A Practical Mechanism for Password Change of Multiple Systems in an Organisational Setting

Ruhi Taş*[‡], Özgür Tanrıöver*

[*] Computer Engineering Department, Faculty of Engineering, Ankara University, Gölbaşı 50.yıl Yerleşkesi Bahçelievler Mah. 06830, Gölbaşı/Ankara/Turkey

[‡], Gölbaşı 50.yıl Yerleşkesi Bahçelievler Mah. 06830, Gölbaşı/Ankara/Turkey Tel: +90 312 463 3967, Fax: +90 312 463 4007, e-mail: ruhitas@yahoo.com

Abstract- Security policies force clients to frequently to change their password. This is particularly an issue for organisation with different administrations controlling applications. In this paper, we propose a functional and minimal effort verification mechanism that lessens client reliance to reset and confirmation of client for password change on multiple sites. The proposed arrangement does not require extra equipment for acquiring the new password to organisation's services. The proposed method includes utilization of a cellular telephone as a SMS based device coupled with password policy check with a citizen info web service.

Keywords- Access Protocol, Password change, Domain Controller, LDAP, Brute Force

1. Introduction

Resources accessible through the web include large number services provided by different organizations such private, open, scholastic, business and government. Every one of these service applications requires username and password. For controlling access to organization assets, for example, web servers (email, FTP and so on) and web based shopping applications require a password. While the web based system offers us numerous advantage and wellbeing and likewise there is security dangers connected with its utilization. One of the most vital difficulties is to guarantee security in these sites. Password confirmation is one of the least complex and long-term verification system over unreliable systems. It helps to authenticate clients to utilize the assets of the remote systems.

Passwords aren't completely unbreakable, but they can keep culprits from getting to access rights of your systems. The vast majority of people use simple to-recall passwords in the system situations. In any case, those feeble passwords are inclined to brute force reference attacks [1]. One-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. OTP systems take care of password security issue that can happen by rehashing the same password a few times for various times. Still, the usage of OTP systems might be expensive or need extra effort to manage it.

A related problem is with media companies which use many different applications for news production and other purposes such as FTP system, news management, electronic document management, graphics automation, advertisement management systems etc. Each of them requires different passwords for different activities. Furthermore, they change regularly, especially for sensitive exchanges; for example, managing an account, long range formal communications.

In this study, we have built up a viable and low-cost confirmation mechanism that decreases client reliance to reset and create clients' password when critical timely access is required. The proposed solution does not require additional hardware for producing new password. The proposed system involves using a mobile phone for SMS based system for password generation coupled with password policy check with a citizen info web service.

2. Background and Related Methods

Recently, many studies on cryptography and security of password administration have been conducted. A generally accepted secure login technique depends on the token or smart card. ISO/IEC 7816 is a series of International Standards specifying these smart cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the systems and the integrated circuit in the card. As a consequence of a data exchange, the card transfers data and/or changes its value [4-5]. This technique gives strong confirmation method with password verification, but it can be lost or stolen. It can be problem to carry them all times [6] OTP creation strategies; to start with, S/key strategy, second the test reaction technique, and time-synchronous strategy where the executive sets a timeframe when the password is valid [7, 8].

The OTP authentication system uses computation technique to generate a sequence of single-use passwords from a single secret. OTP tokens are usually pocket-size fobs with a small screen that displays a number. The number changes every 30 or 60 seconds, depending on how the token is configured. All the security is entirely based on a single secret that is known only by the user [9]. The user enters his user ID, PIN and the OTP to access the system. As e-commerce industry is growing rapidly, security issues become more crucial. Generally speaking, there are three types of identity authentication methods:

a. Identity authentication of something known, such as password.

b. Identity authentication of something used Object or Token, such as smart cards.

c. Identity authentication of some personal characteristics, such as fingerprint,

As of late, numerous remote confirmation systems utilizing smart cards and biometric-based client personality validation plans are proposed. For instance finger print access control systems are well known and mostly used technique [10]. Generally, biometric information is unique to each individual, this is the main advantages and differences of this systems.

