TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. x, No. x, April 2013, pp. 1 ∼ 10
DOI: 10.11591/telkomnika.vXiY.abcd

Implementation of Multi-Factor Authentication Method to Minimize RFID Duplication.

Ayu Anggara* **and M. Yusril Helmi Setyawan**
Applied Bachelor Program of Informatics Engineering, Politeknik Pos Indonesia
Bandung Indonesia, Phone. 022-2009562, 2009570 Fax. 022-2009568
*Ayu Anggara, e-mail: ayuanggaraspentwo@gmail.com

Abstract

RFID technology is an automatic wireless identification system that works with the help of active and passive cards as well as with the reader. The use of unique numbers inside RFID tags is very useful as the identity of an object or as a tracking device. As for weaknesses in RFID systems, it is possible to cloning identification data. Therefore it is necessary to increase security to minimize it. Authentication is the process of user verification. The most common form of Authentication is single-factor Authentication, which requires only one factor for users to log in to the system. This model is weak and can cause harm to those who use it. Therefore Multi-factor Authentication is required that is the way to authenticate users by using multiple layers of Authentication program. The factor to be used in this report is to use One-Time Password. With the system with several steps of this authentication can also minimize the fraud that will occur. As the proxy case absent and minimize the occurrence of duplication of RFID card

Keywords: RFID, Multi-Factor Authentication, One-Time Password, Duplication

1. Introduction

At present, Many industries today are using Radio Frequency Identification (RFID) technology [1], RFID applies in applications such as attendance logging applications [2], warehouse management [3], library [4], object tracking [5], and others. RFID can create objects of "talking" technology, so RFID technology in key technologies from perceptual perception layer positions is very prominent [6]. RFID has several advantages over the traditional identification technologies. RFID does not require random tracks for communication and RFID tags can be read more [7]. RFID is relatively fast, and many tags can read simultaneously. The RFID system consists of RFID tags, RFID reader and PC [8]. Each of RFID tag has a unique ID that corresponds to some useful information (e.g. product, tracking, and position information), from unique ID and position information, users can quickly identify RFID tag locations [9].

While RFID widely use, it is important to note that RFID has weaknesses. The weakness in RFID systems is that it is possible to clone identification data [10]. Cloning attacks make the application unsafe because it duplicates the original tags so that it threatens RFID applications that use tag authenticity to validate objects [11]. This cloning attack can result in financial loss to users [12], [13].

Therefore, to improve system security and minimise duplication in RFID system in this research will apply Multi-Factor Authentication (MFA) method. MFA is a way to authenticate users by using multiple layers of the Authentication program. This is a secure means of authentication that can effectively prevent identity theft [14]. In addition, using this method will be slavish in tracking the precision of the calculation of the tracking results [15]. The factor in this report is using One-Time Password (OTP). Thus, the existence of a system with some authentication steps can minimise the fraud and duplication that will occur [16].

Received May 9, 201x; Revised August 3, 201x; Accepted August 16, 201x

2. RelatedWork

Applications that use Radio Frequency Identification (RFID) are increasing today and are seen applicable in areas such as material flow discharge, quality assurance [17], production control [18], [19], cold chain logistics tracking [20], objects in place of find [21]. RFID consists of two important parts of the RFID reader (combination of transceiver and antenna) and RFID tags (composed of unique numbers). The RFID tag is used to store important data from the observer while the reader is used to read the data stored in the tag. This technology has the advantage of data transfer that is contactless and able to work in every environment [22]. RFID is one of the wireless technologies that use electromagnetic signal detection as identification [23]. Frequencies used in RFID consist of various types of frequencies such as low frequency, high frequency, ultra high frequency, and microwave [24]. In particular, referring to the process tracer category of the process, researchers mainly focus on manufacturing, production logistics, inventory, and supply chain. At an in-place level, RFID improves real-time data retrieval and fuses for process visibility. Propose a formal RFID-based deduction model to monitor changes in the flow of time-sensitive materials in the workshop [25]. Most existing cloning detection protocols are suitable for recognisable systems, requiring knowledge of tag IDs. Such protocols to recognise IDs before detecting which IDs are related to the cloning tag and focus only on the RFID supply chain; they collect IDs from supply chain partners and detect cloned attacks when the IDs appear simultaneously in different places [26].

