MJFAS
Malaysian Journal of Fundamental and Applied Sciences

Refish *et al.* | Malaysian Journal of Fundamental and Applied Sciences, Vol. 19 (2023) 440-446

RESEARCH ARTICLE

One Time Password based Mutual Text Authentication

Salah H Abbdal Refish

Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-sadiq University, Baghdad, Iraq

Abstract Many applications in the internet using Password for identify users. So, this password must be strong and safe to avoid unauthorized users. The critical issue in many applications such as web-sites and data base systems is password authentication code (PAC). In this paper, PAC between two parties to confirm password authentication between them based mutual text authentication has presented. Two factors is the best solution in this field. But to be more secure and to be more efficient a legitimate user needs to make sure about his partner to ensure their communications should use another method without need more costs and avoid plurality of algorithms. So, this solution uses mutual text authentication as new solution which the text is predetermined by users. This method is considered new in this field, as this method tries to make the password highly secure in front of unauthorized users and to make the process of accessing information specific only to the actual authorized users. When analysing this method, we find that it has many characteristics such as the confidentiality of the session key and privacy, in addition to the exchange of authentication between the two parties to ensure that others do not interfere.

Keywords: Password authentication code, mutual text authentication, IOT, Man-In-The-Middle, Resistance against offline-Attacks.

Introduction

The most common problem that occurs in online applications by users when the password is repeated in more than one application [1,2]. Multiple passwords can lead to forgetting, so the user must try again and again for the purpose of obtaining it, and therefore this will negatively affect his security, as it gives an opportunity for attackers to increase the possibility of obtaining a number of passwords belonging to the user [2]. The process of two factor password authentication is widespread for the purpose of protecting applications from expected online-offline attacks [3]. So, we must pay attention to the issue of password security in a way to prevent it from being detected by online – offline attackers. The researchers dealt with improving the performance of the password and trying to make it safe from attackers. Through completely right password authentication makes the resources accessible over insecure channels [4]. Authentication is a very important protection system that is used to limit the process of password penetration if it is used in a way that ensures that it is not hacked by any of the multiple attacks [5]. Therefore, many of papers presented such authentication scheme that utilized two-factor or multiple approaches in order to offer more safety [6]. This concept has been evolving to M2M networks in the internet of things (IOT) [7-10].

For overcoming the vulnerabilities against attackers should be make the password authentication more secure and more memorable for the users. Additionally, the users do not give them any opportunity to penetrate and reveal it [11]. Many researchers have worked to find optimal solutions to authenticate the password, some of them have worked on single server [12 - 15], and some worked on multiple server [16-21]. However, most of these techniques vulnerable to the attackers like replaying attack and denial of service attack. In addition to material and software overheads.

In this paper, do not need more costs and avoid plurality of algorithms. It uses mutual text authentication

***For correspondence:**
salah.hassan@sadiq.edu.iq

Received: 7 Nov. 2022
Accepted: 11 April 2023

10.11113/mjfas.v19n3.2994

as a new solution which the text is predetermined by users. The overall of this method convincingly to be more secure against both online and offline attacks.

Our proposed is that the short number is very easy to use and remember, but we should find a method to protect this password from expected attacks. So, one time password based mutual text authentication is presented in this paper, when the password is used by the user should the other entity uses the text for the authenticate with the user. In the other hand, the user should authenticate with that entity.
The contributions of this paper can be summarized in the following points:

- Using a simple password does not reduce its importance by having a way to keep it confidential.
- Reduce the chances of attackers in the process of hacking the password.
- Implementing the authentication process to increase confidentiality between two specific parties.
- In this paper, mutual text authentication is used as a new solution instead of most of the previous researches, which uses multiple software and other costs.

The rest of this paper is organized as follows: Section 2 shows the related work, section 3 describes the proposed scheme, discusses security analysis in Section 4, Section 5 shows performance of this work, Section 6 concludes the paper.

