ENHANCING PASSWORD AUTHENTICATION USING ASSOCIATION PASSWORD TECHNIQUE: AN ECOLOGICAL THEORY OF MEMORY AND DATA

Raymond Commodore, IT Unit, Presbyterian University College Ghana, Okwahu Campus, r.commodore@presbyuniversity.edu.gh / raymond.commodore@gmial.com

Prof. J. B. Hayfron-Acquah (PhD), Department Of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, jbha@yahoo.com

ABSTRACT

The Study proposes possible solution to enhance Password Authentication using Association Technique based on the Ecological theory of memory and data at the Presbyterian university College Ghana. The study used a deductive research approach and employed two empirical Studies using the non-probability sampling technique where few respondents were selected in categories out of the populace by means of openness in other to get similar categories of respondents with different age groups and education background. The two Empirical study also used a quasi-experimental approach which structure incorporate observation, experimental treatment and timing. The First empirical study carried out an investigation to identify existing Password authentication Technique used by End Users, as well as their behavior in password utilization through a self-completed questionnaires which was analyzed using SPSS version 21 . The Second empirical study was an experiment to compared three kinds of password constructions that is own set, modified dictionary, and association against one another to see which of them would be best meet the ecological theory of memory and data which aims at creating a secured password that is easy to recall. The computation and evaluation of password construction was done using My1login Password meter whiles Levenshtein Distance String Edit Software was also used to compute the memorability of all given password. Across-tabulation was then employed out of the experiment using SPSS version 21. The result from the analysis revealed that the majority of the respondents do have weak passwords and also have few passwords which they even end up sharing with families and friends and reuse it. This confirms statements made by researchers that human being is the weakest connection in information system securities. To maintain Confidentiality, Availability and Integrity of data, the study therefore recommended the use of the Association Password technique which makes it easier to develop a much secured password that is difficult to crack but easy remember.

Keywords

Authentication, Password Authentication, Password Strength, Password Memorability, Association Password Technique, Computer Security.

1. Introduction

One of the basic components of any information security system is the control of people in or out of guaranteed regions. Authentication is the route toward affirming that the individual requesting a resource is the individual who he claims to be. The greater part of the authentication systems nowadays utilizes a blend of a username and password for confirmation. Computer security systems should likewise consider human factors, for example, convenience and openness. Current secure information systems endure in light of the fact that they generally disregard the significance of human factors in security.

Generally, alphanumeric passwords are being utilized for authentication and are known to have security and convenience issues. Vaz and et al. (2017), says a computer Information security systems ought to likewise consider the human issues, for example, effortlessness of utilization and openness

 doi:10.20944/preprints202008.0268.v1

and that, current security systems endure in light of the fact that we generally disregard the significance of some social and human factors in security. They further said that a password is a mystery that is shared by the verifier and the client. "A secret password is a private key that is shared by the verifier and the End user. "Passwords are just a private key that is given by the End-User upon solicitation by a recipient." These passwords are regularly put away on a server in an encrypted format with the goal that a penetration of the system does not uncover password records.

Passwords mostly used for authentication purpose because they do not need special hardware. Usually, passwords are strings of numbers, and letters that are alphanumeric characters and such passwords come with some disadvantage of being hard to remember. About the security and usability problem associated with alphanumeric passwords as the password problem. A graphical password Authentication was an introduction to replace the alphanumeric passwords.

Therefore, this study sought to assess and enhance the Password authentication security measure that exists in Presbyterian University College, Ghana before the study.

In accessing that weak password are often cited as one of the most severe threat to an information system, they are defenseless to dictionary and brute force attack due to fact that: End Users regularly use fragile passwords that are short, straightforward based on individual and significant information which can be effectively speculated.;There is also a consistently growing amount of Users accounts and passwords, this make it difficult for End Users to recall and mastermind it.;End Users also tend to pick simple to recollect and weak passwords. Some also go to the extent of writing down the passwords in the diary, phones etc. the Study examined End users' conduct in password creation and application as well as explored and addressed some passwords vulnerability, best practices for password syntax used by both Staff and Students of Presbyterian University College Ghana, security and policies.