Despite the fact that biometrics is viewed as a good and a safe technique, one needs to consider the disadvantages. Every biometrics application technique has shortcomings, which can bring about issues for its clients. Voice Recognition, Facial Recognition Detector, Iris Scanner & Recognition, Fingerprint reader, Veins and DNA Recognition each has specific problems. Biometrics system requires new and modern technology. Therefore, the cost for equipment is also expensive [11, 17, 18, 19].

Also, many researchers advise Light Weight Directory Access Protocol (LDAP) server password management system integration to the web server application. LDAP integration is used for managing many different integrated systems in companies, universities, e-commerce sites, such as university email service, lesson selection system, Wi-Fi networks [2, 14, 15].

In a few arrangements passwords are created by a token, an equipment token connected with the client, thus the password is not in view of the client's memory. Every time you need new token generated password. Some tokens generates password after the entering pin number. This step adds two-element verification method.

Every methodology has an alternate inconvenience or difficulty to use or need more time to adaptation process. In OTP based systems, the client must enter the new password with in fixed duration. If you failed during this period, user need to produce new one, User must follow all procedure again. This happens regularly and can be troublesome to the user. SMS based password has turned into a well-known remote verification in the world. Banking systems mostly prefers SMS as an additional step in login procedure. [16]

3. Problem Definition

The organization, where we were to implement the system, is using a wide range of application. These include email services, FTP services, news administration management programs, electronic program archive administration systems, and video editing design mechanization framework, advertisement management console and so forth. Within this setting, a user may sign in with a single sign in using one ID and password to access associated services. Or in some other setting user may sign in every application independently. This is regularly provided by utilizing the LDAP and distributed LDAP databases on servers. Currently, LDAP validation is a broadly used uniform user authentication mechanism. It is viewed of as a cross-platform system providing high accessibility [14, 15].

However, some security policies may force the users to change their password frequently. In addition, sometimes user forgets their new passwords. Because of that the users cannot use their organisations services and this can affect all chain of business systems in the organization. The users of the organization may be located anywhere in the world. Due to organizations' structure, they sometimes should be allowed to change their password without any delay in secure way.

4. Implementation Details

The essential value of our system is in its simplicity and practicality for implementation and its adaptability to other LDAP authenticated systems. Another advantage of our system is that users can freely choose and change their passwords at anytime and anywhere. Apart from the other secure login operations, this system doesn't need any extra device and investment to set up. Furthermore, numerous researches had used LDAP with Otp systems, but they didn't focus on strengthening the LDAP authentication [20,21,22]. This system strengthens LDAP authentication with the login application and can manage LDAP passwords too.

This project is implemented using web based asp.net C# programming language. The SQL server 2012 is used as the database. (Fig 1) We utilized the safe hash (SHA-1) encryption strategy for adjustment code checking and gateway served under the SHA 256 piece SSL (Secure Attachments Layer) confirmation. SSL gives a safe association between web programs and sites, permitting you to transmit private information on the web.

