Secured e-payment system based on automated authentication data and iterated salted hash algorithm

Ali Al Farawn[1], Hasanein D. Rjeib[2], Nabeel Salih Ali[1*], Basheer Al-Sadawi[1]
[1]Information Technology Research and Development Centre, University of Kufa, Iraq
[2]ECE Department, Faculty of Engineering, University of Kufa, Iraq

Article Info

Article history:

Received May 1, 2019
Revised Jul 8, 2019
Accepted Jul 20, 2019

Keywords:

Data security
Encryption
Encryption password
Hash
Information security
RFID
SHA

ABSTRACT

Electronic payment has been considered as one of the most significant and convenient applications of modern electronic services e-University compared to traditional methods that impose time-consuming, human resources, and inefficiency. Different automatic identification technologies have been widely used, such as radio frequency identification (RFID). Extensive research and several applications are focusing on taking the maximum advantage of RFID technology. Data and information security had considered a crucial role when information concerning e-commerce, e-banking, or e-payments, especially due to it required real data to establish accessed illegally. Hence, data originality and security fall a very significant and critical issue in data communication services in recent years. Applications such as e-banking or e-commerce regularly contain sensitive and personal information that should be managed and controlled by authorized persons. Thus, keeping a secure password is important to prevent unauthorized users from illegal access. The password hashing is one of the safety methods and means of preventing attacks. In this article, focuses on proposing an RFID based electronic payment and also provide multi-level security privileges for an academic domain by using RFID technology besides the programmable logic circuit as well the system used C# language in visual studio environment also desktop and web-based application for system working purposes. The proposed system aims to manage student payments in a secure manner and provides the capabilities of getting a bus ticket, copying books, buying food, paying registration fees, and other services. The results have shown the system is secured by using the confirmation code in addition to password encryption.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Nabeel Salih Ali,
Information Technology Research and Development Center (ITRDC),
University of Kufa,
Kufa, P.O. Box (21), Najaf Governorate, Iraq.
Email: Nabeel@uokufa.edu.iq

1. INTRODUCTION

Universities are seeking to keep pace with the rapid technological development and the use of modern technology in different several various fields such as electronic payment which allows the student to make all payments within the University electronically [1]. Since such technology can help to manage student payments and provides the capabilities of getting diverse services like a bus ticket, copying books, buying food, registration fees, and other related services. Therefore, provides facilities for managing student budget without the need to carry any additional expenses inside the campus where all the additional would be electronically, so there is a need to use automatic identification for a student by using automatic identification technology [2, 3]. So we are proposing an RFID technology to adopt such a system. Recently, radio frequency identification technology (RFID) has been widely adopted by several organizations, academic institutions, hospitals, markets, etc. [4, 5]. Many organizations, hospitals, and universities have adopted the RFID technology over other identification technologies such as barcoding, biometric, and other identification technologies due to its low cost, small size, easy maintenance, and the ability to identify objects without requiring light of sight [6, 7]. In addition, RFID can be implemented in harsh environments such as dirt and damage, providing the ability of auto-tracking [8]. RFID can identify tags without the need for direct contact where it can identify tags for a specific object within couple feet, tag reusability, and the ability to read multiple tags simultaneously [9, 10]. These functions make RFID technology more preferable over other technologies like barcoding in the field of smart environments like a smart library, smart University, security system – considering cost, etc. [11, 12]. RFID technology involves an RFID tag and an RFID reader. The tag (transponder) consists of a tiny chip with an embedded antenna which stores a unique ID number. Tags can be either active or passive, depending on whether it comes with a power battery source (active) or not (passive); the passive tag is usually powered by the reader. The RFID reader is used to communicate and retrieve data stored in the RFID tags. RFID antenna comes in different sizes, and different communication ranges depending on the distance between the reader and the tag [13]. Most corporations and educational institutions endeavor to provide a secure level of their online applications. Hence, they were allowing more confidential data exchange between organizations [14, 15]. So, there are multifarious security and privacy issues that need to be understood and taken care of [16, 17]. Management identification, disaster recovery, operational integrity, and confidentiality are various domains that suffered from security and privacy challenges [18, 19]. Therefore, service damages or system downtime could cause losses of millions of dollars of a certain company [20]. The more the number of accesses to the system by the user increases, the more security threats also increase; hence, the administrators should use decent approaches for securing the system [21, 22]. Data and information security are considered as a big challenge when it comes to e-banking systems or e-commerce in due to the requirement of real data and money transaction which is considered as a critical issue and should not be accessed without proper identification [23-25]. Therefor in data communication services, it is very important for the data to be original and secured [26-28]. Generally, the number of password predictions to an authenticated online system specifies the measurement of password attack on that system [29-31]. In order to save and secure the date for each system, data integrity, message authentication, access control, authentication of data entity and the key, and all the information security objectives should be maintained safely by the users and the administrators [32, 33]. To achieve the objectives of information security, authentication is the most common methods to do so.