Due to that, the Main goal of the study is to assess and enhance password authentication security measures used. To achieve that, the following specific objectives were understudy. The study Investigated existing Password authentication Security Methods (Technique) used by End Users; It also investigated End Users behavior in password utilization. (Storing and memorability); As well as evaluation of the Passwords Security Syntax Used by End Users and also proposed possible solution for the Password Security issues at the Presbyterian university College Ghana.

2. Authentication

The section presented a review on relevant literature such as Authentication, Password policy standards, Memorability of Passwords and other works done.

A research conducted by Kumar and Bilandi (2014) indicated that an authentication system should energize vigorous passwords while keeping up the ease of use and memorability. According to Gordon (2017) there are three authentication mechanisms, which is something you know, something you have, and something you are. Authentication techniques square measure comprehensively characterized into three principle areas. Token-based Authentication which is commonly known as two-factor authentication, Biometric based Authentication which is also known as three-factor authentication and a Knowledge-based Authentication which is a single factor authentication. The table explains the above statements.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

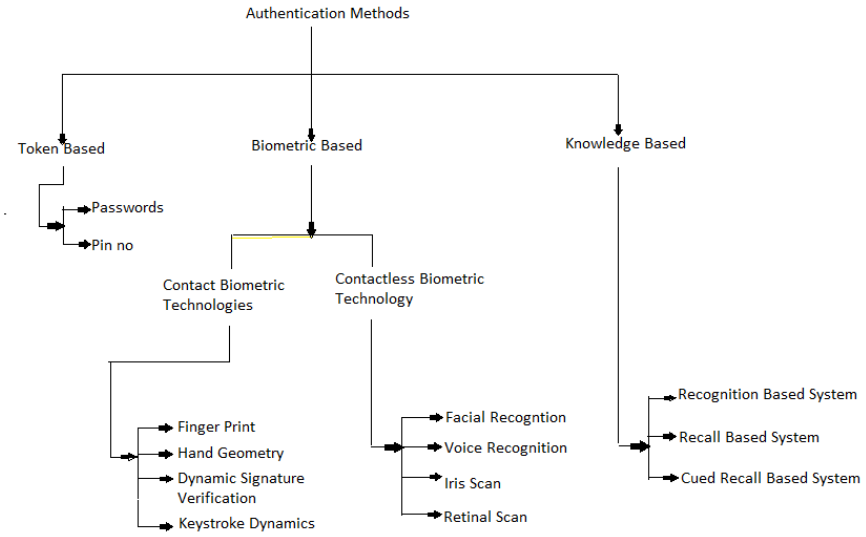


Fig. 2.1 Three Authentication Mechanisms

2.1 Password Authentication

Despite the fact that there are numerous types of authentication techniques by, for example, biometric and smartcard, the most widely recognized technique for validation and verification is the permutation of the End User ID and password for authentication. Sasse et al. (2001) express the two stages of the authentication procedure utilizing passwords which will be depicted in the accompanying area. First, users are given a chance to create an ID or either assigned new Identification. As soon as the Identification has been created, the user selects a password. The password should be undisclosed and shared only between the user and the information systems or computer.

Secondly, Through the login procedure, End users must input both their user Identifications text and passwords. It then processes, compares and analyses the Users Identification and password entered with what has been stored in the database. Should it be similar, the user is then granted permission to have access to his or her system. If not, the user will not be able to access it. A lot of information digital entities suspend unsuccessful user account once there are three to five attempts to log in. Should a user be suspended, he or she must contact the system administrator to reset his or her password.