Related Work

The proposed method in research [22] deals with a good method in the authentication process, but with that, this method suffers in the process of protecting information from some attacks, as in replay attacks and impersonation attacks. Through the proposed method [23], which is used in mobile and communication systems, a new method has been proposed in the over-the-air authentication process for the M2M networks. However, this method is considered irresistible to vulnerability to attacks in the M2M systems. [24] produced a healthcare system based authentication. In this scheme, the authors used ID based authentication method for M2M systems. Although this method strong in front of different attacks but it cannot immune for denial of service. The technique in [25] is very important in achieving authentication because it provides security that ensures that information is protected from attackers, and therefore this method provides all the possibilities for the purpose of high-level protection and on the number of being high-level security, Although this method is safe, it has little usability.

To achieve more security in the process of preserving information from various attacks, scientific research has expanded to find modern methods that include biometrics, which can be used to obtain a high level of security, but they are practically ineffective [26-27]. In research [28-30], the smart card was used to authenticate the password and achieved many security features, but this work is weak against impersonation attacks, in addition to not protecting the session key in a way that guarantees protection from other attacks.

Proposed scheme

In this section we will describe the method. In general, this method depends on mutual text authentication, meaning there are two parties. The first party must agree with the second party on some secret messages between them, such as normal messages or a question and answer in order for the authentication process to take place between them. Figure 1 shows the flowchart of our proposed.

We have two rounds in this scheme. In the first round, the first party (FP) will write its own password, agreed upon in advance by both parties. Then send it to the second party (SP) who will work on it some procedures to obtain E to send it again to the FP. The FP will compare his own E' with E which sent by SP, if the result is match that is mean the authentication is true. Otherwise the result is false and then the system will be terminate. In the second round, and after the FP sent E', the SP will add some procedures on it to produce new result and compares with output which sent by FP, if output of FP=output of SP that is mean there is authentication between them, otherwise, the process of the scheme is terminate. Table 1 shows the notifications of our scheme.