Several studies have been conducted towards establishing a smart university as well as RFID technology has been adopted by several markets and retailers to improve performance while reducing the time for purchasing [34]. Authors developed a smart shopping and billing system to be used at markets in order to assist a customer in shopping while purchasing a product [35]. And, a study is provided an easier way to find, arrange books with minimum time in addition to the simplicity for fetching books [36]. Likewise, researchers have proposed a prototype system for attendance in addition to smart automation of electrical appliances by using RFID with wireless sensor networks [37]. Also, the article has discussed the benefits of adopting RFID technology in markets and retail sectors [38]. Besides, research is provided a mechanism for smart attendance management along with timetable, student information system providing a wide database for University students and staff members [39]. The current paper aims to take advantage of using RFID in smart University and smart markets as well, by designing a smart shopping system for students within a smart University environment, where the students are capable of purchasing a product from any shop inside the University campus by using the same RFID card that holding their information. Besides, presents multi-level secure password in the proposed e-payment system via using hashing cryptography algorithm to prevent illegal access via crafter.

2. MATERIALS AND METHODS (METHODOLOGY)

This section presents components of the proposed electronic circuit design that includes software and hardware requirements as well as methods and implementation steps of the system. The system aims to make all payment inside the University electronically with respect to security issue via proposing multi-level security paradigms. The hardware components required for the implementation are Arduino UNO board, Ethernet shield, and sensors (RFID Reader). Figure 1 provides an overview of the proposing system.

According to Figure 1, The RFID reader is connected to the Arduino Uno microcontroller device which is connected to ethernet shield device. The signal is sent to a client-based system by the Arduino through Ethernet cable, the database (server side) then implements the payment process by using the client-based application to check the balance of the student. The proposed system provides easy access to student information by displaying their information such as total balance, current balance, and the note about all their payment and other information.

The RFID reader reads the ID for the student tag and sends it via the Arduino device using the Ethernet shield attached to the Arduino to the server by desktop application based (MSSQLSERVER AND C#) for Database ID checking procedure. The database is created by MSSQL program and contains the records of the student IDs, once the ID is found, the money withdrawal is to be done. The RFID reader is connected to the Arduino pins as follow in Table 1. The Arduino device processes the signal then sends it via Ethernet cable to the server

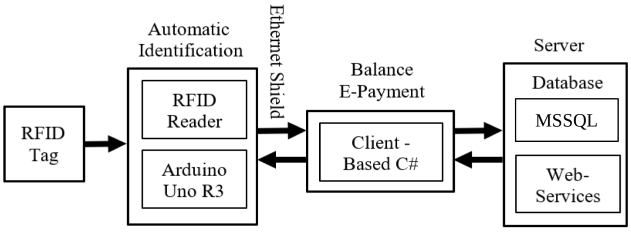


Figure 1. Block diagram for the proposed system architecture

Table 1. RFID module and Arduino UNO pin connectors

RFID module	Arduino UNO pins
RESET	D9
MISO	D12
MOSI	D11
SCK	D13
SAD	D10

2.1. Phase one (e-payment management system)

Figure 2 shows the complete workflow of the e-payment system, including the administrator, students, and sales point managers.

