International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

Secure and Time-Slot Based File Sharing In Cloud

[#1] P.Santhosh santhosh.santy2596@gmail.com
[*2] B.Pugazhenthi pugazhenthi217@gmail.com
[*3] L.Thiruvengada Varadhan d.kar40@gmail.com
[* 4] D.Sterlin Rani sterlinrani@gmail.com

[1,2,3] *U.G. Student, Department of Computer Science and Engineering, Kings Engineering College, Chennai.*
[4] *Assistant Professor, Department of Computer Science and Engineering, Kings Engineering College, Chennai.*

Abstract-Data sharing for increased productivity and efficiency is one of the primary requirements for today's organization. However, protecting online data is critical to the success, which leads to the requirement of efficient and secure cryptographic schemes for the same. A session secret key is a password exceptionally created for each session. The plan enables the framework to naturally create a session password each time the client sign in. The session password is produced arbitrarily in light of the haphazardly created network. The matrix is utilized as a medium for secret key age. While registration the client should typically enter his username and password while enrolling into the framework. Presently the framework stores this password and utilizations it to create a special session password while client sign in whenever. This session based verification framework utilizes the client secret key and thinks about letters in order contained nearby a 6*6 lattice with letters a-z and numbers 0-9. The client has to know the first password and the generation scheme to enter the correct password. Proposed framework breaks down the security and ease of use of the proposed plan, and demonstrates the help of the plan to shield from shoulder surfing assault. A data sharing scheme on the cloud is only successful if data owners can delegate the access rights to their data efficiently to multiple users, who can then access the data directly from the cloud servers. Data sharing is based on the given time interval which given by the data owner to the receiver, after the time interval, the receiver cant able get the file with the old session key.

Keywords: Security, password authentication, anonymity, smart card, dynamic ID.

OBJECTIVE

The main objective is to avoid shoulder surfing attack using pair based scheme which will generate session password for the particular session or transaction where there will be virtual keyboard which will shuffle at every another transaction accordingly.

I. INTRODUCTION

With the rapid development of low-power and highly efficient networks, mobile users can pay bills, buy goods online, and carry out electronic transactions by subscribing to various remote services. Though mobile computing devices are highly portable, they are usually unprotected and easy to be stolen or get lost. Unless precautions are taken, an unauthorized person may gain access to the information stored on them. For instance, illegal access may be acquired by intruders if the data is "sniffed out of the air" in wireless communications or some malware is installed. The lack of authentication and privacy may cause even more severe results like crippled devices, personal data loss, disclosure of non-public data, or charge of abused usage against the device owner. Mobile computing devices are of great security concern not only because of the data stored on them, but also for that they may provide access to other services that store or display non-public data. For almost all these transactions, mutual authentication and user privacy are required in the key exchange before remote servers start providing services to users.

Textual password is used for most authentications. The vulnerabilities of this strategy like eves dropping, word reference assault, social building and shoulder surfing are outstanding. Irregular and long passwords can influence the framework to secure. Nevertheless, the essential issue is the inconvenience of reviewing those passwords. Studies have demonstrated that clients tend to pick short passwords or passwords that are anything but difficult to recall. Shockingly, these passwords can be effectively speculated or split. The elective procedures are graphical passwords and biometrics. In any case, these two methods have their own impediments. Biometrics, for example, fingerprints, iris output or facial acknowledgment have been presented but not yet broadly received. The significant downside of this approach is that such frameworks can be costly and the distinguishing proof process can be moderate. There are numerous graphical secret key plans that are proposed in the most recent decade. Be that as it may, the vast majority of them experience the ill effects of shoulder surfing which is winding up a significant enormous issue. There are graphical passwords conspires that have been proposed which are impervious to bear surfing yet they have their own downsides like ease of use issues or setting aside more opportunity for client to login or having resilience levels. Individual Advanced Partners are being utilized by the general population to store their own and private data

like passwords and Stick numbers. Verification ought to be accommodated the utilization of these gadgets.