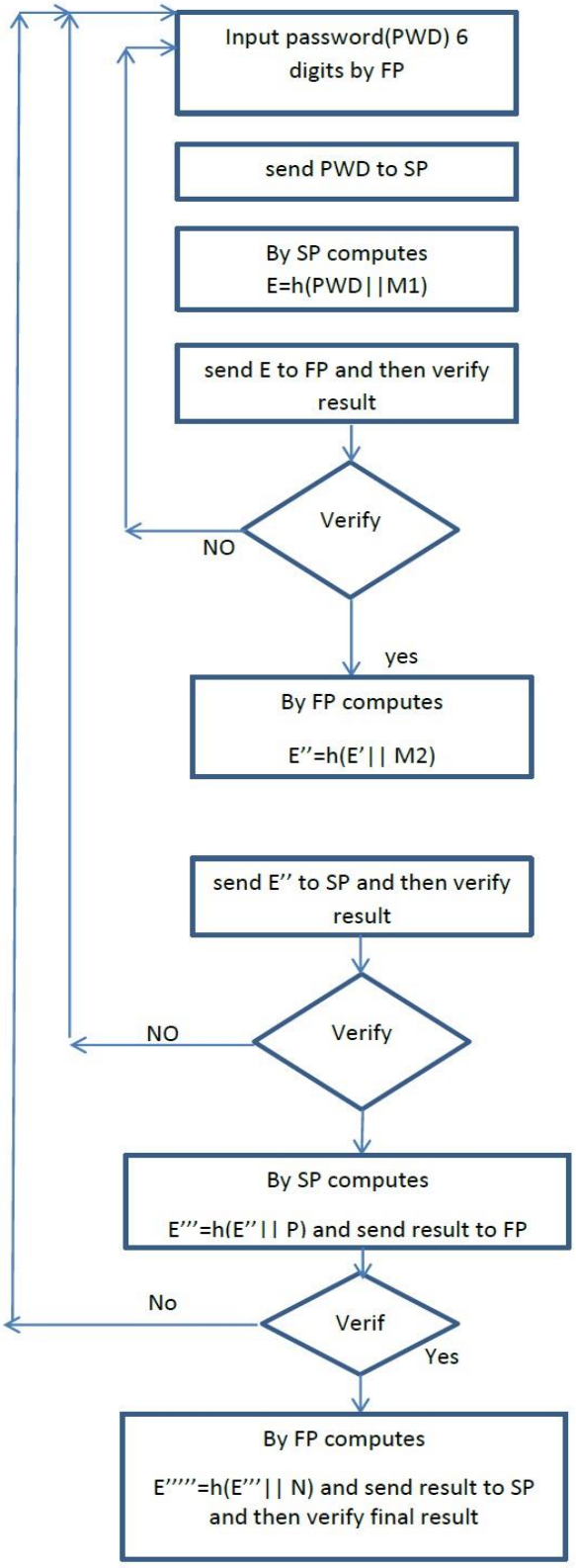

Figure 1. Flowchart of our proposed

Table 1. Notifications of the scheme

Symbol	Definition
FP	First party
SP	Second party
PWD	Password of FP
E	The result after some procedures by SP one round
E’	The result after some procedures by FP one round
E’’	The result by FP second round
E’’’	The result by SP second round
E’’’’	The result by FP third round
E’’’’’	The result by SP third round

The steps of process of authentication between FP and SP will describe as follows: PWD=Password, M=message.

- FP will type his password which contains 6 digits from 0 to 9 randomly. Then, send it to the SP.
- SP will do some procedures on his password:

o E=UpdatePWD=h(PWD||M1).At this point it will be sent E to FP for verification.

- Now, FP again will verify it by using some procedures as follows:

o E’=h(PWD||M1) and compare E with E’ if both equals that is mean the verification is successful and go the next step, otherwise, the process is stop.

- The next step is that the FP sent E’’ which contains E’’=h(E’||M2) to SP.
- SP produces E’’’=h(E’’ ||M2) as a new result and then will compare it with sent by FP, (E’’), if the result is true that is mean SP authenticates with FP. Otherwise, the process is considered a failure. SP computes E’’’’ = h(E’’’||P), and then sends it to FP.
- FP computes E’’’’’= h(E’’’’||P) and then compares it with result of SP. FP generates large prime numbers p and q then calculates E’’’’’=h(E’’’’||N=P*q), then sends E’’’’’ to SP.
- Finally, SP verifies his math with sent by FP. Figure 2 shows the procedures of our proposed scheme.