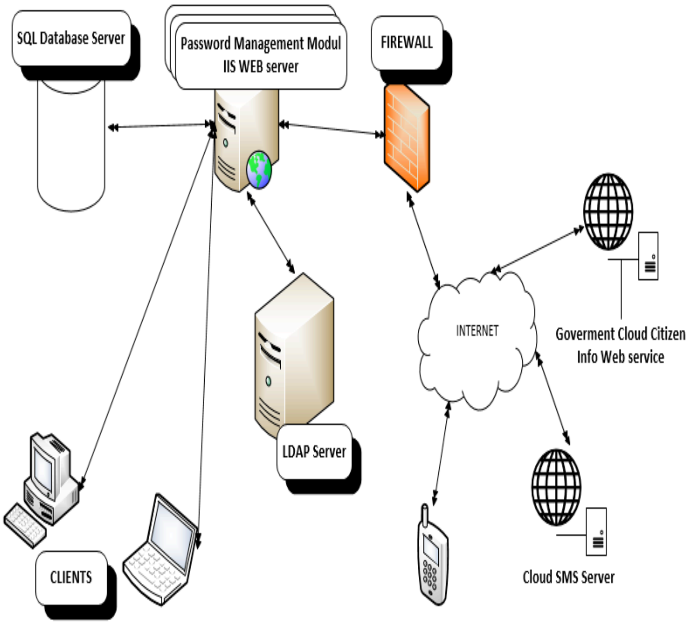
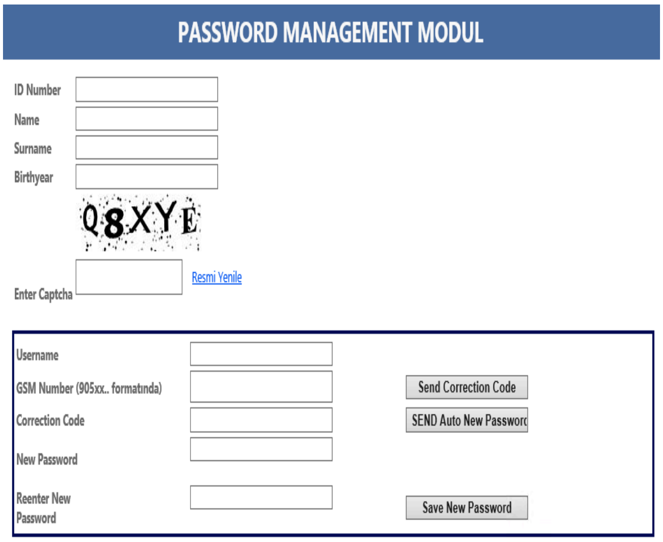


Fig. 1. Project Architecture

When user clicks the link on login page of the portal site, then user must fill information name, surname, User ID number, birth date, username and recorded GSM phone number. These information can be increased for extra information such as ID serial number, Birth place etc. , is sent to the application from this site. (Fig 2)



PASSWORD MANAGEMENT MODUL

ID Number

Name

Surname

Birthyear

Q8XYE

Enter Captcha

Resmi Yenile

Username

GSM Number (905xx.. formatında)

Correction Code

New Password

Reenter New Password

Fig. 2. Login screen (New Password Modul)