II. RELATED WORK

Password-based authenticated key exchange (PAKE)(Bellareetal.,2000;Boykoetal., 2000;Goldreich et al., 2001; Katz et al., 2001) is a two-party key exchange allowing users to utilize memorable passwords as secret information, where each password is shared between a user and an authentication server. Conventional authenticated key exchange protocols based on a public key cryptosystem need a key whose length is too long to remember. Since users cannot memorize such complicated information without devices, the users are unable to respond to any incident such as an emergency call unless the users have the devices. On the other hand, users can rely on PAKE protocols only with a short character string, and PAKE will also be suitable for cloud environments where ubiquitous access is important. There are two cases where conventional PAKE cannot be deployed. The first case is that there exists a gateway between a user and an authentication server as in a global roaming service. The second case is that there exists a malicious authentication server. In fact, the vulnerability of OpenSSL can cause a problem that the passwords stored in servers are leaked. Abdalla et al. (Abdalla et al., 2005; Abdalla et al., 2008) proposed schemes to solve those problems. Gateway PAKE (GPAKE) is a scheme addressing the first problem and Gateway Threshold PAKE (GTPAKE) is a scheme addressing both problems. However, their schemes are vulnerable to Undetectable On-line Dictionary Attack (UDonDA) (Ding et al., 1995), where an adversary guesses a password in online transaction and its password guessing attack is not detected by any authentication server. In their schemes, an authentication server returns a message without authenticating users, so the adversary can make unlimited attempts to guess a password. Due to the low entropy of the password, such a password guessing attack becomes a serious problem.

Bellovin and Merritt [2] in 1992 proposed an encrypted key exchange (EKE) protocol which integrated a secret key and a public key created to prevent delivered data from dictionary attacks. Ballare et al. [4] presented a method for the password-based authenticated key exchange (AKE) protocol which shows the correctness of Bellovin and Merritt's idea. Abdalla and Pointcheval [6] also demonstrated a twopassword-based encrypting key exchange protocol which is more efficient than the one introduced in [2]. However, when two users are communicating with each other, the shared password may be enumerated by hackers by using dictionary attacks. Sui et al. [8] and Lo et al. [12] modified the AKE protocols to improve the effectiveness of Abdalla and Pointcheval's protocol. Sui et al. [8] defined a two party authenticated key exchange (2PAKE) protocol which employs the ECC method, and Lo et al. [12] proposed a 2PAKE protocol for wireless networks following the specifications of the 3GPP2. However, their passwords are only chosen from a small space, and their protocols request each pair of users sharing a password, causing the fact that a huge amount of passwords are necessary when many users are involved in such a system.

On the otherhand, [7]proposed the three-party password authenticated keyexchange(3PAKE) protocol to enhance the security of the 2PAKE. In an insecure network, the 3PAKE utilizes a three-party server to help the communication parties to authenticate each other and exchange session keys. Following the approach proposed in [7], Luetal.[9]introduced a simple three-party password based authenticated key exchange (S-3PAKE) protocol to eliminate server's public key. However, in [10], Chungetal. Showed that the S-3PAKE is still exposed to impersonation-of-initiator attack, and they used a counter to resist such attack. Nevertheless, [11] indicated that the protocols claimed in [9] and [10] are still vulnerable to man-in-the-middle attack and unknown keyshare attack. In order to reduce the communication steps of 3PAKE, [13] designed an efficient 3PAKE protocol requiring neither server public key, nor symmetric cryptosystems. Meanwhile, [14] presented several proposed protocols which are still vulnerable to attacks, such as undetectable online-dictionary attacks [5], key-share attacks [3], and both online and offline password guessing attacks [1].

Various schemes have been proposed so far for the two-party remote authentication; however, some of them have been proved to be insecure. In this paper, we propose an efficient timestamp-based password authentication scheme using smart cards. We demonstrate different sorts of fraud assaults against a formerly proposed timestamp-based secret key verification conspire and enhance that plan to

guarantee vigorous security for the remote validation process, keeping every one of the preferences that were available in that plan. Our plan effectively guards the assaults that could be propelled against other related past plans. We introduce a point by point cryptanalysis of beforehand proposed Shenet. al's plan and an examination of the enhanced plan to demonstrate its upgrades and proficiency. In this paper, we have shown the weaknesses and different types of attacks on Shenet. al. scheme including a new type of attack. We have presented our improved scheme which could successfully defend all sorts of attacks mentioned earlier. We have presented in the related works section that, the other schemes in this area are more or less vulnerable to the attacks that are mentioned in this paper. Our scheme ensures robust security at the time of communication over the insecure channel and keeps all the other advantages that were present in the previous scheme.