According to Schneier (2000), for some time now, passwords are stored in a cryptographic hash format instead of storing in a file, with such; the system computes the hash value of the passwords and compares it with the stored hash one in the file, the user is then allowed if they match. However, if a hacker has acquired a copy of the hashed password file, the hacker can use a dictionary to calculate the hash of every word in the dictionary. then the hacker may obtain the password should the hashed password matches with the one in the database, if he tries all the words in a dictionary and fails, he or she will then guess using the reverse dictionary words, as well as capitalizing letters, and try all character combinations.

Sans Institute developed a password policy that checks the strength and weakness of a password. The policy shows the characteristics of a weak and a strong passwords and other related attributes of Password. In it Brunett (2012) indicates that a good and a strong password should be difficult to crack but must be easy to recall.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

2.8. Theoritical Framework of Password Management

Burnett and Kleiman (2006) in their article reveal three theories on how to strengthen a password which a the rule of complexity, the rule of uniqueness and the rule of security as shown in figure 2.4

Figure 12.4 Theory on how to strengthen a Password

In the rule of complexity, Burnett and Kleiman (2006) explain that a complex password should contain three elements that is characters, letters, numbers, and words or phrases. The complexity number should not be the first or last character in the password and should contain at least 50% of numbers. This explain the theory for keeping data safe.

Secondly, in the rule of uniqueness, Burnett and Kleiman (2006) explain that a password should be unique for every system where it is used and distinct among passwords. Theerefore End users must avoid common words, dictionary words, names or numbers related to them as well as changing their password at least every three to six months to continue keeping a unique password.

Thirdly, in the rule of security, they explain that password must not be shared with anyone or saved on web browser in other to keep the password and maintain data confidentiality. They further advice End Users to always change their password that is automatically assigned to them by an administrator.

2.2 Memorability of Password

Sasse et al. (2001) in their submissions note the following that:The human memory is constrained; Human memory can rot after some time; Frequently utilized passwords are simpler to retain than less normally utilized passwords; Humans can't "overlook on interest," which shows that a few things (passwords) are still in memory despite the fact that they are not required; Meaningful passwords are more available to recall than non-significant passwords and Different things can be identified with each other to help review. Regardless, related or comparable issues can rival each other for memory.

Adams and Sasse (1999) found that Users' with few passwords influences the passwords' memorizability. At the point when users are dispensed a cryptographically hearty password like "*33j? ^4CDa", they will overlook it; accordingly, they will in general record it (Warkentin, Davis, and Bekkering, 2004). Likewise, presently, end Users must recollect such a large number of passwords. The development of internet business has brought about a monstrous increment in the number of passwords required by end Users (Ives et al., 2004).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

Higbee(2001) indicated the three phase of memory which is Acqusition, Storage and Retrieval. In the acquisition or encoding is learning or examining the material. On account of passwords, the securing procedure happens when the user develop the passwords, or they are allocated to the User in any case; Storage is keeping the material until it is required. It is the means by which the information is kept up in memory (Anderson, 1994,). On account of passwords, the capacity procedure happens when the User remember the passwords; and Retrieval is distinguishing the material and getting it to pull out when it is required. On account of passwords, the recovery procedure happens when the User reviews the passwords.

He then indicated that there are two classification of the memory which is the short term Memory and the Long term memory. Short-term memory alludes to "how a few things are regularly seen at just once or what extent an individual will deliberately accumulate to on the double." That recommends that once an individual secures his or her password, the rotting procedure is as of now happening (Higbee, 2001).

The long term also alludes to how allows to how one retains how to accomplish something- Procedural memory; how one recalls true information- Semantic memory and how one recalls individual occasions – Episodic memory. (Higbee, 2001). These show the three sorts of long term memory. (Higbee, 2001).

