Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 1, July 2020, pp. 485~491
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i1.pp485-491

E-PAC: efficient password authentication code based RMPN method and diffie-hellman algorithm

Salah H. Abbdal Refish[1], Salam Waley Shneen[2]
[1]Department of Computer Emgineering, Al-sadiq University, Iraq
[2]Energy and Renewable Energies Technology Center, University of Technology, Iraq

Article Info

Article history:

Received Jul 21, 2019
Revised Nov 26, 2019
Accepted Jan 14, 2020

Keywords:

Diffie-hellman
Mutual authentication
Password authentication code
RMPN

ABSTRACT

Users need more efficient and more secure when they use the Internet. Password authentication code (PAC) is the critical issue in many applications such as web-sites and data base systems etc. In this paper, PAC between two users to confirm authentication between them based two factors has presented. Two factors is the most good solution in this field. A legitimate user needs to make sure about his partner to ensure their communication. So, this solution produces two important algorithms, the first one is utilized the Diffie-Hellman which considered the base of this work. The second is routing in message passing networks (RMPN) algorithm which determine the positions of bits which sent to specific party. The overall of this method convincingly to be more secure against both online and offline attacks. This scheme has some advantages such as secrecy of session key, password privacy, and mutual authentication. The performance and security analyses prove that the scheme is very efficient and mathematically immune for attackers.

Corresponding Author:

Salah H. Abbdal Refish,
Department of Computer Engineering,
Al-Sadiq University, Najaf, Iraq.
Email: manatheraa@yahoo.com

1. INTRODUCTION

One of the most techniques is PAC which is a phrase that gives a permission to the user for accessing more resources of computer such as messages, programs, files, etc. This method used to distinguish the unauthorized user do not allow to access a specific resources. When the users used the internet applications so the password should be top secret key that nobody could guess [1]. Many users use password that is very easy and restricted alphanumeric such as their phone numbers and names [2]. Main one drawback in the design of password schemes is that password lengths are usually short. Thus, a password authentication system and the method thereof are disclosed [3]. Most methods used hybrid password which involves shape and text [4-7]. These methods add the complexity on the schemes according to the user-side. The advantage of short length password is that it is easy to be remembered by the users. But this feature still is a problem since it easier for attackers.

Later on, various password based schemes have been introduced by researchers for diverse applications [8-16]. Therefore, researchers introduced such authentication scheme that utilized two-factor approach in order to offer more safety. 2-Factor Authentication (2FA) is a very suitable with principles of user authentication. A user-a sends his password to the user-b for authentication. The user-b asks the user-a to send his second factor when it ensures from matching of user-a password with a user-b. The user-a gains permit to reach a user-b resources when his first factor and his second factor have validity in the user-b [17].

Biometric methods achieved in some papers [18, 19] to confirm the user identity by concluding biometric features such as finger print, iris, .etc. Although, these schemes use unique biometrics features and

make the systems more secure. However, these techniques are limited due to require additional overheads (devices and time). Our method do not need to use biometrics features compared with other systems to avoid the overhead which mentioned above. A lot of applications such as (PIN personal identification number, ATM automated teller machine suffering from the attacks which may occur. This is why many banks warnings the customers when they deal with such these systems. These systems are not safe since they can be attacked by other parties. This research develops PAC-RMPN paper to be more efficient and to be more secure.

Our suggestion is that the short number is very easy to use and remember, but we should find a method to protect this password from expected eavesdropping. So, one solution is presented in this paper, when the password is used only once for each session. Additionally, to be the scheme more secure should be applying the mutual authentication between the users for getting the authorized users by using Diffie-Hellman as well as, combination password with RMPN which is a one-time method to secure the password. In RMPN, the routing is the way to determine the path over the network. This path help us to reach the destination [20].

In the third section, we explain in details how the RMPN works to generate path which consists of some digits to determine the bits that used in my scheme. This method is new and secure without need to hide the password since it can be changed. The contributions of this paper can be summarized in the following points:

a) Uses the simple password doesn't effect on the scheme since this method maintains the privacy of passwords of users.
b) Decrease the opportunities of the attackers to compromise users, since the other side computes password of the user independently and unique from others.
c) Applying mutual authentication to make the scheme more secure for accessing the authorized users only.