2.2. Phase two (multi-level system security)

In this study, two security level applied to enforce system confidentiality, which is a secret code and password encryption. For the first, level the system asks the user to enter his secret code before starting the process of fees withdrawal to confirm the identification of the user and to protect the privacy of the user when tag lost or theft by requesting the secret code assigned to him and verify the secret code stored (SHA-256) in the database as we mentioned in the second paradigm security if it is true and then doing the user fee process as shown in Figure 3.

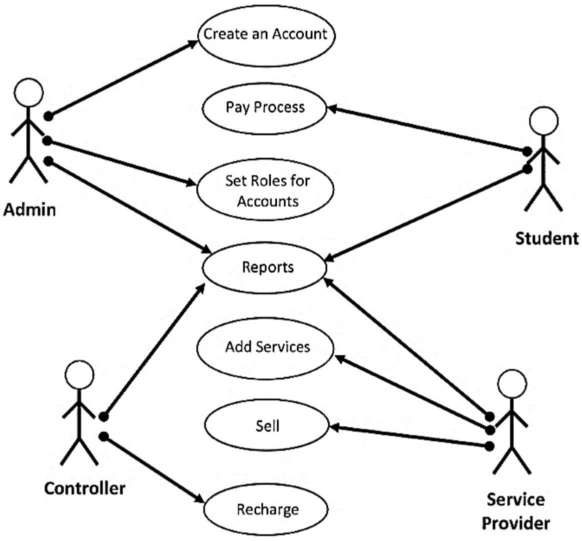


Figure 2. Use case diagram of the proposed system

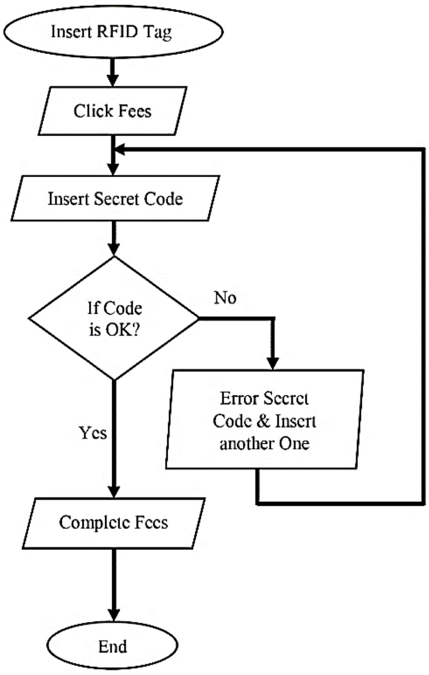


Figure 3. Secret code of the system authentication

The basic interface design of the payment process at the sales points is falling into two steps, the first step is to carry out the payment process by taking the ID from student that stored in RFID card, and the second step is to determine the purchase type and the price and then to press on the button (Fees), in this step the student should enter his/her code to check whether the code is correct before the completion of transaction. For the second paradigm, iterative password salted hash encryption is used for password encryption. Encryption is the process of converting information that is simple text when storing on different storage media to numbers and letters that are randomly ordered so that they become incomprehensible or unreadable to anyone. Encryption is useful because: 1) confidentiality: a service used to store the content of information from all persons, 2) integrity: a service used to save information from change (delete, add, or modify) by unauthorized persons [34]. In this perspective, we conducted an anti-continuous collision salted hash encryption (ACCSHE) technique which extracts a unique features from each user to repeat secured salted hashing algorithm (SHA-256) several times to convert the simple text of the password to complex 64 random numbers and letters encrypted password saved in the database according to [40].

The hashing with salt is used to support hashing results. Whether, when two hashed passwords used the same plain text, the result is not the same [41]. While the e-payment system application needs critical security requirements therefor the salt code cryptographically secure pseudo-random number generator (CSPRNG) is using to guard system security against attacks [42]. Figure 4 presents the password encryption processing in details.