Authentication is one of the critical aspects of securing applications and systems. During the authentication process, Biometric and RFID are validation factors for verifying user identity [10], Combining user location with username and password as Multi-Factor Authentication (MFA) system to make authentication more secure [27]. For secure authentication of e-voting systems using cryptographic and fingerprint IC and FTP MFA techniques [28], Schemes using cryptography and Android enhance security, convenience, flexibility, storage efficiency and MFA performance [14]. Using a phrase-based MFA framework to make resources on the cloud safer [29]. By implementing several MFAs on the mobile cloud, it is possible to know the feasibility of applying the method [30]. Hardware authentication with Fingerprint and Smartphone [31], as well as a combination of passwords with hybrid profiles of user behaviour with a great combination of host-based features, are also to keep user data secure [32]. Utilization of MFA to minimise fraud attendance data such as using face-recognising [33], Cloud verification system that combines biometric factors and Passwords to achieve high levels of security [34]. User database on API device information that can provide that information to web applications [35]. The MFA architecture utilises Identity Federation and Single-Sign-On technologies, for the modular integration of the authentication factor [36]. Authentication security is assured because of the nature of the hash function, the combination of secret vital methods and the method of creating a one-time token [37]. Merging NFC and One Time Password (OTP) methods to improve system security and eliminate attendance cheating [16]. NFC-based MFA systems have better security advantages with a simple login process [38].

Based on previous research, this research will do the design to improve the security of existing attendance system. The design will use Radio Frequency Identification (RFID) card as a tool of attendance by applying Multi-Factor Authentication method. MFA is a way to authenticate users by using multiple layers of authentication programs. One example is to use OTP (One-Time Password). OTP send to each user's mobile device; this OTP is only valid for one login session or transaction and, each user has a different OTP. Thus, using the MFA and OTP method can minimise the occurrence of fraud or duplication of attendance records system.

3. Research Method

In this study, the researchers combine the application of RFID and OTP (One-Time Password) authentication algorithm to achieve reliable Multi-Factor Authentication (MFA) method technique.

3.1. Multi-Factor Authentication

Multi-factor authentication (MFA) is a security approach for using more than one authentication tool from the available independent credentials to verify users. Multi-factor authentication combines two or more layers of the Authentication program: what users know (keywords), what users have (security tokens) and (biometric verification) [28]. The purpose of the MFA is to create layered defences and make it more difficult for unauthorised people to access targets such as physical locations, computing devices, networks or databases. If one factor is compromised or damaged, the attacker still has at least one more barrier to be broken before successfully breaking the target. This is widely known as the most secure method for authenticating access to data or applications [36].

3.2. One-Time Password

One-Time Password (OTP) is an automatically generated numeric or alphanumeric string that authenticates a user for a single transaction or session [39]. OTP is more secure than a fixed password, especially user-generated passwords, which may be vulnerable to attack after a period. OTPs may override authentication login information or may use in addition to adding other security layers. OTP can be synchronised or based on mathematical algorithms, OTPs synchronise to a more well-known type. For time synchronised OTPs, tokens are usually pocket-sized fobs with small screens displaying numbers. The number changes every time depending on the configuration of the token [16].

3.3. Authentication Process

The Authentication process in the application of the entire authentication system divides into two parts namely part (IN) and (OUT):

3.3.1. IN Process

In the process (IN) consists of 4 steps, namely:

1. User Login Account to local system via a smartphone device.
2. User tapping RFID card to attend
3. Verify the data card and generate the OTP
4. Generate the OTP code then send it to the user's account.

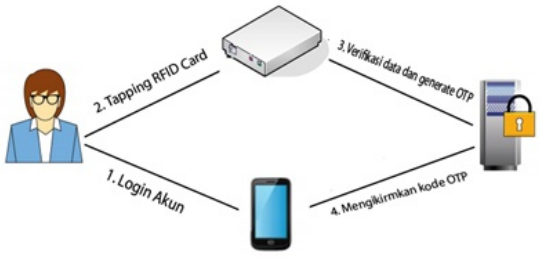

Figure 1. (IN) Process.

3.3.2. OUT Process

In the process (OUT) consists of 4 steps, namely:

1. User Login Account to local system via a smartphone device.
2. User tapping RFID card
3. User Entering the existing OTP code and the system will verify the RFID ID and the inputted OTP code.
4. If appropriate, Data Successfully saved.

