


<b>LEARNING MODULE</b>	 <p><b>PAMANTASAN NG LUNGSOD NG MUNTINLUPA</b>  <b>COLLEGE OF INFORMATION TECHNOLOGY AND  COMPUTER STUDIES</b></p> <p>University Road, Poblacion, Muntinlupa City</p>					
<i>QD/CITCS/0__</i>	<b>Course Title: Systems Analysis and Design</b>					
<i>Issue No.</i>	0	<i>Revision No.</i>	0	<i>Effectivity Date</i>	07 September 2020	<i>Page No.</i> <span style="float: right;"><i>1 of 1</i></span>

## **TOPIC PROPOSAL FORMAT**

**Project Team Leader:** 1. Faderanga Janrey Cyril

Team Member(s): 2. Pangilinan Kyrah

3. Santarin Mary Grace

### **Project Proposal 1:**

Personalized Web-based System for Secure Storage Account Authentications

### **Areas of Investigation:**

The purpose of this proposed topic is to explore the development and implementation of a personalized web-based system for securely storing account authentication credentials. This system aims to provide users with a centralized and secure platform to manage their various account credentials, enhancing convenience while maintaining robust security measures.

### **Purpose and Description of the Proposed Topic:**

The main topic revolves around the design, development, and implementation of a personalized web-based system that offers users a secure repository for storing and managing their account authentication credentials such as username and Password. This system will incorporate features such as encryption, multi-factor authentication, and user-specific customization to ensure the highest level of security and usability.

### **Main Problem:**

The main problem addressed by this topic is the vulnerability of traditional methods of storing account authentication credentials, such as writing them down or using easily guessable passwords. These methods pose significant security risks, including unauthorized access to accounts and potential data breaches.

### **Causes of the Problem:**

A. Lack of awareness about secure password management practices.

- B. Human tendencies to use weak passwords or reuse them across multiple accounts.
- C. Inadequate solutions for securely storing and managing authentication credentials.

### **Effects of the Problem:**

- A. Increased susceptibility to cyber-attacks, including phishing, brute force attacks, and credential stuffing.
- B. Compromised personal and sensitive information.
- C. Potential financial losses and damage to reputation due to unauthorized access to accounts.

### **Target Users/ Beneficiaries:**

Individuals who regularly use online services and need a secure method to manage their account credentials and any entity or individual concerned about the security and privacy of their online accounts.

### **Related Studies/ Projects:**

- [1] P Mell, T Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory, October 7, 2009. <http://www.nist.gov/itl/cloud/>
- [2] MA Sharkh, M Jammal, A Shami, A Ouda, Resource allocation in a network-based cloud computing environment: design challenges. *IEEE Communications Magazine* **51**(11), 46–52 (2013)
- [3] C Wang, Q Wang, K Ren, W Lou, Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers* **62**(2), 1–12 (2013)
- [4] T Paigude, TA Chavan, A survey on privacy preserving public auditing for data storage security. *International Journal of Computer Trends and Technology (IJCTT)* **4**(3), 412–418 (2013)
- [5] Ristic, I. (2014) SHA-1 Depreciation: What you need to know(online),<https://community.qualys.com/blogs/securitylabs/2014/09/09/sha1-deprecation-what-you-need-to-know>
- [6] Beattie, D. (2014) Everything you need to know about the move to SHA-1 (online), <https://www.globalsign.com/en/blog/everything-youneed-to-know-about-the-move-to-sha-256/>
- [7] Strahs, B., Yue, C., Wang, H. (2009) Secure Passwords Through Enhanced Hashing. *Proceedings of the 23rd conference on Large installation system administration, LISA'09*, Baltimore, USA, Nov 1-6th 2009, pp: 7-14.
- [8] Jain, A. (2005) Biometrics: Personal Identification in Networked Society (online), <http://www.kennys.ie/biometrics-15.html>
- [9] Tang, Y., Huang, D., Wang, Y. (2012) ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System, *21st International Conference on Pattern Recognition (ICPR)*, Tsukuba, Japan, pp: 45-54, 11-15 Nov 2012
- [10] Dubin, J. (2007) Complex password compliance requirements made simple (online), <http://searchsecurity.techtarget.com/tip/Complexpassword-compliance-requirements-made-simple>
- [11] Ksiazak, P., Farrelly, W. & Curran, K. (2015) *Journal of Information Security and Privacy*, Vol. 8, No. 4, pp: 62102, October 2015, DOI: 10.4018/IJISP.2014100104
- [12] Choi Y, Lee Y, Moon J, Won D (2017) Security enhanced multi-factor biometric authentication scheme using bio-hash function. *PLoS ONE* **12**(5): e0176250. [nhttps://doi.org/10.1371/journal.pone.0176250](https://doi.org/10.1371/journal.pone.0176250)

[13] Jensen, B. (2015) 5 Myths of Password Security (online),<https://stormpath.com/blog/5-myths-passwordsecurity/>

[14] Prince, M. (2012) The Four Critical Security Flaws that Resulted in Last Friday's Hack. Cloudflare, April 11 2016, <https://blog.cloudflare.com/the-four-criticalsecurity-flaws-that-resulted/>

[15] Rizzo, T. (2013) The Most Recent Password Security Compliance Guidelines <http://insights.scorpionsoft.com/bid/329695/The-MostRecent-Password-SecurityCompliance-Guidelines>

Approved by:

***Asst. Prof. Maria Victoria G. Solatorio***

*Course Instructor Name*