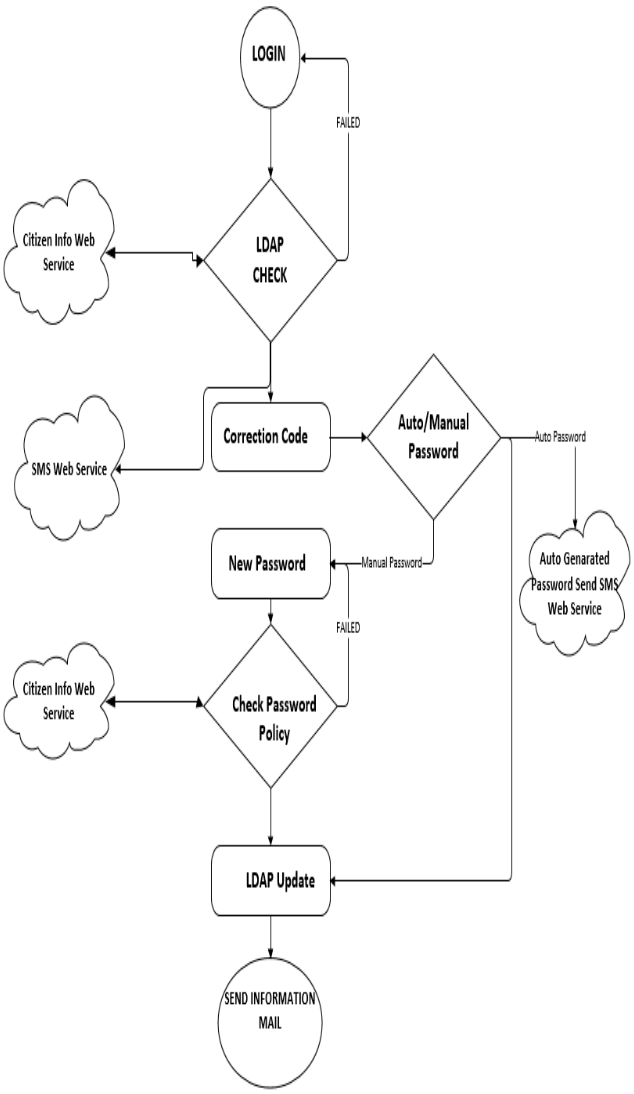


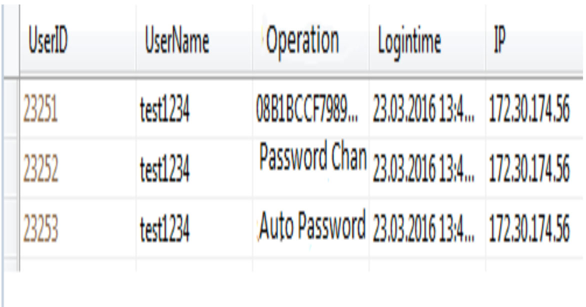
Fig. 3. Application Flowchart

The application fetches the necessary data of the user from the secure web services. (Fig 3) A Web Services is quickly rising and a popular standard in applications for sharing data over the web. Web service is a network accessible interface to application functionality, built using standard Internet technologies. [12, 13] That web service is supplied from Ministry of the Interior General Directorate of Civil Registration and Nationality. This service works as a service of cloud. The cloud computing service models is Software as a Service (SaaS) [22]. Recently many researchers are involved in cloud security, some of them advises MAC address matching [23], some of them advises intelligent systems to detect hackers activity [24] in cloud them automatically generate secure data.

There exist concerns about storage and retrieval of data securely from cloud [25], Therefore the cloud based web service we use is password protected and works only with dedicated special IP addresses of organization. The government info web services may provide various private information of a person such as citizenship number, name, date of birth etc.

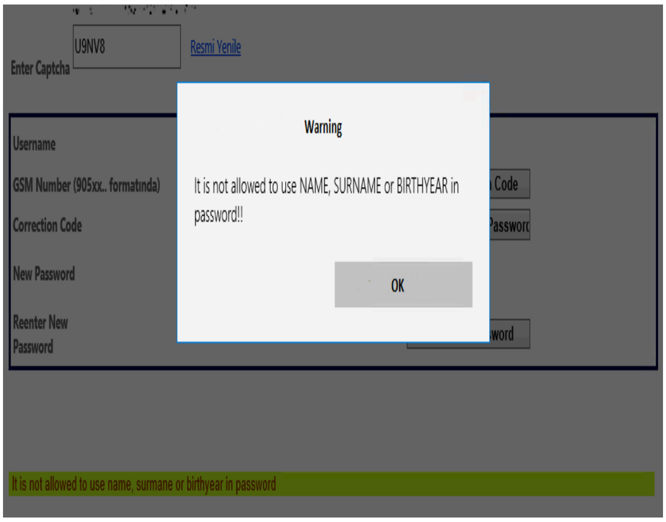
During the password check step uses LDAP and uses citizen info web services. LDAP checks user phone number and username, citizen info web services is used to check user info’s. After the passing this step, system sends correction code SMS message to the user cell phone. These codes are hashed by using the SHA-1 message. Before the applying SHA-1 encryption method, we generate unique string for each user and then apply MD5 encryption before the applying SHA-1 encryption. For consistency of hashing policy with other applications in the organisation SHA-1 has been used. But to further decrease the vulnerability a more recent encryption method such as SHA-3 could be used. (Table 1)

Table 1. Database Login History Table inputs



UserID	UserName	Operation	Logintime	IP
23251	test1234	08B1BCCF7989...	23.03.2016 13:4...	172.30.174.56
23252	test1234	Password Chan	23.03.2016 13:4...	172.30.174.56
23253	test1234	Auto Password	23.03.2016 13:4...	172.30.174.56

Application checks user information from the web services, according to user’s additional information, it is not allowed to use user related info in the password; such as name, surname, birth year etc. This check prevents user related dictionary and guess based attempts. If the user tries to enter user related info, application shows warning message about that. (Fig 4) “It is not allowed to use Name, Surname or Birth Year in the Password!!! “



Enter Captcha U9NV8 Resmi Yenile

Username

GSM Number (905xx.. formatında)

Correction Code

New Password

Reenter New Password

Warning

It is not allowed to use NAME, SURNAME or BIRTHYEAR in password!!