III. SYSTEM ANALYSIS

Existing System

A graphical authentication technique, where the user has to select some images from a set of random pictures when user is going to register and then at the time of login user must have to select the same sequence of images which he has pre-defined at the time of registration.

A color keyboard implementation, where alphabets and numbers of keyboard are given with different colors. After the user click, all keys on the keyboard shuffles every time. Here, user has to note down particular position of key before pressing desired key. Then a button named 'Hide Keys' have to be pressed, which will hide all characters from the keys and empty keys will be displayed before user. Then user has to click on that key which has the desired key earlier. For which the user can make use of key color for remembering it.

Disadvantages

1) A graphical authentication technique and a color keyboard implementation, these techniques are vulnerable to shoulder surfing attack.
2) Receiver can retrieve the file for a long time with the same key, and this receiver can also distribute to other more users.

Proposed System

In this project, it is proposed an improved text-based shoulder surfing resistant scheme by using pair based scheme is used for alphabet, digit , symbols where session password will form at every session or transaction using virtual shuffling keyboard. At the time of registration user have to submit password. Particularly the length of the password is 8 and it can be named as secret key. The secret key consists of even or odd number of characters. Then next stage is the login phase, when the user enters his username as an interface, the 6 x 6 grid display of row and column size screened before user. The grid display consists of alphabets and numbers. These are sequentially placed on the grid at every cell and this interface changes every time according to every transaction.

According to pair based scheme, user have taken first letter from his registered password as row wise and second letter as column wise and then the intersection which will form will be the part of session password. As each and every time the keyboard will shuffle, the session password will also change and hence automatically security is getting to login. A data sharing scheme on the cloud is only successful if data owners can delegate the access rights to their data efficiently to multiple users, who can then access the data directly from the cloud servers. Data sharing is based on the given time interval which given by the data owner to the receiver, after the time interval the receiver cant able get the file with the old session key.

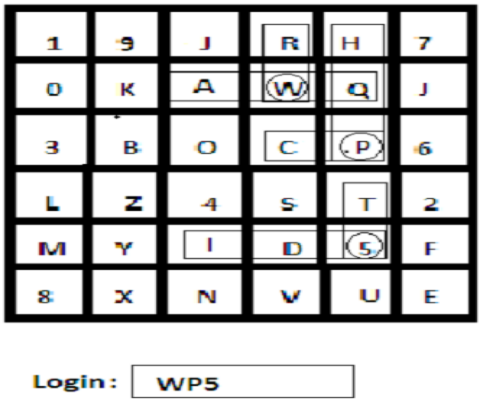

Fig.1. Grid Matrix

Advantages

1) Proposed system analyses the security and usability of the proposed scheme, and shows the support of the scheme to shoulder surfing attack.

2) It must provide in order to prevent hackers from accessing the data present in account of particulars.

3) The vulnerabilities like dictionary attack, social engineering and shoulder surfing attack, are avoidable by using this proposed scheme.

IV. SYSTEM DEVELOPMENT

Modules

1. Session Grid algorithm
2. File upload and Encryption
3. Session based data sharing
4. File Decryption and Download

Session Grid Algorithm

The session password is created haphazardly in light of the arbitrarily produced matrix. The network is utilized as a medium for secret key age. While login the client should regularly enter his username and password while enrolling into the framework. Presently the framework stores this password and uses it to create an extraordinary session password while client sign in whenever. This session based confirmation framework utilizes the client password and looks at letter sets contained nearby a 6*6 network with letters a-z and numbers 0-9. The client has to know the first password and the age plan to enter the correct password.

File Upload And Encryption

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

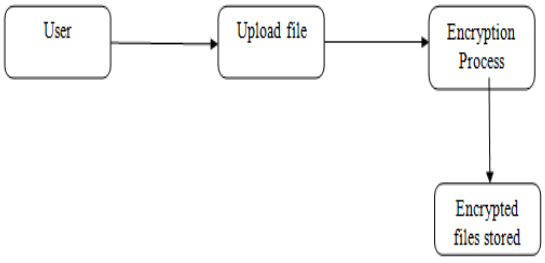

Fig. 2. File Upload

Session Based Data Sharing

The users can view the files which are uploaded by them, and then the users can share the files to the receiver by giving the time limit to accessing the data. Based on the time limit, the session key is generated for that file access. The key is only valid for that user given time, after the time limit the receiver have no access for that file.