The diagram Fig. depicts how memory functions and the connection between short haul and long haul memory dependent on Atkinson and Shiffrin's hypothesis:

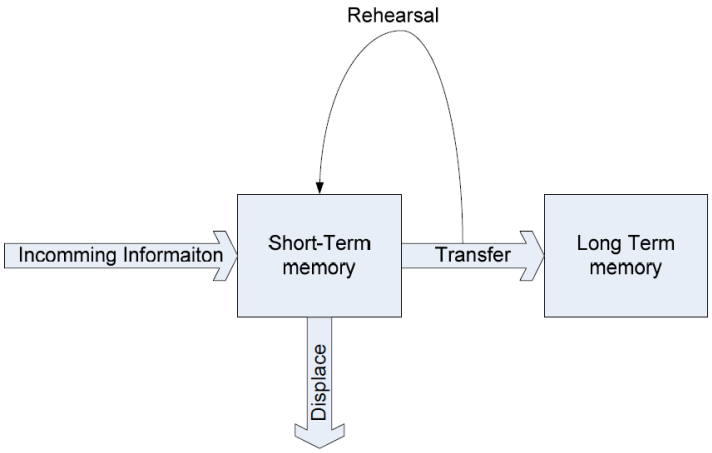


Fig. 2.2 Atkinson and Shiffrin's hypothesis on memory

Higbee (2001) in his submissions reveals some reasons why people forget their passwords which include: Distortion, interferences, Decay etc. and Basic foundation of Memorization such as Meaningfulness, Familiarity, and Rhymes etc. it further indicated the seven necessary Foundation of memorization which also includes; Meaningfulness; Familiarity and Mere Exposure; Rhymes; Patterns; organization, Association; and Repetition

Ecological Theory of Memory and Data

Gao, Yang et all (2018) in their submissions stated the ecological theory on memory and data which derive quantitative perdition for recall odds and retrieval time. The model assumes that the higher the activation, the more accessible a memory representation of password is. The activation is related to the historical use of this memory element and contextual associations related to the memory recall. (Gao, Yang et all, 2018). Miller (1956) shows that human transient memory can store just seven give or take two (7 2) lumps or measures of information. Be that as it may, this standard applies to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

information that must be recalled without practice (Hewett, 1999). Information can be retained for an all-encompassing period in the event that it is practiced (Hewett, 1999; Newell and Simon, 1972).

3. Methodology

The study employed two empirical studies which is a self-completed and experimental questionnaire. The First phase of the study therefore used a quasi-experiment approach (ie. Observation, Experiment, Timing) as shown in Figure 3.1.

