**Abstract:**

This research paper is on the design of the advanced and multifunctional Universal Password Manager based on the Android platform, whose ultimate goal is to reinforce the password strength, promote user experiences and decrease the risk of the hacking private information. In today’s network environment, there are various shopping, application and forum websites which require users to register different accounts to become their memberships to enjoy the exclusive discounts and high-quality service. However, from the questionnaire, we deduced that since people’s memory is limited, most people selected the uniform password when signing up. It is no doubt that the behaviour and psychology are utilised by some hackers. Once they obtain the password of a person in a forum website, then his personal information and bank accounts are exposed. In addition, from the questionnaire, some people claimed that they ever used some over-simple passwords, such as ‘123456’, ‘abcdef’ and ‘qwerty’. Hence, we designed the app to store users’ complicated and multiple passwords and generate a random password with high strength for users’ reference. We believe our app will provide people with plenty of convenient on the aspects of password and cybersecurity.

**Introduction:**

There is a new conceptual word named ‘Hit the library’ on the Internet, which refers to the phenomenon that hackers try to log in to other websites and gain a series of available accounts through collecting the leaked user name and corresponding password information on the Internet. A large number of users in different sites using the same account password, so hackers can access the users’ accounts in the A site to try to log in the B site \cite{gasti2012security}.

In order to acquire the actual data, we generate a questionnaire on the Surverymonkey.com. Shown in diagrams are the result of the survey, 57.14% participants admit that they ever set over-simple passwords. Meanwhile, it showed the incredible proportion of participants who set the same passwords for some websites, which reaches 88.57%, and among them, the reason primarily is that different and various passwords are difficult to memorise \cite{questionnaire}. Also, 80% participants are willing to utilise the password manager app to manage passwords \cite{questionnaire}. Li et al. \cite{li2014emperor} also indicated that users expect that password manager could reduce their memory fatigue.

Therefore, we built the app and expected it to improve the bad behaviour of users when signing in. The app contains four core functions, including access with biometrics, passwords storage, strong password generation and cloud services. We absorbed the experience of similar apps in the market and aimed at making functions interact with user experience and entertainment. In addition, we interviewed three users and collected feedbacks on this app from them.