2. EXISTING PROBLEM

Password is very important issue in many applications related to the websites and some applications. This password should prevent illegal users when the users deal with their data over internet. The users when visit different websites they use the same credentials. However, these credentials may be compromised since their data has stored by websites. In other words, any attacker try to get credential which belong to the users, surly he can involve it for other websites [21, 22]. This reason why the users using various passwords for diverse websites. Many papers focused about this problem and they try to get a good solutions to avoid these risks [23]. One solution is password authentication code based RMPN. But it still vulnerable and a malicious users. So, we should get another way for this password to be more immune and secure opposite of attackers.

3. PROPOSED SCHEME

3.1. Structure of the scheme

At the first, and user-1 before types his password, the user-1 and user-2 will agree about the following via secrete channel according to Diffie-Hellman method [24]:

a) Primary number q.
b) Integer primary number according to q which is α.

User-1 chooses $xa < q$ as integer random number. Then, the user-1 will computes: $Ya = q^{xa} \bmod q$. Then sends (Ya) to user-b. When the user-2 receives this value and also he chooses integer random number $xb < q$ he computes: $Yb = q^{xb} \bmod q$, $h(Kb=Ya^{xb} \bmod q)$ and then sends ($h(Kb=Ya^{xb} \bmod q)$, Yb)) to the user-1. Now, user-1 computes: $h(Ka=Yb^{xa}.mod\ q)$ If the $h(Ka=Yb^{xa}.\ mod\ q)=h(Kb=Ya^{xb}\ mod\ q)$ so the first authenticated is applied and go to the next step, otherwise, stop the password authentication.

In next step, RMPN is an important algorithm to determine the path which used in my method, so we should explain this algorithm to be more clear to the reader. This work can be described as follows: the user---i (U_i) generates a simple password which consists of six digits (0-9) during the login stage. Upon receiving the password, the U_j does some processes on this password based RMPN to generate new value and sends it to the U_i for comparing it with his value to confirm the U_j is not impersonate.

In message passing network the routing is the way to determine the path over the network. This path help us to reach the destination. Here in my method, the path taken by the password of the U_1 depending on the RMPN algorithm. The example bellow explains how the RMPN works and how can get the path [20]. General RMPN idea is explained in Figure 1.

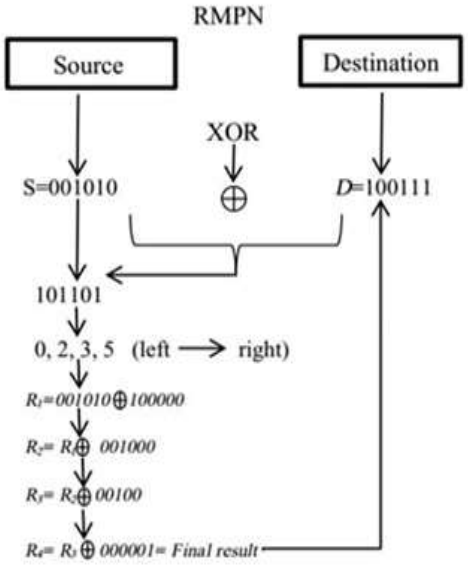

Figure 1. General idea of RMPN

For instance, S=S5,S4,……,S1,S0 denoted to the source node, and the D=D5,D4,…..,D1,D0 denoted to the destination node. The first step in this algorithm is the apply XOR operation on the Source S and destination D using six digits, R=S(+)D to get the result R which represents the digits of the path that determined to reach the destination D. For example, the source S=10 that is mean in binary number 001010 and D=39 which represent 100111 in binary number. So, the result *R* will be 101101 that is mean in this algorithm the message should be sent to the D dimensions 0, 2, 3, and 5 to reach the destination D. So, the operations bellow determine the route according to the dimensions of D destination.

3.2. Details of the results above

10(001010) XOR with the binary number of 5 digit from the path above, so

001010 (+) 100000 where the fifth digit should be 1 and the rest are 0. After that the result XOR with binary number of 3 so, the operation will be

101010 (+) 001000 and so on. Note that the order of the binary number according to the concluded path will be start with 0. So the results will be as follows:

001010 (+) 100000 the result is 101010, where 001010=10, and 100000 for 5 digit, here the algorithm put 1 just for five digit as a binary number consists of 6 digits.

