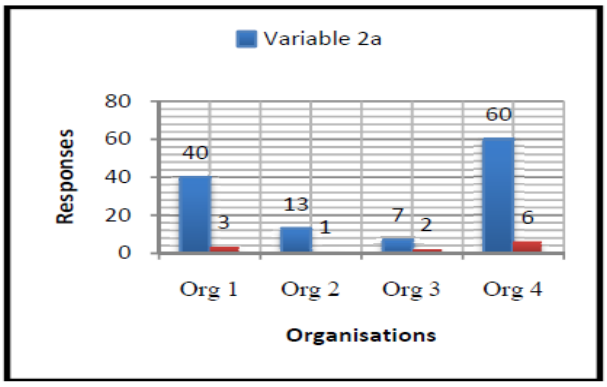

Figure 1 Level of Password Awareness

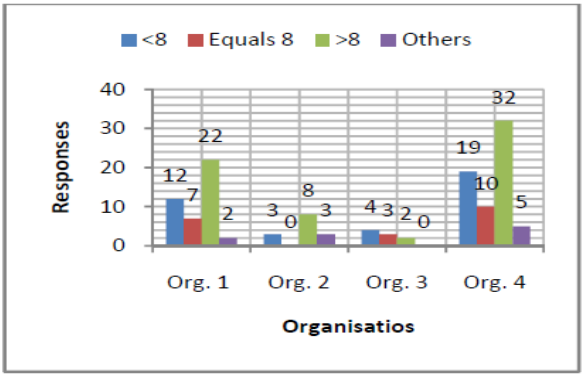

Figure 2 Significance of Password Length Awareness

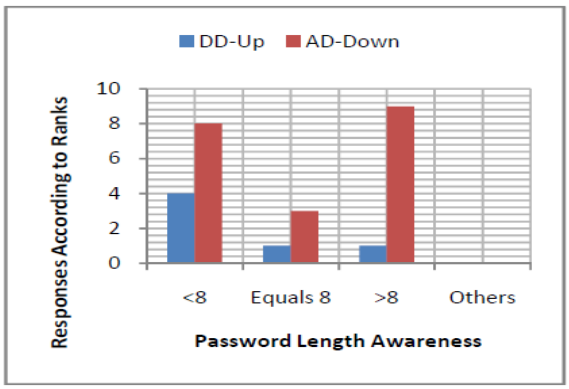

Figure 3 Significance of Password Length Awareness

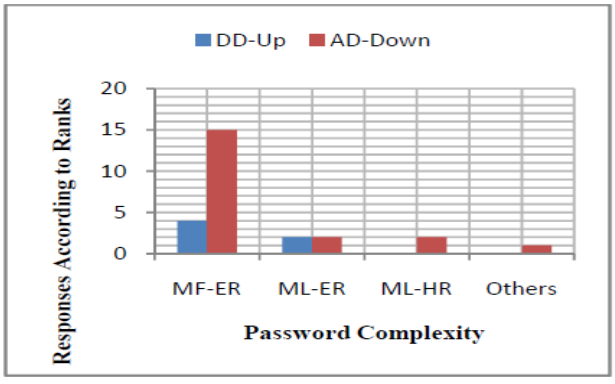

Figure 4 Significance of Password Complexity Awareness

Looking at the national statistics of this survey, Figures 1 and 2 shows that the levels of awareness are generally okay, but the percentage of users with passwords less than eight characters in figure 2 is too high for comfort. Figure 4 also shows a satisfactory result with the same caveat as in Figure 2.This result also illustrates the possibility that organizational administrators from AD-DOWN (about the age of 40 downwards) are not only more active on the net but also more security-conscious; the implication is that they take instructions from their less security conscious superiors. Lastly, Figure 4 confirms the fear that most internet users are inclined to choosing passwords that are both meaningful and easily remember-able.

3. Problem Statement

Many organizations have long lists of rules governing the content of passwords, primarily designed to defeat brute-force attacks; this has not succeeded due to rapid advancement in computing power and failure of many organizations to adequately monitor for failed login attempts. This seems to have eroded the value of the password as a single line of defense. Other disadvantages of complex passwords include the difficulty in remembering them, costs of generation and enforcing the password rules, as well as supporting users who have forgotten their passwords. In addition, users are skeptical of a system that imposes so many rules and regulations which they perceive as a burden. This results in evasive attitude, with attendant consequences.