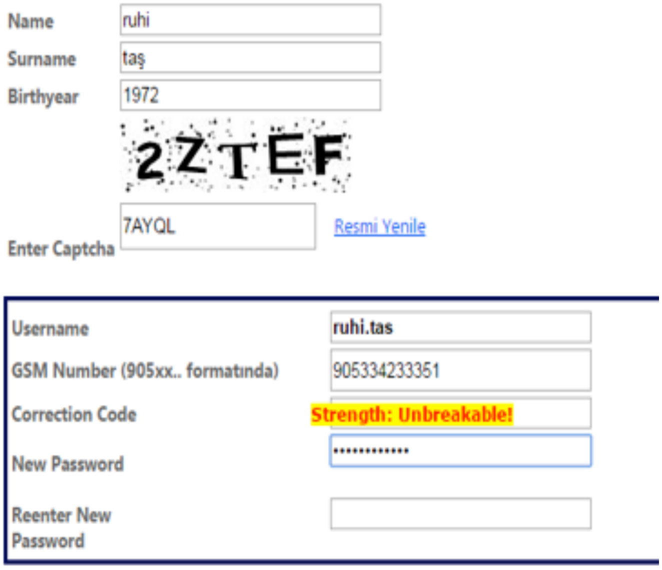
OK

It is not allowed to use name, surmane or birthyear in password

Fig. 4. Checking Password weakness and policy

Password format for the new password will meet the following criteria: Password length – default length is 8 characters, but default may be overridden by specifying a password length on the Identity key Windows Logon policy, character set – the random password will consist of the following character set: a to z A to Z 0 to 9 printable symbols - !@#%^&*()"+=-_[]\|/?<> Complexity requirements: The random password must not contain the User's User ID or parts of the User's full name that exceed two consecutive characters. The random password must contain characters from three of the four character set components listed above. Our password auto generator follows these basic rules. (Fig. 5) If the user selects auto-generated password, then the system sends the password by SMS to the user's pre-registered cell phone. (Fig. 6) During this operation, if the user's entered a GSM number not equal to the pre-registered number, user is warned.

If company needs further strengthen the security of the authentication, it is easy to increase the complexity and length of password according new security policy. The entire user related operations such as password change or phone number change operations; system sends automatic email for warning the users about this process.



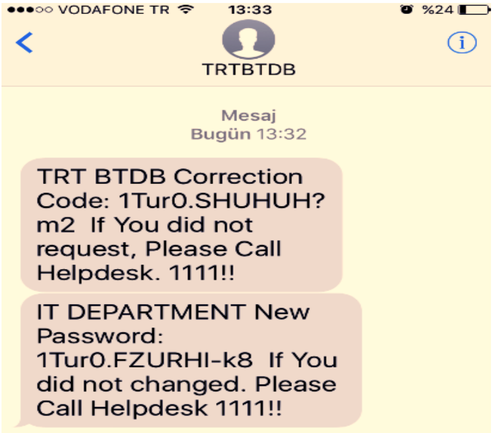
Name	ruhi
Surname	taş
Birthyear	1972
Enter Captcha	7AYQL Resmi Yenile

Username	ruhi.tas
GSM Number (905xx.. formatında)	905334233351
Correction Code	Strength: Unbreakable!
New Password	••••••••••••
Reenter New Password	

Fig. 5. Checking password weakness and policy

5. Application Analysis

While the analysing the application use periods, we realized that most users had changed their password after the working hour from 18:00 PM to 09:00 AM. (Fig 7) User password change process has been done that each hour of the day. This is critical process for organisation, because some departments are working for 24 hours a day.