File Decryption And Download

User requests the file by providing details and in response system replies with encrypted file. Before that the system will check the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it's correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

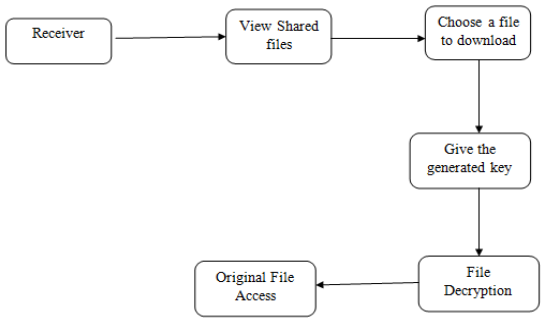

Fig. 3. File Download

V. IMPLEMENTATION

Step 1: Password Registration-In the proposed scheme user has to set textual password K of length L. The minimum length of Password is 8 Characters and the maximum length of password is 15 characters i.e. password length is between 8 to 15 Characters. And, the user has to register an e-mail address for enabling his account when he enters a wrong password. In this scheme, registration process should carried out in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user's textual password in the users entry in the password table, which should be encrypted by the system key. So in short in registration phase the user set is textual password.

Step 2: After the successful registration user have been forwarded to the Login page. In this page we can able to see the grid matrix. The grid matrix shuffle each and every session when the user login. The user enters is username and password and the grid used to store as the encrypted format. Grid takes the user password as a combination of two letters. for an example if user password is 'apple' it takes as 'ap' as a first combination, 'pl' as a second combination and the third we can see that there is remaining only one letter called 'l', the grid take it as 'l0' it automatically assigned '0' to the odd number of characters. It encrypt the password like , first letter in the row wise and second letter in the column wise , the intersection of both letter makes as an encrypted key. So in Login phase the password stores as an encrypted format.

Step 3**:** In the proposed scheme, the uploaded files are store in an encrypted format, in which the hackers cannot be open a file. The files are encrypted by using Advance Encryption Algorithm (AES). Then the file can be sharing to another the user. The receiver cannot be able to download the file directly. They can download the file by using secret key which have been send along with file. That secret key can be generated by Random Generation Key which is the combination of alphanumeric, case-sensitive, and symbols eg,.Acf12e@#. This key can be available in View key menu. There also a time limit for the file and the shared file can be able to download during this time limit with the secret key. If the time limit varies then the secret key becomes invalid and the file could not be downloaded. This gives more security in sharing of files. The vulnerabilities like dictionary attack, social engineering and shoulder surfing attack, are avoidable by using this proposed scheme.

First of all the user have to register the details. After the registration, user go to the login page. The user have to type the registered user name and password, the grid matrix analyze and stores the password in encrypted format. After the successful login, the user can upload the files; these files are stored in an encrypted format. Then the user can share the file to the user with the time limit given to the file.

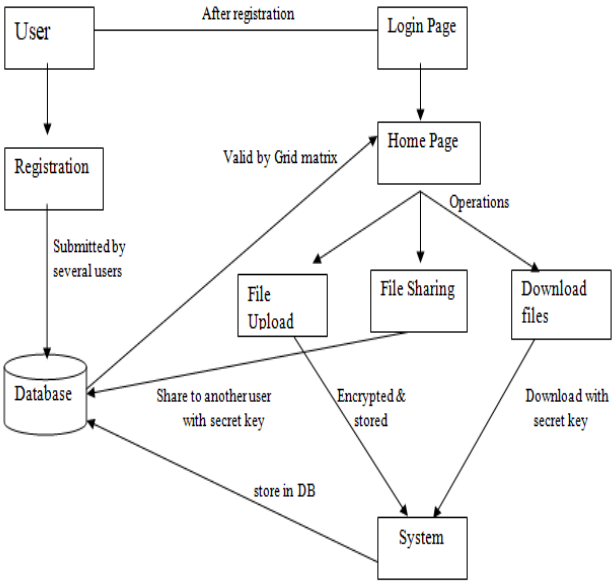

Fig. 4.Proposed System Architecture Diagram

The receiver can download the file by pasting the secret key of the file. The secret key can be available in View key section.