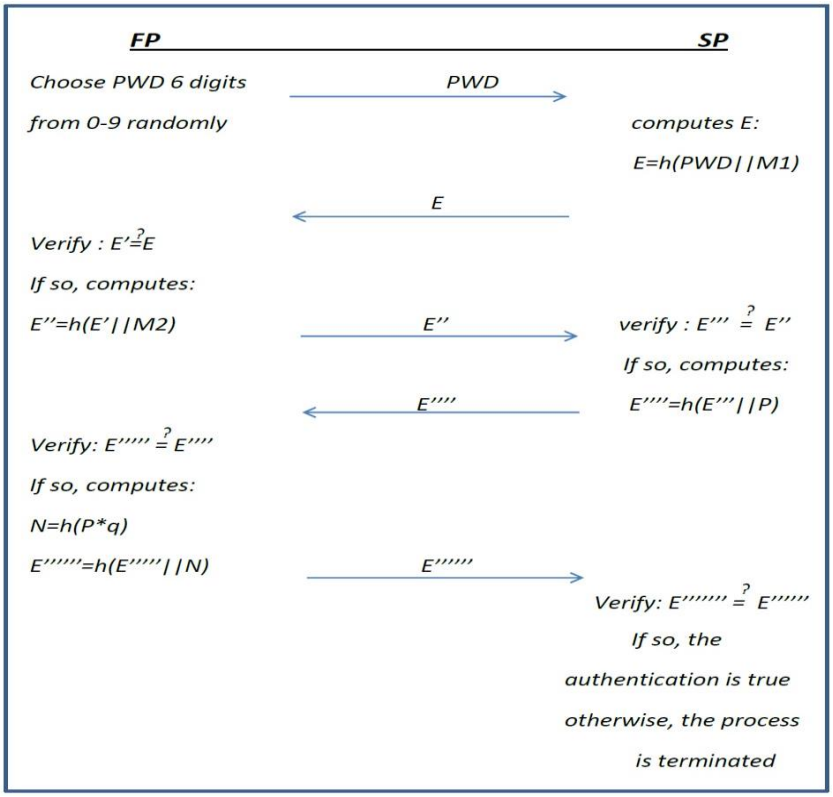

Figure 2. Structure of our proposed

Security Analysis

At this point and in this section of the research, we will discuss the most important security features that characterize it, and we will mention them as follows:

Mutual Authentication

Means that an attacker cannot impersonate the intended party. In this scheme, Password authentication requires that there are four rounds in order to be achieved, otherwise the authentication process is considered a failure and that it has been hacked by unauthorized parties.

As we can see in the above scheme Figure 1, the password will not alone be subject to unauthorized parties, but rather it will be subject to pre-agreed changes between two specific parties. Therefore, if the password is hacked, it will not benefit anything as long as it is subject to four rounds that are difficult to penetrate and used once for each session between the two parties.

We note that in the method used there is an agreement between two specific parties on private messages, as well as on the generation of large prime numbers and the hash process that is applied in each calculation process, and all of this makes the process of hacking the password very difficult.

MITM (Man-In-The-Middle) attack

The attacker uses this attack when the user signs out the applications. The task of this attacker is that he intersects between two parties for the purpose of obtaining information through which the hack takes place. In our method, he does not benefit from any information he obtains as long as there are four rounds to verify the work, and in each round the information is changed for one time only. As long as this attack is used in the event of getting out of work in many cases, then it has no meaning in the method used, where in each session the information is changed based on the information agreed upon between the two parties. So, our scheme can resist MITM.

Our scheme resist the replay and dictionary attacks

The proposed system requires multiple operations to obtain the results, which are for one time in the event of entering any application through the password. Thus, the values obtained are incomprehensible and this can avoid dictionary attacks. Since at the end of the rounds, other values are used to verify the password, and these values are calculated after adding large prime numbers, the system is resistant to replay attacks. FP sends E to the SP in the first step. SP does some operations on E to generate E' and then sends it again to FP. At this point, the first round is begin for authentication process. And the situation continues until the last round and the generation of new values and approval by both parties. You can see that in Figure 1.

Resistance against offline-Attacks

The password, as we noted from the above figure, has been added to multiple calculations and for four rounds for the purpose of obtaining authentication, so it cannot be hacked or known by offline dictionary attacks. Only the person who can know what changes have occurred to the password is the one who knows the confidential information of the system.

Performance scheme

We tested the method on 500 users and it achieved a great speed in performance. The average time spent for each user is 0.0098. The following Figure 3 shows the speed gradient for a number of users in this system, which is an ideal ratio while maintaining the confidentiality of information, as we mentioned in the security analysis.