101010 (+) 001000 for 3 digit, the last digit in the path is o which will be in the six binary number is 000001 and the final result is 100111. Table 1 describes the equations with the operations depending on the position of digits.

The common notations in Table 2 will be used to explain the symbols in the Figure 3. It is very important to explain this method structure with two components, the first one is User---1 (U_1) and the second is User---2 (U_2). U_1 uses simple password *PWD* consists of 6 digits where ($0 \leq PWD \leq 9$) without using any further features. The block diagram which is used in this scheme to determine digits path shown in Figure 2.

Table 1. Describe the equations of RMPN

Equation	Operation with the Position of digit
R_1=001010	XOR the *S* with The fifth
(+)100000	position
R_2= R_1 (+)001000	XOR the R_1 with The third position
R3= R2(+)000100	XOR the R2 with The second position
R4= R3(+)000001	XOR the R3 with The first position

Table 2. Notifications of Figure 3

Symbol	Definition
U_1	The user 1
U_2	The user 1
PWD	Password of U_1
FR	The final result after xor-ing the values

Then, XOR the R_1 with R_2 to get R_3 and XOR R_3 with the result of R_4 and so on, to get the final R_n which sent to the U_1 to prove the password authentication code. In the next subsection bellow I describe the method in details.

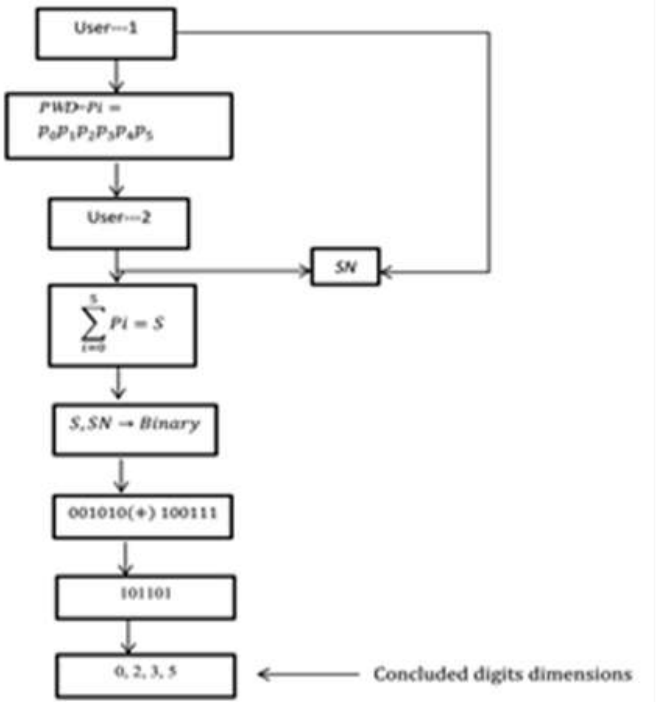

Figure 2. Block diagram to determine digits path

3.3. Analysis of the scheme

When the user---1 (u_1) enter the password: 0 0 8 0 2 0. The user---2 (u_2) do the *SUM* operation on the password which entered by u_1. After that, u_2 converts the decimal number to 6-bits binary number. So, the 6-bits of 10 decimal number is 001010. I used the *S=001010* and the *SN* is *100111*. The next step is to XOR *(S* With *SN):*R_1*=S (+) SN* (applying RMPN).

R_1=101101 (1)

As (RMPN) I take the positions which have the one's only. So, (5, 3, 2, 0 from left to right) are the bits which used in this method to complete the algorithm for securing the password as follows:

001010 (+) 100000=101010 (2)

101010 (+) 001000=100010 (3)

100010 (+) 000100=100110 (4)

100110 (+) 000001=100111 (5)

After that:

(2) XOR (3): R2=101010 (+)100010=001000 (6)

(6) XOR (4): R_3=001000 (+) 100110=101110 (7)

(7) XOR (5): R_4=101110 (+)100111=001001 (8)

Finally, XOR R_4 with R_1: 001001 (+)101101=100100 (9)

The final result is: (*FR*= 100100)

The u_2 will apply hash algorithm [14] to hash *FR* and then sends hashed code *h(HFR|| h(Kb=Ya*^{xb} *mod q)*) to the u_1. The u_1 apply this algorithm to confirm the u_2 is second authenticated or not (Figure 3).