VI. RESULT and DISCUSSION

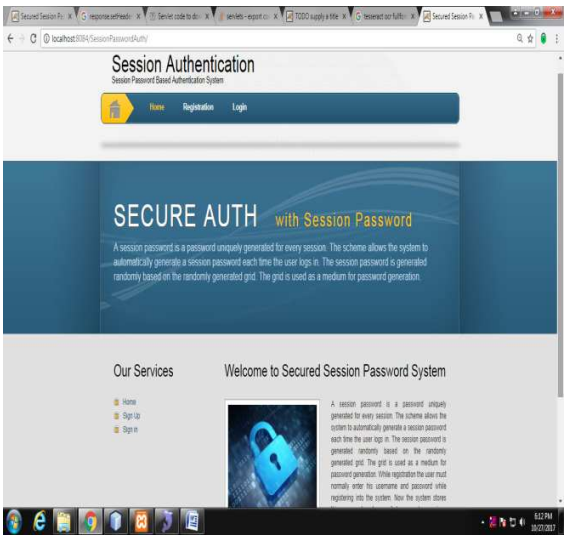

Fig.4.1. Homepage

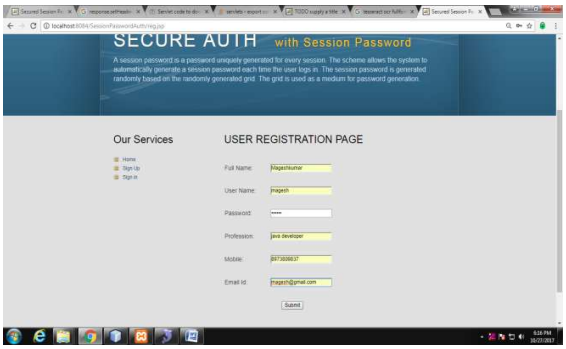

Fig.4.2. Register the user details

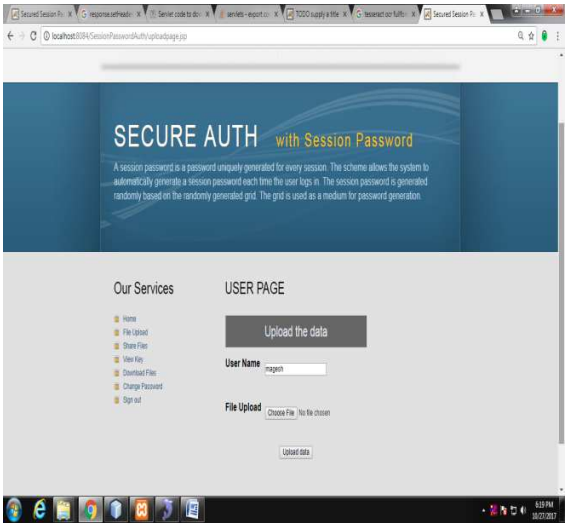

*Fig.4.3. Select the File to Upload***.**

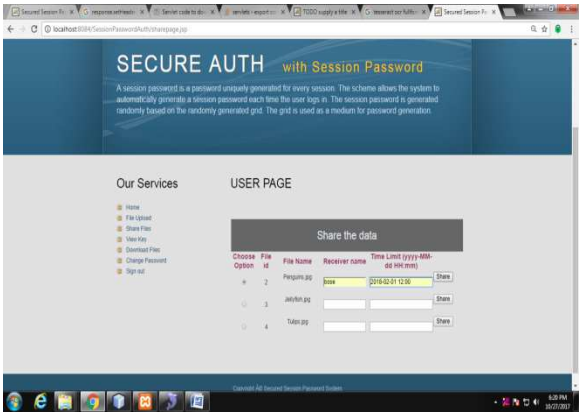

Fig.4.4. Share the File to the other user

CONCLUSION

There are many techniques which are proposed for preventing shoulder surfing attack, with all proposed techniques the session based password scheme using shuffling keyboard with Pair Based method is more effective and secure to shoulder surfing attack, as this technique is providing a particular session password for every session or transaction Also, it is easy to use and handle, hence in near future, this technique has scope to use in many fields for the security purpose. In this paper, we proposed an Anonymous Two-Factor AKE scheme which preserves security against various attacks including de-synchronization attack, lost-smart-card attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or intractability, adaptively password change, no centralized password storage, and no long-term public key. Furthermore, our protocols maintain high efficiency in terms of storage requirement, communication cost as well as computational complexity. Our protocol requires only a few number of message flows and all the transmitted messages are short in size. Additional, the proposed scheme is provably secure in our extended security model of AKE. Therefore, the proposed scheme is suitable for deployment in various low-power networks, in particular, the pervasive and mobile computing networks.