Mesaj
Bugün 13:32

TRT BTDB Correction Code: 1Tur0.SHUHUH?m2 If You did not request, Please Call Helpdesk. 1111!!

IT DEPARTMENT New Password: 1Tur0.FZURHI-k8 If You did not changed. Please Call Helpdesk 1111!!

Fig. 6. Correction Code and New Password Mobile Phone SMS

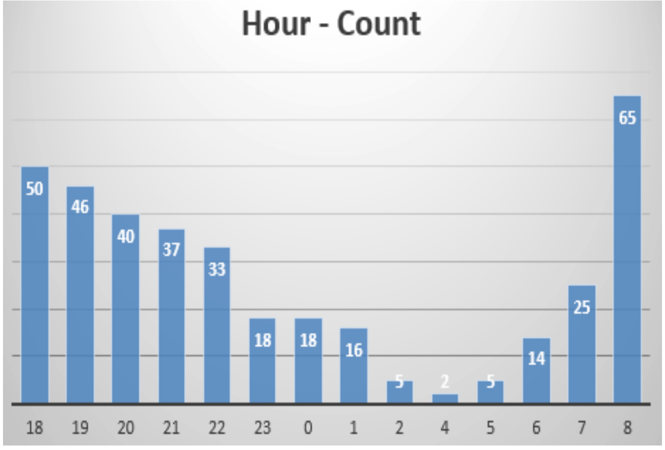


Fig 7 Usage rates after working hour

The daily analysis also showed that; users are forgetting their password in a short period after changing password and Monday is the most password-changed day of the week. The daily analysis also showed that a few users may need to change their password during the weekend, too (Fig 8). However, this may be a critical operation for continuity of work for certain organisations giving 7 day service.

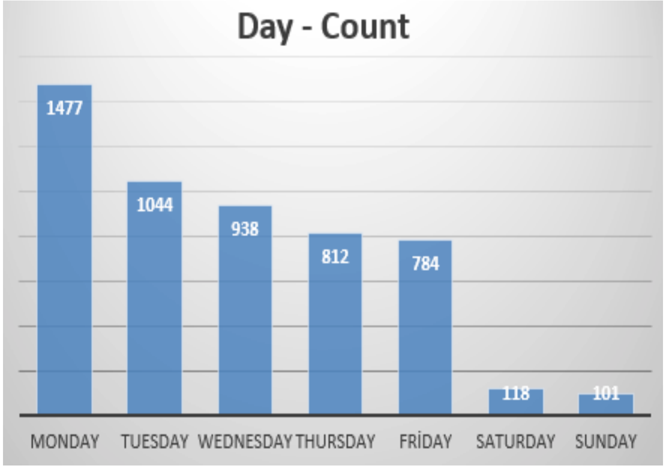


Fig 8 Usage rates on weekdays

Implemented application manages 7000 LDAP users' passwords in the organisation. After the releasing the application, during the first 2 months period, 1598 user used the system. (Changed password or phone number) 1335 password change operation are completed by users. In the 6 month period, the number of users increased to 3980 and in the next 2 month the number of users is increased to 4350 user. (Table 2)

Table 2. Password operation results

Password Change Type	Count (first 2 month)	Count (in 6 Month)	Count (in 8 month)
Auto Password Change	263	1176	1806
Mobile Password Change	12	70	119
Password Change	1062	2734	3355
Password Op. Total	1335	3980	5280
Number of Users	1598	3596	4350

Day use of the system has been shown to increase the rate day by day. Due to the holiday period more users forget the password, the system's operability rate was greater during this period. (July -986 and August - 1020)