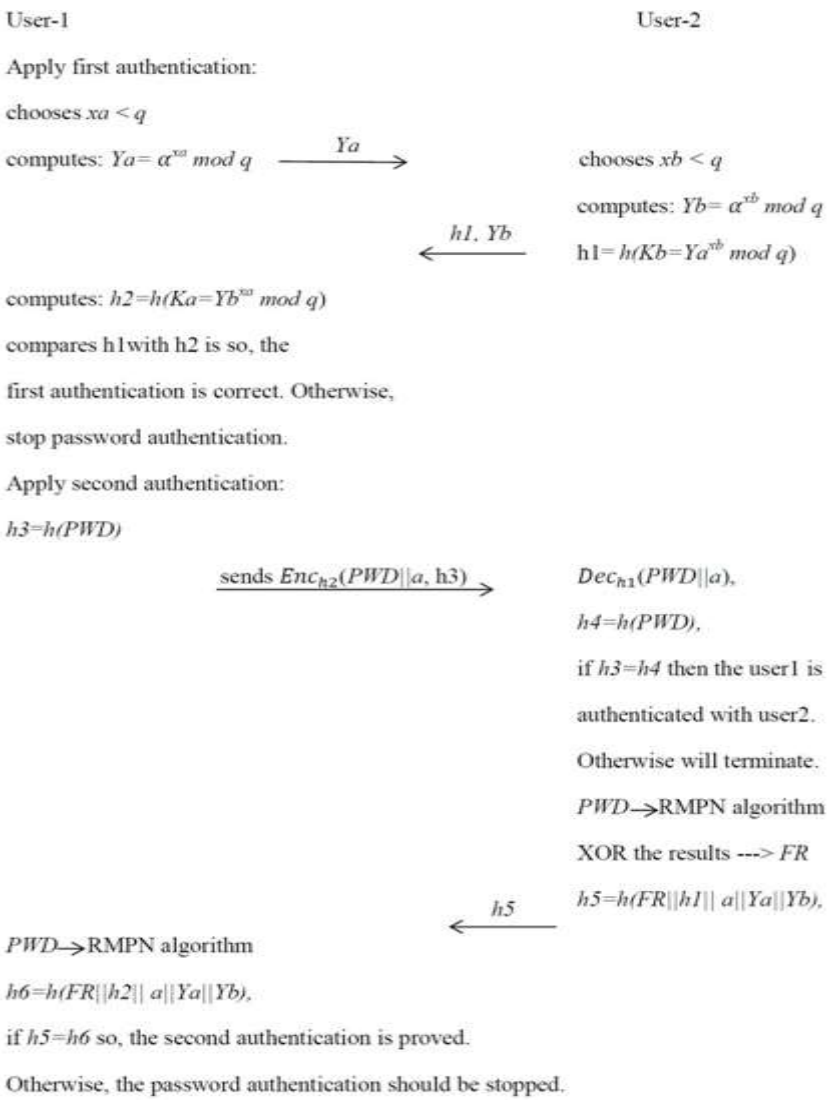

Figure 3. E-PAC structure

4. SECURITY ANALUSIS

In this section, the security features are supported in this scheme as follows:

4.1. Mutual authentication

Means that an attacker cannot impersonate the actual U_i. In this work, two factors used as authentication between U_i and U_j. Additionally, an attacker is not able to conclude (*HFR*). This is unforgeability because it uses a hash function. (A hash function can be involved to uniquely generate secure data. The hash function is collision-resistant, which means that it is very difficult to get information that will compute the same hash value. Authentication of U_i to U_j is by using the shared key (*sn*), therefore an attacker cannot learn the secret key between U_i and U_j. As well as, an attacker cannot get (r_i), that should be equal to (*FR*). Here, there are two steps for authentication. The first one will be prove as follows:

$Yb^{xa} \bmod q = Ya^{xb} \bmod q$?