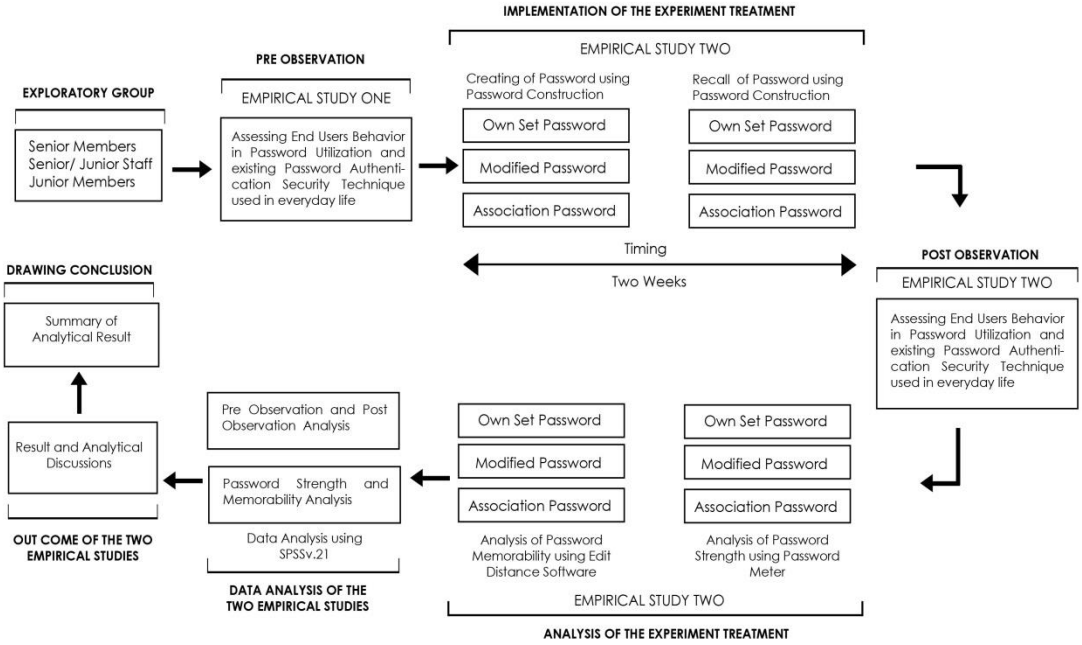


Figure 3.2 quasi-experiment approach in relation to the study

The study employed IBM's Statistical Package for Social Scientist (SPSS) version 21 to analyze data collected from the five campuses of the Presbyterian University College, Ghana using the convenience sampling technique. 28 questions comprising of four parts was administered to 90 Respondents which includes 30 Senior Member, 30 Senior /Junior Staff and 30 Junior member from different Faculty and departments of the University. The analysis was based on descriptive and Statistical analysis.

The second phase of the study used an experimental research approach and the tools employed for the simulation were My1login Password meter which was used to compute and evaluate the strength of a given password in milliseconds to billions of years, Levenshtein Distance String Edit Software which was also used to calculate the memorability of the given password. A Across-tabulation was then employed out of the experiment using IBM's Statistical Package for Social Scientist (SPSS) version 21.

In the experiment, Respondents created three different passwords using different password construction technique. The First password technique which is the own set password was to understand how End users create their passwords in everyday life; the second password construction which is the Modified Password was inspired by Sasse, Brostoff and Weirich (2001) with these, password created for the first passwords construction are modified by changing some of the letters to particular characters and number. The last Password Construction which is the Association password

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

Technique help Respondents in creating a memorable sentence of an event that took place with dates attached and this sentence was then used to create a password using the first letter of every world and last two numbers of every date with some special character which made it much easier to remember. This technique was inspired by Yan, Blackwell, Anderson and Grant (2004) based on association.

4. Result and Discussion

4.1 Existing Password authentication Security Method used by End Users

Finding from the survey one proves that; Almost all of the respondents avoid the use of special characters in their since it will be difficult for them to type or remember. Burnett and Kleiman (2006), in their submission made it clear that using special characters in password creation can decrease the danger of being hacked and also be a target for a dictionary attack. It was also realized that most of the Respondent don't change their password frequently whiles others wait for the system to prompt them before they do change the passwords. Burnett and Kleiman (2006), makes it clear in their article that a password must be changed regularly and at least every six months avoid hackers from getting into information system.

4.2 End Users Behavior in Password Utilization

A number of the respondents utilize a strong password in their everyday life. It also appears that most of them store their passwords in memory due to the use of the same passwords for different account. Some also go to the extent of writing down their passwords in books and electronic devices whiles others sharing their passwords with friends and families since they might forget. In the second follow up survey also proves that the result of how the how the respondents could remember a given password was based on the measurement of the memory. After the experiment, we realized that the first password construction (Own set Password) was one the second passwords highest memory ratio because most of the respondents create their own passwords that are related to their capacity and knew how they could remember them. Most of the respondents forgot their passwords in the second password construction due to some criteria used in that given construction which may be a factor (Sasse, Brostoff & Weirich 2001).

In the other hand, only a limited number of the respondents use extraordinary characters in their everyday password creation which may also be a motive why they easily forget their passwords. According to Burnett and Kleiman (2006), a good password ought to be a password that is difficult to crack, simple to type and easy to remember. Using special characters in a password would increase the strength of it. Bryman and Bell (2015) stated that another reason affecting this experiment can be the respondents educational and Information technology Knowledge. Each respondent has a different background of studies and kind of knowledge and experiences regarding the creation of passwords and its securities.

