**CHAPTER TWO: LITERATURE REVIEW**

**2.0 Introduction**

The technologies embraced in the development of this project are discussed in this chapter. Related works are also reviewed and analyzed in the later section of this chapter.

**2.1 Theoretical Background**

In this chapter, we will look into the technologies related to password management and introduce the technologies used in development process. We also elaborate more on the literature review of other research done in this field and also compare it with current ones to effectively see similarities, contrasts and improvements so far.

The major technologies used in this project are web related technologies such as PHP and relational database technology such as MySQL. With PHP as the frontend and MySQL as the backend database. PHP (Hypertext Preprocessor) is a widely used open source general purpose scripting language that is especially suited for web development and can be embedded into HTML (Hypertext Markup Language) SQL (Structural programming Language) server provides database to store information on remote location. The system can be accessed using a username and password by the user and the saved details cannot be seen or used by the manager of the system.

The basic functionalities of this system are that user can be able to create, save, and delete username and password on this platform. This security system has also a way to make user not to forget the login details of this system by using OTP (0ne time password) for logging in. password managers always face a challenge, which is phishing that happens through extensions built on other browser password management system but this system is developed without an extension, it serves as a password bank.

**2.2 Literature Review**

This section explores the different web password management systems previously developed by companies or proposed in publications.

Morris and Thompson pointed out long ago in 1979 that weak passwords

Suffer from brute-force and dictionary attacks [6], this passwords are called weak in the sense that the user uses simple and easy to remember words such as user first name, last name or words in the dictionary as password which the attacker can easily get by running very large set of words to generate potential passwords. . Later, Feldmeier and Karn Further emphasized that increasing password entropy is critical to improving Password security [7].

However, strong passwords that is sufficiently long, Random, and hard to crack by attackers are often difficult to remember by Users due to human memory limitations. Adams and Sasse discussed pass- word memorability and other usability issues and emphasized the importance

of user-centered design in security mechanisms [8].

Web Wallet [9] is an anti-phishing solution and is also a password manager that can help users fill login forms using stored information; however, as pointed out by

the authors, users have a strong tendency to use traditional Web forms for

typing sensitive information instead of using a special browser sidebar user

interface.

In addition, Web Wallet is not cloud-based, which means the user information are saved in the local machine. In [10] the authors have proposed user-centric trust Identity service with an aim to create trust among Cloud

Service Providers (CSP). Their model has Authentication, Authorization, and Provisioning and Audit modules along with the Trust agent. The federated environment will allow users to login to various Cloud Service Providers

depending on the application access. When the user moves to different CSP the user credentials follow in the federated environment. The Trust Agent in the Identity Management sends the Trust Token along with the user attribute which creates a trust between CSPs.

In [11] the authors have propose an Identity and Access Management architecture in cloud to achieve security requirement like Strong Authentication, Data Loss Prevention, Security as a Service. The various systems components for addressing the above security requirements are Cloud Resource provider, Identity Management, Policy Management, Resource Engine and Access Decision-making. The various advantages of their approach were Comprehensive identity management, standardized architecture, and scalable design.

Information security can be defined as protecting information with regard to three main requirements: confidentiality, integrity, and availability. Confidentiality meaning that unauthorized parties are not allowed to intercept the information. Integrity meaning that the information has not been corrupted or changed during storage or transmission by unauthorized parties. Availability meaning that information is available to the authorized parties when trying to access it. This model is often referred to as the CIA triad. Modern business needs have also increased the need for non-repudiation which means that an action, e.g. a business transaction, cannot be denied afterwards [12]. Some has criticized the model of not including enough principles to ensure the information security of an organization. Dhillon and Backhouse proposed already in 2000 that the principles of responsibility, integrity (integrity of a person and not only information), trust and ethicality could be added to the model [13]. Another study proposes that authentication, access control, and non-repudiation should be added to the model [14]. Even though the CIA triad may not present the whole picture when it comes to information security there is consensus in the scientific community that confidentiality, integrity, and availability are key concepts in ensuring the security of information [13],[10] [17].

**Reference**

[6] R. Morris, K. Thompson, Password security: a case history, Commun.

ACM 22 (11) (1979) 594–597.

[7] D. C. Feldmeier, P. R. Karn, Unix password security – ten years later,

in: Proceedings of the Annual International Cryptology Conference

(CRYPTO), 1989, pp. 44–63.

[8] A. Adams, M. A. Sasse, Users are not the enemy, Commun. ACM 42 (12)

(1999) 40–46.

[9] M. Wu, R. C. Miller, G. Little, Web wallet: preventing phishing at-

tacks by revealing user intentions, in: Proceedings of the Symposium on

Usable Privacy and Security (SOUPS), 2006, pp. 102–113.

[10]. Samlinson, E.; Usha, M., "User-centric trust based identity as a service for federated cloud environment," in Computing, Communications and

Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1-5, 4-6 July 2013

[11]. Yan Yang; Xingyuan Chen; Guangxia Wang; Lifeng Cao, "An Identity and Access Management Architecture in Cloud," in Computational

Intelligence and Design (ISCID), 2014 Seventh International Symposium on, vol.2, no., pp.200-203, 13-14 Dec. 2014

[12] Rui Zhao and Chuan Yue, Toward A Secure and Usable Cloud-based Password

Manager for Web Browsers, 2014, pp11-15

[13] Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. The Data Base for Advances in Information Systems, 38(1), 60-80.

[14] Dhillon, G., & Backhouse, J. (2000). Information System Security Management in the New Millenium. Communications of the ACM, 43(7), 125-128.

[15] Simmonds, A., Sandilands, P., & Ekert, L. (2004). An Ontology for Network Security Attacks. Proceedings of the Second Asian Applied Computing Conference (AACC), (pp. 317-323). Kathmandu, Nepal.

[16] Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. The Data Base for Advances in Information Systems, 38(1), 60-80.

[17] Hilton, J., & Cherdantseva, Y. (2013). A Reference Model of Information Assurance & Security. Eighth International Conference on Availability, Reliability and Security (ARES) (pp. 546-555). Regensburg: IEEE.