$(\alpha^{xb} \bmod q)^{xa} \bmod q =$

$(\alpha^{xb})^{xa} \bmod q =$

$\alpha^{xbxa} \bmod q =$

$(\alpha^{xa})^{xb} \bmod q =$

$(\alpha^{xa} \bmod q)^{xb} \bmod q = Ya^{xb} \bmod q$

And the second authentication is the value of *HFR* will be hashed with the value of the *Uj* which is $h(Kb=Ya^{xb} \bmod q)$.

4.2. MITM (Man-In-The-Middle) attack

This attack indicates that an attacker can able to intercept the message between the users. After that, this attacker replaces this message with his own message. The attacker use this attack when the user signs out the applications. In my method, the value which sent to the user is secure since applying hash function on the generated value. Computing the r_i is through the generation data (R_1, R_2, ……, R_9) after getting it from the specific positions r_i. These selected data becomes useless when U_i signs off the application. So, an attacker spotting communication between U_i and U_j cannot know r_i which are used only once after applying RMPN; thus he is not able to compute *FR*. Nevertheless, when U_i signs out the application, an attacker couldn't generate both factors to impersonate the actual user. So, our scheme can resist MITM.

4.3. Our method hinder the replay and dictionary attacks

In the authentication process, U_j generates the hash value for the each passwords logged. The values of *sn* and r_i make our scheme more secure because it is known only by U_j and U_i. The *sn* and r_i values are used to prevent the dictionary attacks since it uses one time for each authentication process. In the final step of authentication process, U_j sends *HFR* to U_i for avoiding the replay attack. So, when U_i computes *HFR* which will be hashed with the value of the *Uj* ($h(Kb=Ya^{xb} \bmod q)$) and compares it with his secret *HFR* he will know the U_j is authenticated or not.

5. PERFORMACE SCHEME

This work has tested to know the efficiency of our method. The differences of performance for scheme [1] and E-PAC as shown in the Figure 4 and Figure 5. Additionally, the average time for the authentication processes in this method is equal to 0.022319 seconds for each user compares with the last one which is equal to 0.005282 that refer to high speed and the difference is very little.

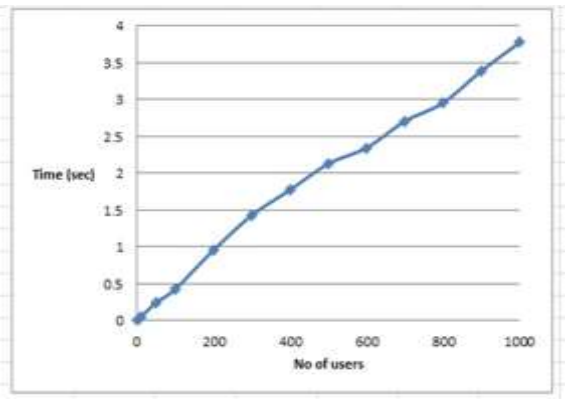

Figure 4. Performance of old proposal [1]

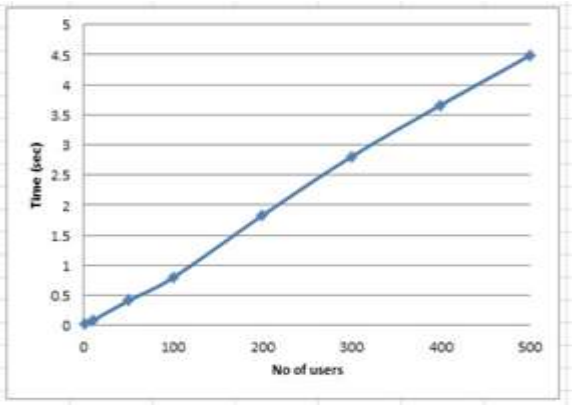

Figure 5. Performance of new E-PAC proposal

6. CONCLUSION

Efficient Password Authentication Code (E-PAC) is an approach assists to distinguish the unauthorized users do not allow to access a restricted resources such as printers, programs, files,…, etc. The password should be secret key that no one could guess. In this paper, a one solution to the era long problem password Authentication at incoming level is presented. E-PAC based RMPN and Diffie-Hellman is a new method to secure the password. RMPN determines the positions of bits which sent to reach the destination D. Our method regenerates a new code each authentication session based RMPN and Diffie-Helman that is convincingly more secure against both online and offline attacks. This technique makes the user to be free-worry about his short password since the return value is hashed code based two-factors. This method introduced for one time password authentication system. The scheme is protected from different attackers. Two factors and encrypted password presented in this work for preventing more attackers and to be more secure.