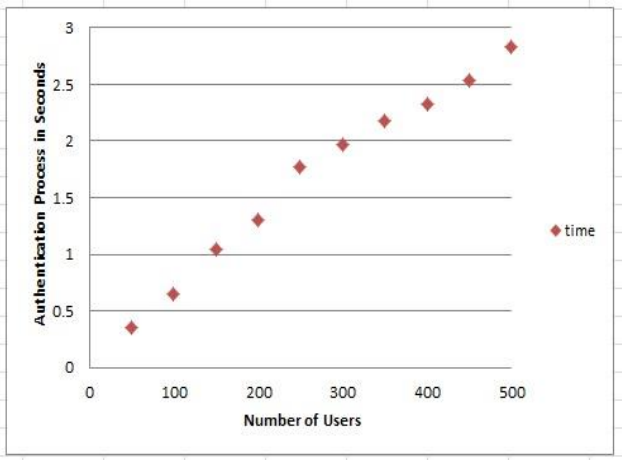

Figure 3. Performance of the proposed system

Conclusion

This research paper deals with a very important topic, which is the confidentiality of the password between two specific parties. Only an agreement between the parties on confidential information was used in this way. It was assumed that this confidential information would be pre-agreed messages as well as large prime numbers and use of this information for the purpose of authentication between the two parties. The method used in the password authentication process is only one time in order to avoid the various attacks that may occur to break the password, and it is just information previously agreed upon. Therefore, we can say that this method is very impervious to online and offline attacks. The security analysis shows that this scheme is very effective in resisting the various attacks that may occur. In addition, the proposed system has achieved a high speed of implementation, as one user needs only 0.0098 seconds for the purpose of implementation.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Acknowledgment

This work is part of a research project, supported by Faculty of Information Technology, Imam Ja'afar Al-sadiq University, Baghdad, Iraq

References

[1] Refish, S. (2018, October). PAC-RMPN: Password authentication code based RMPN. *2018 International Conference on Advanced Science and Engineering* (ICOASE) (pp. 286-289). IEEE.

[2] Doğanay, C., & Küpçü, A. (2020, December). Comparative survey on single password authentication techniques. *2020 International Conference on Information Security and Cryptology* (ISCTURKEY) (pp. 5-10). IEEE.

[3] Wang, Q., Wang, D., Cheng, C., & He, D. (2021). Quantum2fa: efficient quantum-resistant two-factor authentication scheme for mobile devices. *IEEE Transactions on Dependable and Secure Computing*.

[4] Karuppiah, M., Das, A. K., Li, X., Kumari, S., Wu, F., Chaudhry, S. A., & Niranchana, R. (2019). Secure remote user mutual authentication scheme with key agreement for cloud environment. *Mobile Networks and Applications*, *24*, 1046-1062.

[5] Aljewaw, O. B., Karim, M. K. A., Kamari, H. M., Zaid, M. H. M., Salim, A. A., & Mhareb, M. H. A. (2022). Physical and spectroscopic characteristics of lithium-aluminium-borate glass: Effects of varying Nd_2O_3 doping contents. *Journal of Non-Crystalline Solids*, *575*, 121214.

[6] Ma, S., Feng, R., Li, J., Liu, Y., Nepal, S., Bertino, E., ... & Jha, S. (2019, December). An empirical study of sms one-time password authentication in android apps. *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 339-354).

[7] Renuka, K. M., Kumari, S., Zhao, D., & Li, L. (2019). Design of a secure password-based authentication

scheme for M2M networks in IoT enabled cyber-physical systems. *IEEE Access*, *7*, 51014-51027.

[8] Salim, A. A., Ghoshal, S. K., Danmallam, I. M., Sazali, E. S., Krishnan, G., Aziz, M. S., & Bakhtiar, H. (2021, April). Distinct optical response of colloidal gold-cinnamon nanocomposites: Role of pH sensitization. *Journal of Physics: Conference Series*, 1892(1), 012039. IOP Publishing

[9] Osei, E. O., Hayfron-Acquah, J. B., & Kumasi, K. N. U. S. T. (2014). Cloud computing login authentication redesign. *International Journal of Electronics and Information Engineering*, *1*(1), 1-8.

[10] Salim, A. A., Bidin, N., Bakhtiar, H., Ghoshal, S. K., Al Azawi, M., & Krishnan, G. (2018, May). Optical and structure characterization of cinnamon nanoparticles synthesized by pulse laser ablation in liquid (PLAL). *Journal of Physics: Conference Series*, *1027*(1), 012002. IOP Publishing.