4.3 Evaluation of Password Security Syntax Used by End Users

Table 4.1: Cross tabulation Password construction

Password Construction	100% Remembered	Partial Remembered	Chi-Square	Minimum Expected

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1

	Strong	Weak	Strong	Weak	Sig. Value	Count.
Own Set Password	18.9%	32.2%	24.45%	24.45%	1.558[a]	19.07
Modified Password	23.3%	13.3%	37.8%	25.6%	0.140[a]	12.83
Association Password	60.0%	6.7%	31.1%	2.2%	0.74[a]	2.67

Source : Extract from SPSS cross Table Analysis, 2019

4.3.1 Own Set Password (Password Construction 1)

In the first password construction, the significance was 21, 1% which implies that there was 21, 1% shot of contrast. As per Norusis (2008), the significance must be a limit of 5% powerlessness not to be a coincidence. On account of the main table, the significance was high which implies that there is a no association between the password strength and the memorability from the first password construction. Be that as it may, should the significance not to be there, it shows an inclination to the pattern which can be found in the cross tabulation. The more fragile and more grounded passwords don't have an equivalent measure of respondents recalling them to 100%, that implies, the own set passwords don't influence the memory related with what strength the password has.

4.3.2 Modified Password (Password Construction 2)

In the second password construction cross-tabulation, the significance is 70, 8 % which implies that the modified password, has a high coincidence. The possibility has an excessively incredible of an effect in the modified password construction for it to have an association in SPSS. While breaking down the cross tabulation in Table 4.3, the majority of the Respondents was not able to recollect their passwords created, both weaker password and stronger password.

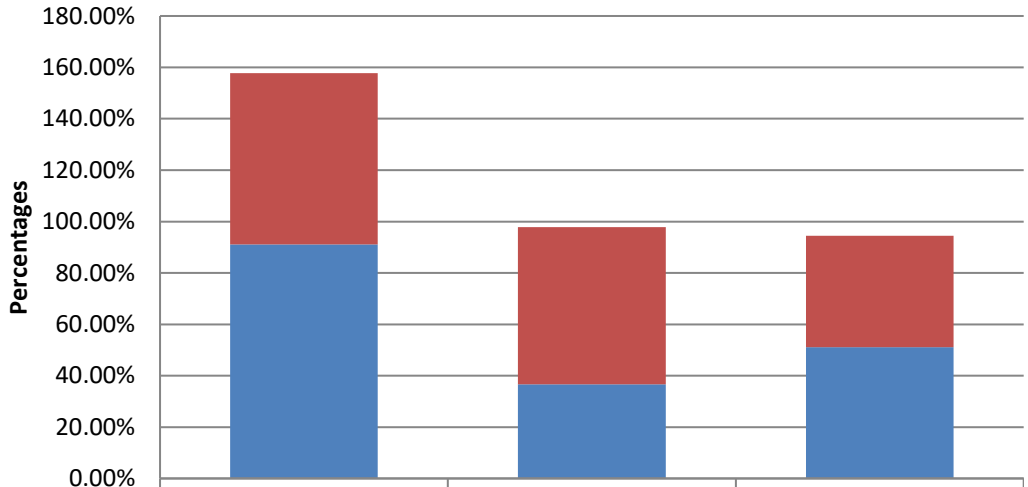
4.3.3 Association Password (Password Construction 3)

The Association Password construction is different from the other two password constructions, the own set, and the modified password. These imply that there was a superior number in the significance. The significance in this password construction was 59, 2% which makes the likelihood for it to be an opportunity just 59, 2%. As per Norusis (2008), the significance must be 5%, yet in this, moderately think about, is 59, 2% significance a great number, despite the fact that it isn't ideal. In the cross tabulation in Table 4.5, the measure of the respondents who recall their password to 100% was not the same as while making a weak and strong password. Of the respondents who did not recall their passwords completely, which was 31.1 % created a strong password.