Some organizations even specify minimum password ages (to prevent users from immediately switching back to the previous password); password histories to prevent reuse of passwords; and minimum number of characters to change to ensure that a new password is different enough from previous password. All of these elaborate rules make authorized access difficult, while driving up administrative and support costs for implementing and enforcing the rules. The objective for mandatory password changes stems from believes that passwords do leak out over time; but mandatory password changes address only a symptom, not the underlying cause of leakages. Eliminating account sharing, prompt account closing when users leave, regular auditing of all accounts, and educating users not to divulge passwords under any circumstances would be far more effective for addressing the sources of leakages.

It is noted that the human factor is the most critical factor in the security system for at least three possible reasons: it is the weakest link; it is the only factor that exercises initiatives; and the factor that transcends all the other elements of the entire system. This underscores the significance of social engineering in every security arrangement. It is thus recommended that, in the handling of password security issues, the human factors should be given priority over technological factors. It is realized that most of the password security-related problems have linkages with lack of secure storage system; thus encouraging users to choose weak passwords and compelling security engineers and managers to insist that passwords must not be written down and must be changed frequently.

4. Project Description

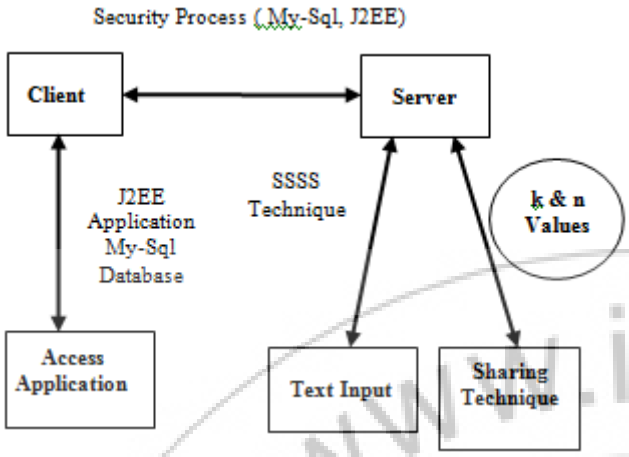

Figure 5: System Architecture

4.1 Strengthen User's Input

To strengthen the user input password we need to encrypt it and make it as unreadable formats. Make it we need some encryption algorithms. This scheme stores the inputs passwords and makes it as valuable one. To get the valuable password from the user and apply the Shamir's secret-sharing scheme to make a passwords in secure in the plain text that make the password into unreadable format, It will explore the use of the (k, n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of password repository.

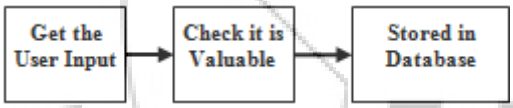

Figure 6: Strengthen User's Input

4.2 Shamir's secret-sharing scheme

Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

Some of the useful properties of Shamir's (k, n) threshold scheme are:

1) **Secure:** Information theoretic security.
2) **Minimal:** The size of each piece does not exceed the size of the original data.
3) **Extensible:** When k is kept fixed, D_i pieces can be dynamically added or deleted without affecting the other pieces.
4) **Dynamic:** Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5) **Flexible:** In organizations where hierarchy is important, we can supply each participant different number of pieces according to their importance inside the organization. For instance, the president can unlock the safe alone, whereas 3 secretaries are required together to unlock it.

4.3 Encryption

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message

To encrypt the user format as to convert plain text into cipher text model. Within that we need to add polynomial algorithm and stored into the database. That wise we make our password as more secured and stored in the database.

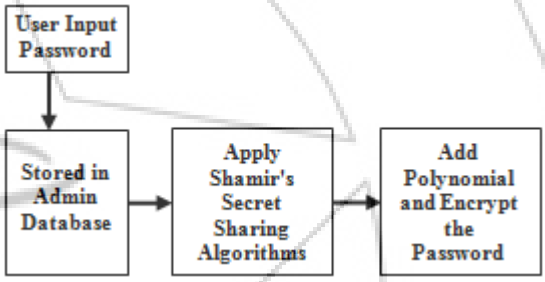

Figure 7: Encryption

4.4 Decryption

The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. We need to login means the passwords are decrypted from the encrypted element in the database. That retrieves the password from the polynomial conversion. It will reconstruct the cipher text and to make it as plain text.