Figure 2. (OUT) Process.

4. Experiment

The experiment is performed to determine the function and performance of the whole system. The experiment program is simulated in a suitable system. This experiment is conducted to determine the reliability of the system and to determine whether it is in accordance with the planning or not. The experiment will be done that is in accordance with the step steps in Figure 1 and Figure 2.

4.1. Hardware Used

The modules have been compiled with all the required sequences and have been implemented with the required components. The overall design result of the tool and system can be seen in the following figure:

Figure 3. RFID Tools.

4.2. Implementation Methods

The application of the Multi-Factor Authentication method with the implementation of the OTP code is used to secure and verify the user. With this method user authentication will be performed. The process of applying the method on this hardware is when the user tapping in the morning or early entry to work then the code will be sent to the user account based on the card ID, then when the clock home has arrived the user will do tapping and input the code on the keypad that has been provided. After entering the OTP code 'hash' button on the keypad is pressed to transmit data and check the code in the database.

```
if (customKey == '#') {
    Ethernet.begin(mac, ip, gateway, subnet);
    delay(100);
    Serial.print("Full key=");
    Serial.println(fullkey);
    cursorkey = 0;
    check = 1;
    cekData();
    //kirimData();
    id = "";
    goto endstartloop;
  }
```

If wrong inserts the OTP key 'star' key on the keypad is pressed to delete the wrong number

```
if (cursorkey == 1) {
    if (customKey == '*') {
      fullkey = "";
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Kode OTP=");
      lcd.setCursor(0, 1);
      lcd.print(fullkey);
      cursorkey--;
      goto endkey;
    }
```

4.3. Working of The System

The concatenation in Figure 3 will be tested to perform user authentication process that is by way of initial entry, user will tapping rfid card to rfid reader. If the card has been registered with the OTP code will be sent to the user's account and the clock data entry will be stored on the database. And If the curfew, the user will be tapping an RFID card again and enter the code OTP had previously been sent to the account. Users will enter OTP code with a keypad that has been provided, if the code OTP appropriate then clock out successfully saved to the database, if it fails you will be notified if the code is entered incorrectly OTP.

If the card is not registered then the OTP code can not be sent and on the LCD will show the notification that the card used is not listed.

```
if (inout.equals("no")) {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Tidak terdaftar");
    delay(1000);
    lcd.clear();
    id = "";
    loopagain = 0;
```

Furthermore, if the card is already registered but not feeding the notification that the OTP code is incorrect.

```
if (inout.equals("fa")) {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Kode OTP salah");
    delay(1000);
    lcd.clear();
    id = "";
    loopagain = 0;
  }
```

Therefore the system and Hardware will be interconnected with each other. Namely connected using ethernet and access to the system using the IP address is: 192.168.1.102.

```
client.println( " HTTP/1.1");
  client.println( "Host: 192.168.1.102" );//ur web server
  //client.println( "Content-Type: application/x-www-form-urlencoded" );
  client.println( "Connection: close" );
  client.println();
  // client.stop();
  Serial.println("Data berhasil");
 }
 else {
  Serial.println("gagal");
  id = "";
  delay(100);
 }
}
```

5. Result

Systems and tools to minimize duplication of RFID cards have been successfully constructed using Multi-Factor Authentication method with username, password and OTP codes and can provide more security than using one authentication factor. Using multiple stages of authentication will minimize the occurrence of duplication and fraud. By utilizing some of these Authentication steps make the security system better than ever before. And the existing recordings are more organized. The results of this study users will get OTP code in each account that has been registered in accordance with the card owned. The code will be sent to the user's account. Users can access the account by logging into the IP that has been provided. Code will be obtained every time the user tapping in the morning. And Code will be verified at home hours. The system will match the code that has been previously submitted based on the user card.

From the experimental results obtained:

1. if the card has not been registered then the card can not be read by system and will notification "Card is not Register".

2. If the inserted OTP code does not match the code sent to the feeding user's account it will be rejected by the system and on the LCD it will display the notification of 'Invalid OTP Code'.

3. If the OTP code and the card is in accordance then the data will be stored and the LCD will show the notification 'Thank you'

4. The system can only be accessed using a predefined IP that is 192.168.1.102

5. OTP code will be different every day and will be automatically generated when user tapping.

Here are the results of the OTP code that was successfully sent to the user's account or card owner.