FUTURE ENHANCEMENT

1. Optimal Algorithms for Complex Data Structures
2. Different Fusion Operators
3. Concurrent Updates on Backup Structures

REFERENCES

[1]D.Yunand H. Patrick, ‘‘Undetectable on-line password guessing attacks,’’ ACM SIGOPS Oper. Syst. Rev., vol. 29, no. 4, pp. 77–86, Oct. 1995.

[2] S.M.Bellovinand M.Merritt, ‘‘Encrypted key exchange :Password-based protocols secure against dictionary attacks,’’inProc.Symp.Secure.Privacy, May 1992, pp. 72–84.

[3]B.W. Simon and M. Alfred, ‘‘Unknown key-share attacks on the stationto-station (STS) protocol,’’ in Proc. Int. Workshop Pract. Theory Public Key Cryptogr., Mar. 1999, pp. 154–170.

[4]M.Bellare, D.Pointcheval, and P.Rogaway, ‘‘Authenticated key exchange secure against dictionary attacks,’’ in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Bruges, May 2000, pp. 139–155.

[5]W.S.Robert, Internet Security Glossary, document 55, May 2000.

[6]M. Abdalla and D. Pointcheval, ‘‘Simple password-based encrypted key exchange protocols,’’ in Topics Cryptology. Berlin, Germany: SpringerVerlag, 2005, pp. 191–208.

[7] M. Abdalla, P. A. Fouque, and D. Pointcheval, ‘‘Password-based authenticated key exchange in the three-party setting,’’ in Proc. Int. Workshop Theory Pract. Public Key Cryptogr., Jan. 2005, pp. 65–84.

[8]A.-F. Sui et al., ‘‘An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication,’’ in Proc. IEEE Wireless Commun. Netw.Conf., vol. 4. Mar. 2005, pp. 2088–2093.

[9]R. X. Lu and Z. F. Cao, ‘‘Simple three-party key exchange protocol,’’ Comput. Secur., vol. 26, no. 1, pp. 94–97, Feb. 2007.

[10]H.R.Chungand W.C.Ku,‘‘Three weaknesses in a simple three-party key exchange protocol,’’ Inf. Sci., vol. 178, no. 1, pp. 220–229, Jan. 2008.

[11]H. Guo, Z. J. Li, Y. Mu, and X. Y. Zhang, ‘‘Cryptanalysis of Simple Three-party Key Exchange Protocol,’’ Comput.Security, vol.27, nos.1–2, pp. 16–21, Mar. 2008.

[12]J. W. Lo, C. C. Lee, M. S. Hwang, and Y. P. Chu, ‘‘A secure and efficient ECC-based AKA protocol for wireless mobile communications,’’ Int. J. Innov. Comput., Inf. Control, vol. 6, no. 11, pp. 5249–5258, Nov. 2010.

[13]T. Y. Chang, M. S. Hwang, and W. P. Yang, ‘‘A communication-efficient three-party password authenticated key exchange protocol,’’ Inf. Sci., vol. 181, no. 1, pp. 217–226, Jan. 2011.

[14]E.J.Yoonand K.Y.Yoo, ‘‘Cryptanalysis of a simple three-party password based key exchange protocol,’’ Int. J.Commun. Syst., vol. 24, no. 4, pp. 532–542, Apr. 2011.

[15] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol.9, no. 1, pp. 277-293, 2013.

[16] V. C. Gungor, and G. P. Hancke, "Industrial wireless sensor networks: challenges, design principles and technical approaches," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258-4265, Oct. 2009.

[17] D. Liu, M. C. Lee, and D. Wu, "A Node-to-Node Location Verification Method," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1526 - 1537, May 2010.

[18] C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629-637, Jan. 2012.

[19] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-On Mechanism for Distributed Computer Networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 294-302, 2013.

[20] L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163-2172, Oct. 2010.

[21] Y. Huang, W. Lin, and H. Li, "Efficient Implementation of RFID Mutual Authentication Protocol," IEEE Trans. Ind. Electron., vol. 59, no. 12, pp. 4784 - 4791, 2012.

[22] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689-696, Aug. 2012.