REFERENCES

[1] S. Refish, "*PAC-RMPN: Password Authentication Code Based RMPN*," Proc. of the IEEE International Conference on Advanced Science and Engineering (ICOASE), Dhoke, Iraq, pp. 286-289, 2018.

[2] A. E. Omolara, et al., "Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication," *International Journal of Electrical & Computer Engineering*, vol. 9, no. 3, 2019.

[3] A. Al Farawn, et al., "Secured e-payment system based on automated authentication data and iterated salted hash algorithm," *International Journal of Power Electronics and Drive System (IJPEDS)*, vol. 11, no. 1, pp. 302-308, Mar 2020.

[4] H. E. Harianto and D. Gunawan, "Wi-Fi password stealing program using USB rubber ducky," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 2, 2019.

[5] S. Nagaraj, et al., "A Bio-Crypto Protocol for Password Protection Using ECC," *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 1, pp. 67-72, 2015.

[6] P. Wanda and H. J. Jie, "Efficient Data Security for Mobile Instant Messenger," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 16, no. 3, 2018.

[7] H. Gao, et al., "*YAGP: Yet another graphical password strategy*," in Annual Computer Security Applications Conference, pp. 121-129, 2008.

[8] D. Z. Sun, et al., "Improvements of Juang's password-authenticated key agreement scheme using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 6, pp. 2284-2291, 2009.

[9] R. Lu, et al., "A dynamic privacy-preserving key management scheme for location-based services in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127-139, 2012.

[10] D. Zhao, et al., "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247-269, 2014.

[11] Y. Lu, et al., "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *Journal of medical systems*, vol. 39, no. 3, pp. 1-8, 2015.

[12] D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816-823, 2015.

[13] M. S. Farash and M. A. Attari, "An anonymous and untraceable password-based authentication scheme for session initiation protocol using smart cards," *International Journal of Communication Systems*, vol. 29, no. 13, pp. 1956-1967, 2016.

[14] A. Irshad, et al., "A single round-trip sip authentication scheme for voice over internet protocol using smart card," *Multimedia Tools and Applications*, vol. 74, no. 11, pp. 3967-3984, 2015.

[15] L. Wu, et al., "Efficient and anonymous authentication scheme for wireless body area networks," *Journal of Medical Systems*, vol. 40, no. 6, pp. 1-12, 2016.

[16] C. Jin, et al., "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," *Journal of Medical Systems*, vol. 40, no. 1, pp. 1-6, 2015.

[17] A. A. Yassin, et al., "*A Practical Privacypreserving Password authentication Scheme for Cloud Computing*," Proc. of the IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12), Shanghai, China, pp. 1204-1211, May 2012.

[18] A. Jain and L. Hong, "On-line fingerprint verification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, pp. 302-314, 1997.

[19] A. A. Yassin, et al., "Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing," *Proc.of the IEEE Second International Conference on Cloud and Green Computing*, Xiangtan, Hunan, China, pp. 282-289, 2012.

[20] A. Y. Zomaya, "Wiley series on parallel and distributed computing," Series editor.

[21] S. Kumar M. and V. Mathivanan, "NFC Secured Offline Password Storage," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 3, pp. 730-732, Dec 2017.

[22] S. H. Refish, et al., "Ensuring Data Integrity Scheme Based on Digital Signature and Iris Features in Cloud," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 2, no. 2, pp. 452-460, May 2016.

[23] B. U. I. Khan, et al., "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 832-842, Nov 2018.

[24] W. Stallings, "Cryptography and Network Security Principles and Practices," Fourth Edition, Publisher: Prentice Hall, 2005.