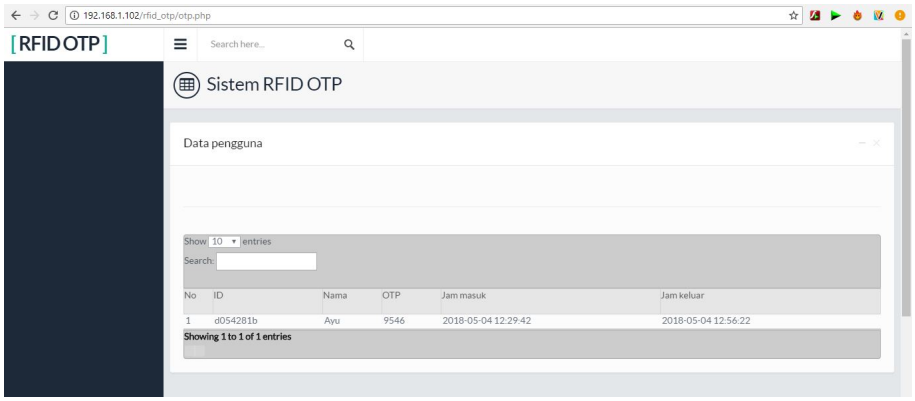

Figure 4. User Account.

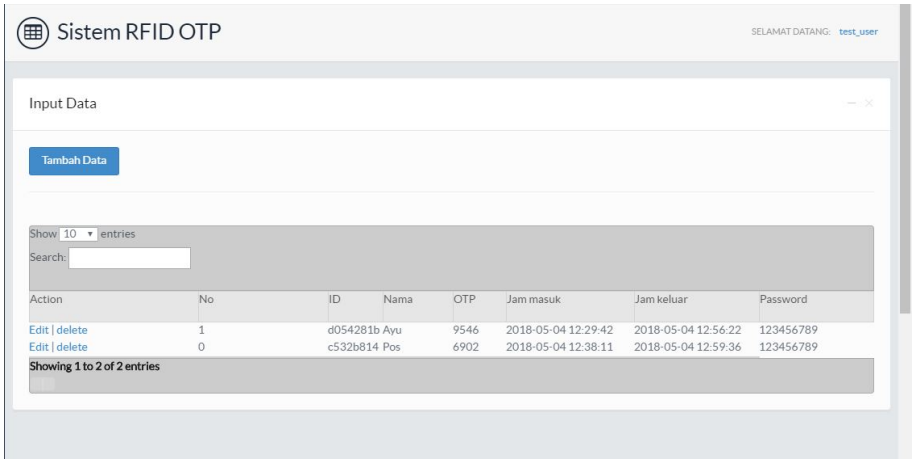

Figure 5. Admin.

6. Conclusion

Based on the results of experiments that have been done show that, by utilizing the method of Multi-Factor Authentication to make the existing system becomes more secure by performing several steps of authentication. Each user has a card each and on the card has different IDs. Every day while tapping, users will get an OTP Authentication code. The code will be sent to each user account. The OTP code will be used at home from work. Users will tapping and entering the code that has been sent. If the code is appropriate then the data will be updated and stored into the data base. But if it is wrong then the data will not be stored, and will be rejected by the system. Likewise when the card used is not registered in the database. System can be accessed through IP that has been provided. So with the system by using some steps of this authentication can minimize the occurrence of duplication of RFID card and minimize the occurrence of cheating that will happen later.

7. Discussion

Based on the results of experiments that have been done show that, by utilizing the method of Multi-Factor Authentication to make the existing system becomes more secure by performing several steps of authentication. Each user has a card each and on the card has different IDs. Every day while tapping, users will get an OTP Authentication code. The code will be sent to each user

account. The OTP code will be used at home from work. Users will tapping and entering the code that has been sent. If the code is appropriate then the data will be updated and stored into the data base. But if it is wrong then the data will not be stored, and will be rejected by the system. Likewise when the card used is not registered in the database. System can be accessed through IP that has been provided. So with the system by using some steps of this authentication can minimize the occurrence of duplication of RFID card and minimize the occurrence of cheating that will happen later.