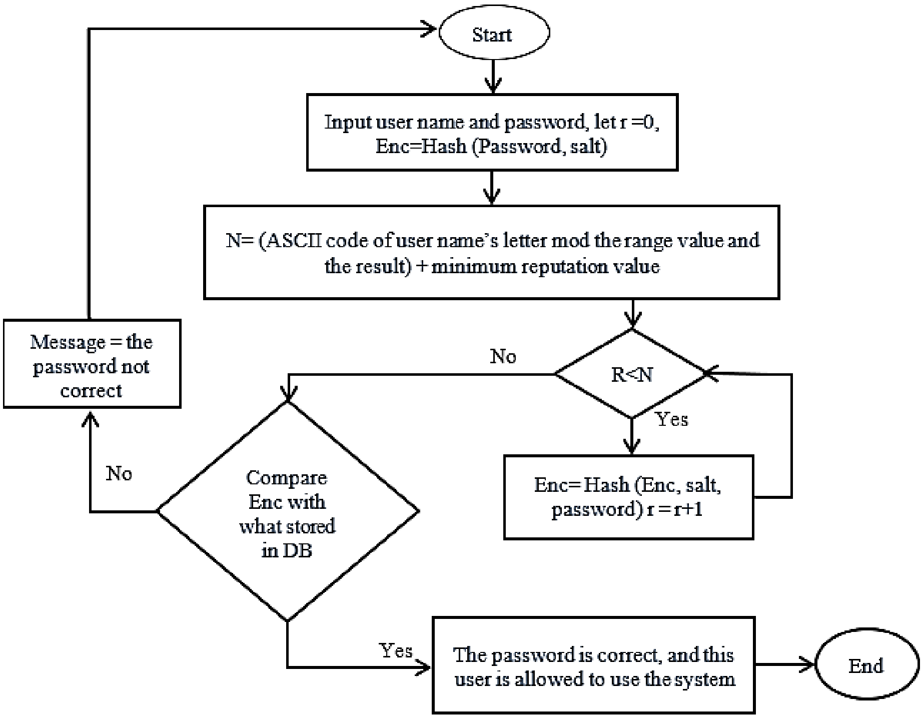
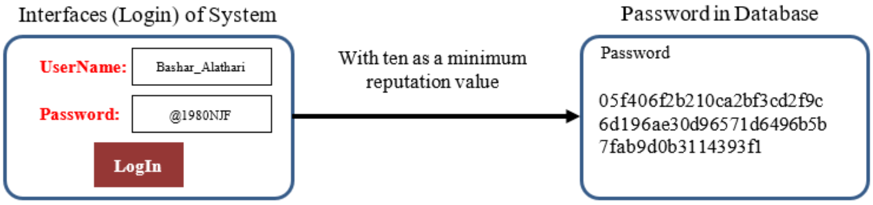

Start
Input user name and password, let r =0, Enc=Hash (Password, salt)
N= (ASCII code of user name's letter mod the range value and the result) + minimum reputation value
R<N
No
Yes
Enc= Hash (Enc, salt, password) r = r+1
Message = the password not correct
No
Compare Enc with what stored in DB
Yes
The password is correct, and this user is allowed to use the system
End

Figure 4. Password encryption processing

3. RESULTS AND DISCUSSION

The presented system is achieving electronic payment and transaction to provide facilities for managing student budget in e-University. This system has a level of security by confirming the secret code by a student to confirmation purposes. The transaction is done only if the code is correct and the system will also be more secure by adopting password encryption scheme to prevent hacking of the user account. The encryption example is used in the system is shown in Figure 5. When typing a password in a login interface such as (@1980NJF), it will encode directly into the database with random images and non-intrusive characters, and this feature provides a high level of security for the students as it is difficult to hack by intruders and also in the case of robbery.

The advantage for repeated secured salted hashing algorithm is to create a more complex and more difficult password to break [43]. As shown in Figure 6, which explain the time required to calculate the encrypted password increased when the value of minimum alteration increasing, which means the time complexity increase fore break password. The average time of 20 users, the value of minimum alteration changed from 10, 100, 10000, and 100000. Finally, the (ACCSHE) method has several control key features to chang the results, such as the number of repetition and salt used without affecting the usability system as we show in Figure 6.


Interfaces (Login) of System
LogIn
With ten as a minimum reputation value
Password in Database

UserName: Bashar_Alathari

Password: @1980NJF

Password

05f406f2b210ca2bf3cd2f9c
6d196ae30d96571d6496b5b
7fab9d0b3114393f1

Figure 5. Example of the encryption in encryption mechanism in the proposed system.

