisitions and Diminishes

1. Force manual human test after various failed login: While the customer could without a very remarkable stretch neglect which mystery word he used for the record, this will help impede the aggressor. This is a phenomenal technique to thwart as present day manual human test is difficult to overcome PCs. Various manual human tests require manual commitment to be settled.
2. Lock Accounts: Ideally, after a particular proportion of login attempt, the mechanical assembly can be set to jolt the record. Various destinations cause more prominent security for customers with reiterated attempts at weak passwords.
3. Monitor for characteristics: Lastly, the affiliation that screens security should screen customer speaks to issues, for instance, login from dark zones or contraptions, or duplicate login disillusionment. The Employee Security Center (SOC) can recognize these events dynamically and respond quickly by closing the record, obstructing the IP address, talking with the customer, and searching for various activities from the assailant. **[26]**

Related Security in Android

Android is the most accessible and widely used operating system because of it being open source and the phones being cheap. There are high chances that most mobile learners are android users.

Android operating system uses a permission-based system that enables Android apps to access information about Mobile consumers, digitization, application information, and external tools. The developer must announce the permissions for the Android app. For the successful installation of the system regarding, the user must approve those permissions **[7]**. These permissions are advertisements. During installation, if the user grants permissions, the application can access resources and information at any time. It need not re- request for permissions again. Android OS is susceptible to various security attacks due to its weakness in security. Thus mobile learning applications should have very low access and be very restricted **[8]**.

SSL/Secured Socket Layer

Safe Sockets Layer (SSL) is a common security technology for creating an encrypted connexion between a server and a client — in this case a mobile app (website) and a server[8]. Most mobile learning applications will need to connect with the server. For instance, when a user will use log in method which sends a GET request for server data. This communication can undergo some form of packet tampering (Man In The Middle) and may cause leak of a lot of sensitive data[9]. Even though SSL and its successor TLS are quite secure they still have a vulnerabilities and still need to be improved.

A Look at LinkedIn Learning

LinkedIn Learning is a very popular mobile learning application. After taking over Lynda, they have grown exponentially. For mitigating these risks, they have restricted risks by reducing the info gathered on the learner and have a very strict privacy policy. Along with this, the use of technologies like OTP and Two Factor authentication the mobile learning portal is one the most secure learning applications.

Future Work

A lot of organizations and developers neglect security. As digital learning, especially mobile learning grows, it is important that organizations improve on confidentiality, availability, and integrity. Security is a burning issue, often neglected. Secure mobile learning portals areable to provide protection but it is difficult to maintain over large scale databases. Thus, more efforts need to be put in this field to ensure that e-commerce becomes more safe and accessible.

IV. CONCLUSIONS

Latest advances in mobile technologies have placed the smart networks at the frontline of malicious attacks. As observed, it draws a lot of unwelcome interest when any technology becomes popular. The trends show a sharp rise in mobile malware, as many threats are migrating to mobile devices, built for PC operating systems. Mobile learning sites are at a high risk because of negligence in security.

In this paper we presented a different kind of threats a mobile learning portal can face based on the attacker. We were evaluating the aims of the attacker and attacking tactics. Attacks like dos, phishing and so on were analysed and solutions to fix them were presented. In addition, we addressed and put forward techniques to prevent these attacks.

Mobile learning platforms continue to grow at exponential rates generating a lot of interests. As mobile learning grows, it is of utmost importance that these threats are addressed.