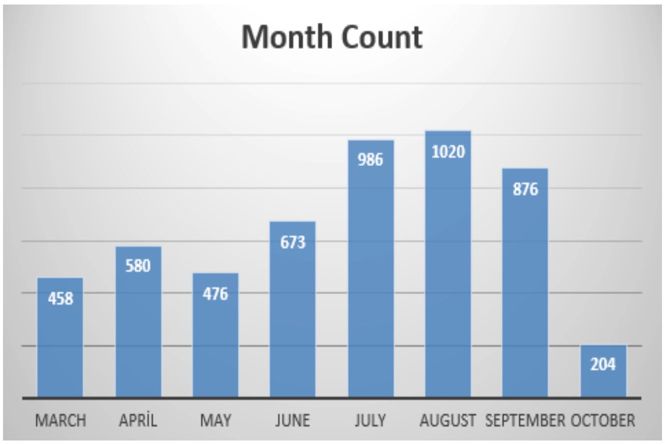


Fig 9 Usage rates on months

Main differences between with this approach and previous works; others researchers try to integrate LDAP to the other login required applications, and some of them send passwords to the clients cell phones. But none of them have any capability to check user related info in the passwords. (Table 3) Our system checks user info in passwords for overseeing brute force attacks. This citizen info is supplied by government web services.

Table 3. Systems Comparison

Properties	Our System	Other LDAP systems	Biometric Systems
LDAP Integration	yes	yes	yes
SMS	yes	some	no
Trusted user related info Password Check	yes	no	no
Strong Correction/Challenge Code	yes	some	yes
Easy Implementation	yes	yes	no
Special Device Requirement	no	no	yes
Adaptation Duration	short	short	long

6. Conclusion

In this paper, we have proposed another password verification system less vulnerable to brute force attacks associated with LDAP combination. This methodology proposes a compelling confirmation framework, which robustly and effectively set new LDAP passwords with sending over GSM system. Particularly issue of strong client password is achieved, which is normally weak in most other applications. This framework warns clients about the shortcoming of password and not permits to utilize predictable client related password. This method also decreased IT costs because of lower number of IT help center calls about password change request. This mechanism can be utilized for strengthinig the login of online applications utilized as a part of the organisations. It can be adjusted to use with different security frameworks' login modules as well.

References

[1] E. Sediyono, K I. Santoso and JL I. Bardjo, "Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS", Proceedings of the Advances in Computing, Communications and Informatics, Mysore, USA, pp. 1604 – 1608, 22-25 Aug. 2013. (Conference Paper)

[2] E. Jamhour, "Distributed security management using LDAP directories", Computer Science Society SCCC '01. Proceedings. XXI Internatinal Conference of the Chilean, Punta Arenas, Chile, pp. 144 - 153, 07-09 November 2001. (Conference Paper)

[3] M. Long and U. Blumenthal, "Manageable One-Time Password for Consumer Applications", Internationla Conference Consumer Electronics, Digest of Technical Papers. , Las Vegas, USA pp 1-2, 10-14 January. 2007. (Conference Paper)

[4] International Standard ISO/IEC 7816-3 Third edition 2006, https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-3:ed-3:v1:en (Standards) Latest Access Time for the website is 21 July 2016.

[5] H.C. Kim, H.W. Lee, K.S Lee and M.S Jun, "A Design of One-Time Password Mechanism using Public Key Infrastructure", Proceedings of Fouth International Conference the Networked Computing and Advanced Information Management, Gyeongju, , South Korea, vol.1, pp. 18 – 24, 2-4 September. 2008. (Conference Paper)

[6] D.G. Shin and M.S Jun, "Micro-payment system using OTP for customer's anonymous", Proceedings of the International Conference Information Science and Applications, Jeju, South Korea, pp. 1-5, 2011. (Conference Paper)

[7] H. Wang, C Fan, S. Yang J Zou and X Zhang, "A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP)", 7th International Conference Wireless Communications, Networking and Mobile Computing, Wuhan,China pp. 1-4, 23-25 Sept.ember 2011. (Conference Paper)

[8] Nail M. Haller "The S/KEY One-Time Password System" Proceedings of the. Internet Society Symposium on Network and Distributed System Security, San Diego, USA, pp.151-158, Feburary 1994. (Conference Paper)