[11] Anwar, N., Riadi, I., & Luthfi, A. (2016). Forensic SIM card cloning using authentication algorithm. *International Journal of Electronics and Information Engineering*, *4*(2), 71-81.

[12] Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on consumer Electronics*, *46*(1), 28-30.

[13] Ramasamy, R., & Muniyandi, A. P. (2012). An Efficient Password Authentication Scheme for Smart Card. *Int. J. Netw. Secur.*, *14*(3), 180-186.

[14] Salim, A. A., Ghoshal, S. K., Shamsudin, M. S., Rosli, M. I., Aziz, M. S., Harun, S. W., ... & Bakhtiar, H. (2021). Absorption, fluorescence and sensing quality of Rose Bengal dye-encapsulated cinnamon nanoparticles. *Sensors and Actuators A: Physical*, *332*, 113055.

[15] Chen, T. Y., Lee, C. C., Hwang, M. S., & Jan, J. K. (2013). Towards secure and efficient user authentication scheme using smart card for multi-server environments. *The Journal of Supercomputing, 66*, 1008-1032.

[16] Guo, C., Chang, C. C., & Chang, S. C. (2018). A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless c*ommunications. Int. J. Netw. Secur.*, *20*(2), 323-331.

[17] Lin, I. C., Hwang, M. S., & Li, L. H. (2003). A new remote user authentication scheme for multi-server architecture. *Future Generation Computer Systems*, *19*(1), 13-22.

[18] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[19] Salim, A. A., Bidin, N., & Islam, S. (2017). Low power CO2 laser modified iron/nickel alloyed pure aluminum surface: Evaluation of structural and mechanical properties. *Surface and Coatings Technology*, *315*, 24-31.

[20] Liu, Y., Chang, C. C., & Sun, C. Y. (2016). Notes on" An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics*". Int. J. Netw. Secur.*, *18*(5), 997-1000.

[21] Lu, R., Li, X., Liang, X., Shen, X., & Lin, X. (2011). GRS: The green, reliability, and security of emerging machine to machine communications. *IEEE Communications Magazine*, *49*(4), 28-35.

[22] Agarwal, S., Peylo, C., Borgaonkar, R., & Seifert, J. P. (2010, October). Operator-based over-the-air M2M wireless sensor network security. *2010 14th International Conference on Intelligence in Next Generation Networks* (pp. 1-5). IEEE.

[23] Abbas, S. I., Hathot, S. F., Abbas, A. S., & Salim, A. A. (2021). Influence of Cu doping on structure, morphology and optical characteristics of SnO2 thin films prepared by chemical bath deposition technique. *Optical Materials*, *117*, 111212.

[24] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4), 208-220.

[25] Lin, H., Wen, F., & Du, C. (2015). An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. *Wireless Personal Communications*, *84*, 2351-2362.

[26] Barman, S., Das, A. K., Samanta, D., Chattopadhyay, S., Rodrigues, J. J., & Park, Y. (2018). Provably secure multi-server authentication protocol using fuzzy commitment. *IEEE Access*, *6*, 38578-38594.

[27] A. A., Salim, Bakhtiar, H., Shamsudin, M. S., Aziz, M. S., Johari, A. R., & Ghoshal, S. K. (2022). Performance evaluation of rose bengal dye-decorated plasmonic gold nanoparticles-coated fiber-optic humidity sensor: A mechanism for improved sensing. *Sensors and Actuators: A. Physical*, *347*, 113943.

[28] Wang, C., Wang, D., Xu, G., & Guo, Y. (2017). A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems*, *30*(16), e3336.

[29] Waheed, S. R., Suaib, N. M., Rahim, M. S. M., Adnan, M. M., & Salim, A. A. (2021, April). Deep Learning Algorithms-based Object Detection and Localization Revisited. *Journal of Physics: Conference Series*. *1892*(1), 012001. IOP Publishing.