Brute force attack*:* These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

SQL injection Attack: Also in this proposed system the encryption of password stored in the database is done using rijn dael's algorithm, so in case if the attacker got access to the database the data is no longer useful unless it is decrypted by the code which present at the application side.

V. RIJN-DAEL'S ALGORITHM

Rijn dael (pronounced rain-dhal) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). [11]

The Rijn dael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. Rijn dael uses a variable number of rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits
11 rounds if the key/block size is 192 bits
13 rounds if the key/block size is 256 bits

Also other asymmetric algorithm can be used for the purpose of encryption such as RSA algorithm but since it includes the concept of public and private key cryptography it makes the system very slow and rijn dael algorithm if used the efficiency of the system will much better.

VI. CONCLUSION

These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. This technique use grid for session passwords generation. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensive.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
[2] Real User Corporation: Pass faces. www.passfaces.com
[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin. "The design and analysis of graphical Passwords" in Proceedings of USENIX Security Symposium, August 1999.
[4] A. F. Sutra, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written With Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[5] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.
[6] Passlogix, site http://www.passlogix.com.
[7] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing
[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation
of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.
[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security*, 2004.
[10] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian Information Technology Security Symposium*, 2003.
[11] http://perso.uclouvain.be/fstandae/PUBLIS/11.pdf