[9] G Jaspher W Kathrine E Kirubakaran and P. Prakash, "Smart card based Remote User Authentication Schemes: A Survey", Proceedings of the International Conference on Modelling Optimization and Computing, Coimbatore, India, pp. 1 – 5, 26-28 July 2012. (Conference Paper)

[10] PBworks, "Advantages and Disadvantages of technologies",http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies , Latest Access Time for the website is 15 May 2017

[11] J. P. Kumar, S. Umar, C. S. Harsha and B. Nagasai "A Study on Web Services Security", International Journal of Computer Science Engineering and Technology, Vol 4, No. 7, pp. 235-237, July 2014. (Article)

[12] Y. Hu and H. Wang, "Constraints in Web Services Composition", Proceedings of 4th International Conference Wireless Communications, Networking and Mobile Computing, Dalian, China, pp. 1-4, 12-14 Oct.ober 2008. (Conference Paper)

[13] Y He, J. Li and H. Tang, “Research of Heterogeneous Authentication Information Synchronization Based on LDAP and Web Service”, Proceedings of International Symposium on the Computational Intelligence and Design, Hangzhou, China Vol. 2, pp. 52 – 55, 29-31 October 2010. (Conference Paper)

[14] R. F. Sari and S. Hidayat, “Integrating Web Server Applications With LDAP Authentication: Case Study on Human Resources Information System of UI”, Proceedings of the International Symposium on Communications and Information Technologies, Bangkok, Thailand, pp. 307 – 312, 18-20 Octoper 2006. (Conference Paper)

[15] M. K. Ibrahim and W. Z. Ameen, “Secure SMS System for E-Commerce Applications”, International Journal of Computer Science Engineering and Technology, Vol. 4, No. 4, pp. 137-142, June 2014. (Article)

[16] E. Liao, C.C Lee, M.-S. Hwang and E Liao “A password authentication scheme over insecure networks”, Journal of Computer and System Sciences, Vol. 72, Issue 4, pp. 727–740, 2006. (Article)

[17] F. Monrose and A. D. Rubin, “Keystroke dynamics as a biometric for authentication”, Future Generation Computer Systems, Vol. 16, No. 4, pp. 351–359, February 2000. (Article)

[18] D. Shanmugapriya and G. Padmavathi, “A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges”, International Journal of Computer Science and Information Security, Vol. 5, No. 1, September, 2009. (Article)

[19] C. S. Yang, C. Y. Liu, J. H. Chen and C. Y. Sung, ”Design and implementation of secure Web-based LDAP management system”, Information Networking, Proceedings. 15th International Conference, Beppu, Japan, pp. 259 – 264, 31 January - 02 February 2001. (Conference Paper)

[20] M A. Thakur and R. Gaikwad, “User identity & lifecycle management using LDAP directory server on distributed network”, Proceedings of the International Conference Pervasive Computing, Pune, India, pp. 1-3, 8-10 January 2015. (Conference Paper)

[21] Y. Guo, C. X. Shen and Z. Han, ”A LDAP synchronization model based on Trusted Computing”, International Conference on Machine Learning and Cybernetics, Boading, China, pp. 2771 – 2774, 12-15 July 2009. (Conference Paper)

[22] S. K. Mandal and F. Basith, “Enhanced Security Framework to Ensure Data Security in Cloud Using Security Blanked Algorithm”, International Journal of Engineering and Technology, pp. 225 – 229, Vol 02, No.4, October 2013 (Article)

[23] H. V. Taiwade, “Enhanced Security Mechanisms for Cloud Computing” International Journal of Advanced Research in Computer Sicence and Software Enginering, pp. 564 - 567 Vol. 5, No. 7, July 2015 (Article)

[24] B. Balusamy, P. Venkatakrishna, G. Palani and U. Ravikumar, “An Intelligent Cloud Security System for Critical Applications”, Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, pp. 33- 40, 2015 (Article)

[25] Balamurugan, B., and P. Venkata Krishna. "An Enhanced Security Framework for a Cloud Application." Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, pp. 825-836, 2015 (Article)