REFERENCES

1. *R. Power, "Design of Mobile Teaching and Learning in Higher Education: An Introduction," Handbook of Mobile Teaching and Learning, pp. 3–11, Aug. 2019.*
2. *Basak, Sujit & Wotto, Marguerite & Bélanger, Paul. (2018). E-learning, M-learning and D- learning: Conceptual definition and comparative analysis. E-Learning and Digital Media. 15. 191-216. 10.1177/2042753018785180.*
3. *J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993, 2014.*
4. *Salahdine, Fatima & Kaabouch, Naima. (2019). Social Engineering Attacks: A Survey. Future Internet. 11. 10.3390/fi11040089.*
5. *Hernandez Bejarano, Miguel & Baquero Rey, Luis & Gil, Celio. (2018). Ethical Hacking on Mobile Devices: Considerations and practical uses. International Journal of Applied Engineering Research. 13. 16637-16647.*
6. *Karim, Ahmad & Shah, Syed & Salleh, Rosli & Arif, Muhammad & Md. Noor, Rafidah & Shamshirband PhD,. (2015). Mobile Botnet Attacks – an Emerging Threat: Classification, Review and Open Issues. KSII Transactions on Internet and Information Systems. 9. 10.3837/tiis.2015.04.012.*
7. *M. S. Adagale, "A Review of Android Smart Security," International Journal Of Engineering And Computer Science, 2017.*
8. *Sowndarajan, Karthick & Binu, Sumitra. (2017). Android security issues and solutions. 686-689. 10.1109/ICIMIA.2017.7975551.*
9. *Elnaggar, Ahmed. (2015). Secure Socket Layer. 10.13140/RG.2.1.2671.3044.*
10. *M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016, doi: 10.1109/COMST.2016.2548426.*
11. *Ade Shonola, Mike Joy,(2014) "Mobile Learning Security Concerns from University Students' Perspectives" International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014), doi: 0.1109/IMCTL.2014.7011125*
12. *Adeshonola,(2015) "Security issues in E-learning and M-learning Systems: A Comparative Analysis" Doctoral Research and Innovation Conference.*
13. *Mohd Amin Mohd Yunus, Muhammad Zainulariff Brohan, Nazri Mohd Nawi, Ely Salwana MatSurin, Nurhakimah Azwani Md Najib, Chan Wei Liang,(2018) Review of SQL Injection : Problems and Prevention, INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, doi: 10.30630/joiv.2.3-2.144*
14. *Zainab S. Alwan, Manal F. Younis,(2017) Detection and Prevention of SQL Injection Attack: A Survey, International Journal of Computer Science and Mobile Computing Vol.6 Issue.8, August- 2017, pg. 5-17.*
15. *Shaimaa Khalifa Mahmoud, Marco Alfonse, Mohamed Ismail Roushdy, Abdel-Badeeh M. Salem (2017),A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques, Eighth International Conference on Intelligent Computing and Information Systems (ICICIS) doi: 10.1109/INTELCIS.2017.8260024*
16. *Sentamilselvan K, Dr.S.Lakshamana Pandian, Dr.K.Sathiyamurthy(2013), Survey on Cross Site Request Forgery, International Conference on Research and Development Prospects on Engineering and Technology March 29, 30 - 2013 Vol.5.*
17. *Anuj Kumar Baitha, Prof. Smitha Vinod (2018), Session Hijacking and Prevention Technique, International Journal of Engineering & Technology, 7 (2.6) (2018) 193-198, doi: 10.14419/ijet.v7i2.6.10566*
18. *K. Bhattacharyya, "DDoS Attacks," 2016.*

19. *S. Newman, "Under the radar: the danger of stealthy DDoS attacks," Network Security, vol. 2019, no. 2, pp. 18–19, 2019.*
20. *"DDoS Prevention," DDoS Attacks, pp. 145–159, 2016.*
21. *K. Bicakci, D. Unal, N. Ascioglu, and O. Adalier, "Mobile Authentication Secure Against Man-In-The-Middle Attacks," Procedia Computer Science, vol. 34, pp. 323–329, 2014.*
22. *Mallik, "Man-In-The-Middle-Attack: Understanding In Simple Words," Cyberspace: Jurnal Pendidikan Teknologi Informasi, vol. 2, no. 2, p. 109, 2019.*
23. *P. Jourdan and E. Stavrou, "Towards Designing Advanced Password Cracking Toolkits," Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization - UMAP19 Adjunct, 2019.*
24. *L. Bosnjak, J. Sres, and B. Brumen, "Brute-force and dictionary attack on hashed real- world passwords," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018.*
25. *Thriveni and K. Madhavi, "A Secure Authentication Scheme against password Guessing Attacks," International Journal of Computer Sciences and Engineering, vol. 6, no. 6, pp. 162–166, 2018.*
26. *T. Kwon and J. Song, "Efficient and secure password-based authentication protocols against guessing attacks," Computer Communications, vol. 21, no. 9, pp. 853–861, 1998.*