4.3.4 Password Strength and Memorability Analysis

To discovery which password construction was superlative, both the Password strength memory were analyzed together. Figure 4.17 Shows that Association Password is the best passwords because it has the highest strength of Password (91.10%) and the majority of passwords were remembered (66.70%) as compared to other password constructions. Modified Password construction also shows that 36.70% of its password was recorded as strong and 61.10% was being remembered. Lastly, the own set password recorded 51.10% as strong, and 43.30% of its passwords were also remembered.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 August 2020 doi:10.20944/preprints202008.0268.v1



	Association Password	Modified Password	Own Password
Memorability	66.70%	61.10%	43.30%
Strength	91.10%	36.70%	51.10%

Figure 4. 1 Password Strength and Memorability Analysis

5. Conclusions

The research was to investigate existing Password authentication security methods used by Individual and End users' behavior in password utilization and evaluate the Password Security used by those individuals. Lastly, to also recommending possible solutions to strengthen the Password authentication Security used of which this experiment has been able to analyze and improvement made through a seminar on how to create a good password that is strong, simple and able to remember and typed on a computer to prevent hackers from intruding into our accounts. At the end of the experiment, three password construction used, that is, own set password (construction 1), Modified Password (construction 2) and Association Password (construction 2) the own password recorded the second highest memory ratio; the modified password recorded the weakest memory rate but the strong password. And lastly, the Association password recorded the strongest password construction as well as the highest memory rate.

We also conclude that the majority of the respondents do have weak passwords which confirm statements made by researchers that Human being is the weakest connection in information system securities. This conclusion was also based on philosophies about passwords authentication securities. From our first survey. Again it was noted that majority of the respondents have few passwords which they even end up sharing with families and friends and reuse it. Once creating a password, the strength and memorability of the password must be taken into consideration to have a safe and straightforward password to remember. Therefore, passwords strength and memorability is an essential vital for safe and good password creation.

6. Acknowledgements

Many thanks to Staff and Students of the Presbyterian University College, Ghana and to my supervisor who played a key role in supervising this thesis.

7. REFERENCES

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Association for Computing Machinery. Communications of the ACM, 42(12), 40 (47 pages)
- Anderson, J. R. (1994). Learning and Memory: An Integrated Approach: John Wiley & Sons Inc.
- Bryman, A. & Bell, E. (2015). *Business research methods.* 4.th edn., Oxford: Oxford University.
- Burnett, M. & Kleiman, D. (2006). *Perfect passwords: selection, protection, authentication, Syngress*. Rockland: Mass.
- Gordon, J. C., Keskin, C., & Betser, M. (2017). *U.S. Patent Application No. 15/169,359*.
- Higbee, K. L. (2001). Your Memory: How It Works & How To Improve It (2 ed.). New York NY: Marlowe & Company.
- Ives, B., Walsh, K. R., & Schneider, H. (2004). The Domino Effect of Password Reuse. Association for Computing Machinery. Communications of the ACM, 47(4).
- Kumar, E. A., & Bilandi, E. N. (2014). A graphical password-based authentication based system for mobile devices. *International Journal of Computer Science and Mobile Computing*, *3*(4), 744-754.
- Norusis, M. (2008). *SPSS Statistics 17.0 Guide to Data Analysis*. Chicago: Prentice Hall Inc.
- Sans.org. (2013). Password Policy: www.sans.org
- Sasse, M A., Brostoff, S. & Weirich, D. (2001*).* Transforming the 'Weakest Link': *a Human/Computer Interaction Approach to Usable and Effective Security*. BT Technology Journal, pp. 122-131. DOI: 10.1023/A:1011902718709
- Schneier, B. (2000). Secrets and Lies. New York: John Wiley and Sons.
- Vaz, C. S., Fernendes, S., Sardinha, R., & Student, P. G. (2017). Authentication Technique for Security using Ensemble Graphical Password. *International Journal of Engineering Science*, *10992*.
- Warkentin, M., Davis, K., & Bekkering, E. (200 4). Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security. Journal of Organizational and End User Computing, 16(3), 41 (18 pages).