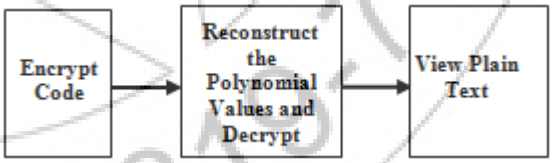

Figure 8: Decryption

4.5 Security

Security is the degree of protection to safeguard a nation, union of nations, persons or person against danger, damage, loss, and crime. Security as a form of protection is structures and processes that provide or improve security as a condition. The Institute for Security and Open Methodologies (ISECOM) in the OSSTMM 3 defines security as "a form of protection where a separation is created between the assets and the threat". This includes but is not limited to the elimination of either the asset or the threat. Security as a national condition was defined in a United Nations study (1986) so that countries can develop

and progress safely.

Security has to be compared to related concepts: safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of people attempting to cause destruction.

Different scenarios also give rise to the context in which security is maintained:

1) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
2) Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

4.5.1 Security concepts

Certain concepts recur throughout different fields of security

- **Assurance:** Assurance is the level of guarantee that a security system will behave as expected
- **Countermeasure**: A countermeasure is a way to stop a threat from triggering a risk event
- **Defense in depth**: Never rely on one single security measure alone
- **Exploit: A** vulnerability that has been triggered by a threat - a risk of 1.0 (100%)
- **Risk:** A risk is a possible event which could cause a loss
- **Vulnerability:** A weakness in a target that can potentially be exploited by a security threat

4.6 Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be.

4.6.1 Authentication methods

In art, antiques, and anthropology, a common problem is verifying that a person has the said identity, or a given artifact was produced by a certain person or was produced in a certain place or period of history.

There are three types of techniques for doing this.

1. The first type of authentication is accepting proof of identity given by a credible person who has evidence on the said identity, or on the originator and the object under assessment as the originator's artifact respectively.
2. The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verify the age of an artifact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos. Attribute comparison may be vulnerable to forgery. In general, it relies on the facts that creating a forgery indistinguishable from a genuine artifact requires expert knowledge, that mistakes are easily made, and that the amount of effort required to do so is considerably greater than the amount of profit that can be gained from the forgery. In art and antiques, certificates are of great importance for authenticating an object of interest and value. Certificates can, however, also be forged, and the authentication of these poses a problem. For instance, the son of Han van Meegeren, the well-known art-forger, forged the work of his father and provided a certificate for its provenance as well; see the article Jacques van Meegeren. Criminal and civil penalties for fraud, forgery, and counterfeiting can reduce the incentive for falsification, depending on the risk of getting caught.
3. The third type of authentication relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost. Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheques incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify. Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods.

5. Conclusion

Experts are now divided as regards whether it is better to write down the passwords or not. Due to the large number of password-protected systems that users must access, some experts encourage writing down passwords, as long as the written password lists are kept in a safe place, such as a wallet or safe; not attached to a monitor or in an unlocked desk drawer. Similarly, some even argue that the concept of password expirations is obsolete, because mathematically speaking, the practice of changing passwords frequently does not gain much security at all; one gains much more security if one increases the password length by just one character than changing the password on every usage and attempted usage. Hence, in order to ensure password security, we must strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security.

The human factor is the most critical factor in the security system for at least three possible reasons: it is the weakest

link; it is the only factor that exercises initiatives; and the factor that transcends all the other elements of the entire system. This line of reasoning buttresses the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and social engineering. In the course of organizational security awareness education processes, personnel should be informed on the need for the various techniques employed in the organization's password security architecture as an important means of checkmating human hacking or social hackers (socio-cryptanalysts). Let all concerned know that there can be no technical hacking in vacuum (independent of human hacking).