References

[1] H. U. Zaman, J. S. Hossain, T. T. Anika, and D. Choudhury, "RFID based attendance system," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2017.

[2] D. Eridani and E. D. Widianto, "Simulation of attendance application on campus based on RFID (radio frequency identifiation)," in *2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*. IEEE, 2015.

[3] L. Xie, H. Han, Q. Li, J. Wu, and S. Lu, "Efficiently collecting histograms over rfid tags," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 145–153.

[4] J. Liu, F. Zhu, Y. Wang, X. Wang, Q. Pan, and L. Chen, "Rf-scanner: Shelf scanning with robot-assisted rfid systems," in *INFOCOM 2017-IEEE Conference on Computer Communications, IEEE*. IEEE, 2017, pp. 1–9.

[5] K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic detection of cloning attacks for anonymous rfid systems," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1255–1266, 2015.

[6] S. F. Pane, R. M. Awangga, and B. R. Azhari, "Qualitative evaluation of rfid implementationon warehouse management system," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 3, 2018.

[7] L. Arjona, H. Landaluce, A. Perallos, and S. Martin, "Hardware based design and performance evaluation of a tree based RFID anti-collision protocol," in *2015 International EURASIP Workshop on RFID Technology (EURFID)*. IEEE, 2015.

[8] A. Almaaitah, H. S. Hassanein, and M. Ibnkahla, "Tag modulation silencing: Design and application in RFID anti-collision protocols," pp. 4068–4079, 2014.

[9] P. Xu and T. Jiang, "Research on indoor location algorithm using RFID," in *2016 IEEE 5th Asia-Pacific Conference on Antennas and Propagation (APCAP)*. IEEE, 2016.

[10] J. Basilio-Ramirez, H. Perez-Meana, and V. Ponomaryov, "Multifactor authentication system based on biometrics and radio frequency identification," in *Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 2016 9th International Kharkiv Symposium on*. IEEE, 2016, pp. 1–4.

[11] H. Maleki, R. Rahaeimehr, C. Jin, and M. van Dijk, "New clone-detection approach for rfid-based supply chains," in *Hardware Oriented Security and Trust (HOST), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 122–127.

[12] C. Shao, T. Kim, J. Yu, J. Choi, and W. Lee, "Protar: Probabilistic tag retardation for missing tag identification in large-scale rfid systems," *IEEE transactions on industrial informatics*, vol. 11, no. 2, pp. 513–522, 2015.

[13] J. Huang, X. Li, C.-C. Xing, W. Wang, K. Hua, and S. Guo, "Dtd: A novel double-track approach to clone detection for rfid-enabled supply chains," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 1, pp. 134–140, 2017.

[14] V. Venukumar and V. Pathari, "Multi-factor authentication using threshold cryptography," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2016.

[15] R. M. Awangga, N. S. Fathonah, and T. I. Hasanudin, "Colenak: GPS tracking model for post-stroke rehabilitation program using AES-CBC URL encryption and QR-Code," in *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*. IEEE, nov 2017, pp. 255–260. [Online]. Available:

http://ieeexplore.ieee.org/document/8285506/
[16] J. Jacob, K. Jha, P. Kotak, and S. Puthran, "Mobile attendance using near field communication and one-time password," in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on.* IEEE, 2015, pp. 1298–1303.
[17] C. Marcus and E. A. Armijo, "System and method for automated rfid quality control," Feb. 14 2017, uS Patent 9,569,714.
[18] M. Ramadan, H. Al-Maimani, and B. Noche, "Rfid-enabled smart real-time manufacturing cost tracking system," *The International Journal of Advanced Manufacturing Technology*, vol. 89, no. 1-4, pp. 969–985, 2017.
[19] F. Tao, Y. Cheng, L. Zhang, and A. Y. Nee, "Advanced manufacturing systems: socialization characteristics and trends," *Journal of Intelligent Manufacturing*, vol. 28, no. 5, pp. 1079–1094, 2017.
[20] Y.-Y. Chen, Y.-J. Wang, and J.-K. Jan, "A novel deployment of smart cold chain system using 2g-rfid-sys," *Journal of Food Engineering*, vol. 141, pp. 113–121, 2014.
[21] H. Cai, A. R. Andoh, X. Su, and S. Li, "A boundary condition based algorithm for locating construction site objects using rfid and gps," *Advanced Engineering Informatics*, vol. 28, no. 4, pp. 455–468, 2014.
[22] C. Wang and P. Jiang, "Deep neural networks based order completion time prediction by using real-time job shop rfid data," *Journal of Intelligent Manufacturing*, pp. 1–16, 2017.
[23] M. A. Abas, M. Dahlui *et al.*, "Attendance management system (ams): Comparison of two different approaches," in *Engineering Technology and Technopreneurship (ICE2T), 2017 International Conference on.* IEEE, 2017, pp. 1–7.
[24] M. Srinidhi and R. Roy, "A web enabled secured system for attendance monitoring and real time location tracking using biometric and radio frequency identification (rfid) technology," in *Computer Communication and Informatics (ICCCI), 2015 International Conference on.* IEEE, 2015, pp. 1–5.
[25] W. Cao, P. Jiang, P. Lu, B. Liu, and K. Jiang, "Real-time data-driven monitoring in job-shop floor based on radio frequency identification," *The International Journal of Advanced Manufacturing Technology*, vol. 92, no. 5-8, pp. 2099–2120, 2017.
[26] Y.-S. Kang and Y.-H. Lee, "Development of generic rfid traceability services," *Computers in industry*, vol. 64, no. 5, pp. 609–623, 2013.
[27] K. I. Ramatsakane and W. S. Leung, "Pick location security: Seamless integrated multi-factor authentication," in *2017 IST-Africa Week Conference (IST-Africa).* IEEE, 2017.
[28] B. Oke, O. Olaniyi, A. Aboaba, and O. Arulogun, "Developing multifactor authentication technique for secure electronic voting system," in *Computing Networking and Informatics (ICCNI), 2017 International Conference on.* IEEE, 2017, pp. 1–6.
[29] F. Rehman, S. Akram, and M. A. Shah, "The framework for efficient passphrase-based multi-factor authentication in cloud computing," in *Automation and Computing (ICAC), 2016 22nd International Conference on.* IEEE, 2016, pp. 37–41.
[30] M. Alizadeh, W. H. Hassan, and T. Khodadadi, "Feasibility of implementing multi-factor authentication schemes in mobile cloud computing," in *Intelligent Systems, Modelling and Simulation (ISMS), 2014 5th International Conference on.* IEEE, 2014, pp. 615–618.
[31] Z. Ba and K. Ren, "Addressing smartphone-based multi-factor authentication via hardware-rooted technologies," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on.* IEEE, 2017, pp. 1910–1914.
[32] A. S. Uluagac, W. Liu, and R. Beyah, "A multi-factor re-authentication framework with user privacy," in *Communications and Network Security (CNS), 2014 IEEE Conference on.* IEEE, 2014, pp. 504–505.
[33] D. K. Sarker, N. I. Hossain, and I. A. Jamil, "Design and implementation of smart attendance management system using multiple step authentication," in *Computational Intelligence (IWCI), International Workshop on.* IEEE, 2016, pp. 91–95.
[34] S. H. Khan and M. A. Akbar, "Multi-factor authentication on cloud," in *Digital Image Computing: Techniques and Applications (DICTA), 2015 International Conference on.* IEEE,

2015, pp. 1–7.
[35] G. D. Mandyam and M. Milikich, "Leveraging contextual data for multifactor authentication in the mobile web," in *Communication Systems and Networks (COMSNETS), 2015 7th International Conference on*. IEEE, 2015, pp. 1–4.
[36] Y. Shah, V. Choyi, and L. Subramanian, "Multi-factor authentication as a service," in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on*. IEEE, 2015, pp. 144–150.
[37] G. Zhao, Y. Li, L. Du, and X. Zhao, "Asynchronous challenge-response authentication solution based on smart card in cloud environment," in *Information Science and Control Engineering (ICISCE), 2015 2nd International Conference on*. IEEE, 2015, pp. 156–159.
[38] W. A. Hufstetler, M. J. H. Ramos, and S. Wang, "Nfc unlock: Secure two-factor computer authentication using nfc," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2017, pp. 507–510.
[39] C.-H. Huang and S.-C. Huang, "Rfid systems integrated otp security authentication design," in *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacific*. IEEE, 2013, pp. 1–8.