References

[1] M. Bando, 101st Airborne: The Screaming Eagles in World War II. Mbi Publishing Company,2007.[Online].Available at:http://books.google.com/books?id=cBSBtgAACAAJ. [Accessed: 20 May 2012].
[2] D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies." IJCSNS, vol. 10, no.4. April, 2010.
[3] S.M. Furnell et al., "Authentication and Supervision: A Survey of User Attitudes." Computers & Security, vol.19 no.6, pp 529-539, 2000.
[4] R.J. Sutton, Secure Communications: Applications and Management. Chichester: John Wiley & Sons, Ltd. 2002.
[5] E.F. Gehringer, (2002) "Choosing Passwords: Security and Human Factors." IEEE, 0-7803-7824-0/02/$10.00 8.
[6] S. Farrell, "Password Policy Purgatory." IEEE Computing Society. pp. 84-87, 2008.
[7] M.I.U. Adeka, J.S. Shepherd, and R.A. Abd-Alhameed, "Cryptography and Computer Communications Security: Social and Technological Aspects of Cyber Defence," Ongoing PhD Research Work, Schoolof Engineering, Design and Technology, University of Bradford,
[8] Lyquix Blog: Do We Need to Hide Passwords?. Lyquix.com. [Accessed: 17 Sept. 2012].
[9] "Cyber Security Tip ST04-002". Choosing and Protecting Passwords. US CERT. [Online]. Available: http://www.uscert.gov/cas/tips/ST04-002.html. [Accessed: 20 Jun. 2009].
[10] EmmaSoft, (2002) "Darn! Reminder Software!" [Online]. Available at: http://www.ordarn.com. [Accessed : 20 September, 20012].
[11] Human Factors of Security Systems: A Brief Review; Andrew Patrick, National Research Council of Canada
[12] Password Safe 1.7.1, Counterpane Labs,. [Online]. Available: http://www.counterpane.com/passsafe.html. [Accessed: 15 Oct. 2012].
[13] Q*Wallat, http://qwallet.com. [Accessed: 15 Oct. 2012].
[14] http://www.selznick.com/products/passwordwallet. [Accessed: 15 Oct. 2012].
[15] Microsoft Corporation, "Strong passwords: How to create and use them." [Online]. Available:(http://www.microsoft.com/security/online-privacy/passwordscreate.aspx) [Accessed: 11 Nov 2012].
[16] B. Schneier, 2005 "Schneier on Security: Write Down Your Password."[Online]. Availableat:
[17] (http://www.schneier.com/blog/archives/2005/06/write_ down_your. html). [Accessed: 25 Sep. 2012].
[18] E. Spafford, "Security Myths and Passwords." The Center for Education and Research in Information Assurance and Security. 2008. [Online]. Available: http://slashdot.org/story/06/04/25/0033238/spafford-on-securitymyths-and-passwords [Accessed: 21 Sep. 2012].
[19] www.internetworldstats.com. [Accessed: 15 November 2012] International Conference on Computer Applications Technology 2013 (ICCAT'2013), January 20 – 22, Sousse, Tunisia
[20] C. Swenson, Modern Cryptanalysis: Techniques for Advanced Code Breaking. Indianapolis:Wiley Publishing, Inc., 2008.
[21] J. Long, No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Publishing Inc., 2008.
[22] D. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks." EICAR Conferenc, 1998. [Online]. Available: http://cluestick.info/hoax/harley_eicar98.htm. {Accessed: 06 Oct. [2012].
[23] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_5.html. [Accessed: 16 November, 2012].
[24] http://www.zdnet.co.uk/news/security/2010/11/17/whitehall-officialoutlines-
[25] Cybersecurity-funding-plan-40090898/. [Accessed: 29 Sep. 2011].
[26] http://www.nesnip.org/securitychapter1.htm#Section%20I [Accessed: 10 Oct. 2012].
[27] Polybius on the Roman Military. Available: Ancienthistory.about.com. [Online]. [Accessed: 20 May 2012].
[28] R. Oliver, 8 Myths of Computer Security. [Online].Available: http://www.tech-mavens.com/myths.htm. [Accessed: 23 November 2012].
[29] J. Long, No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Publishing Inc., 2008.
[30] D. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks." EICAR Conferenc, 1998. [Online]. Available: http://cluestick.info/hoax/harley_eicar98.htm. {Accessed: 06 Oct.[2012].

Author Profile

Malladi Venkata Naga Kiranmai received Bachelor of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University Hyderabad. She is pursuing Master of Technology in Computer Science in School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. Her research interest is Computer Architecture, Human Computer Interaction, Wireless Network, Network Security and Data mining.

Avinab Marahatta received Bachelor of Engineering in Computer Engineering from Purbancal University. He is pursuing Master of Technology in Computer Science in School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. He worked in Higher Secondary Education Board (HSEB) Nepal, under the ministry of Education as Computer Engineer. His research interests are Computer Architecture, Human Computer Interaction, Wireless Network, Network Security and Data mining.

Kare Suresh Babu has completed his Master of Technology in Computer Science from Hyderabad Central University (HCU), Hyderabad. He is the Asst. Professor and course Coordinator for School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. His subjects of interests are Computer Networks, Network Security, Operating Systems, Wireless Networks, mobile Computing, Ethical Hacking and Wireless & Web Security.