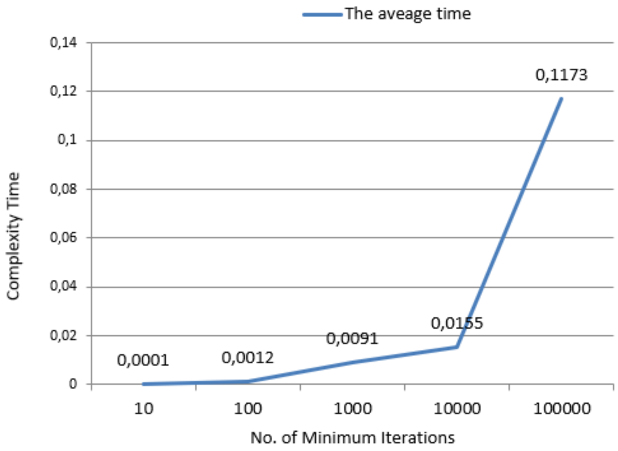


Figure 6. The average time for 20 users based on the password encryption scheme

4. CONCLUSIONS AND FUTURE DIRECTIONS

An electronic payment system is implemented by designing and creating a database system for holding students information (name, id, budget, etc.), the system provides a mechanism that allows students to inquire about their balance and give a notification for recharging. Besides, design and test the complete hardware system that works with the database to maintain the deposit and payment electronically. This system has a level of security as a confirmation code and (SHA-256) password encryption method to enforce the system authentication and confirmation paradigms from illegal access as well to provide e-University apps. The future direction of the system is to add a web interface that shows extra details for the student account, in addition, to implement a mobile application that is capable for purchasing, charging, and withdrawing.

REFERENCES

[1] Park S. Y., "An analysis of the technology acceptance model in understanding University students' behavioral intention to use e-learning," *Journal of Educational Technology & Society*, vol. 12, no. 3, pp. 150-162, 2009.

[2] Alhilali A. H., Ali N. S., Kadhim M. F., Al-Sadawi B., Alsharqi H., "Multi-objective attendance and management information system using computer application in industry strip," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 1, pp. 371-381, 2019.

[3] Ihamji M., Abdelmounim E., Zbitou J., Bennis H., Latrach M., "A compact miniature fractal planar antenna for RFID readers," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 300-305, 2019.

[4] Yuru Z., Delong C., Liping T., "The Research and Application of College Student Attendance System based on RFID Technology," *International Journal of Control and Automation*, vol. 6, no. 2, pp. 273-282, 2013.

[5] Arif Z. H., Ali N. S., Zakaria N. A., Al-Mhiqani M. N., "Attendance Management System for Educational Sector: Critical Review," *International Journal of Computer Science and Mobile Computing*, vol. 7, no. 8, pp. 60-66, 2018.

[6] Abbasi A. Z., Shaikh Z. A., "Building a smart University using RFID technology," *IEEE-2008 International Conference on Computer Science and Software Engineering*, vol. 5, pp. 641-644, December 2008.

[7] El Boutahiri A., El Alaoui M., El Khadiri K., Tahiri A., Qjidaa H., "Design of New Power Generating Circuit for Passive UHF RFID Tag," *International Journal of Power Electronics and Drive Systems*, vol. 9, no. 3, pp. 1389-1397, 2018

[8] Tarbouch M., El Amri A., Terchoune H., "Design, Realization and Measurements of Compact Dual-band CPW-fed Patch Antenna for 2.45/5.80 GHz RFID Applications," *International Journal of Electrical & Computer Engineering*, vol. 8, no. 1, pp. 2088-8708, 2018.

[9] Sunehra D., Goud V. S., "Attendance recording and consolidation system using Arduino and Raspberry Pi," *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 1240-1245, October 2016.

[10] El Hachimi Y., Gmih Y., Makroum E. M., Farchi A., "A Miniaturized Patch Antenna Designed and Manufactured Using Slot's Technique for RFID UHF Mobile Applications," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, pp. 5134-5143, 2018.

[11] Curtin J., Kauffman R. J., Riggins F. J. "Making the 'MOST'out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID," *Information Technology and Management*, vol. 8, no. 2, 2007.

[12] White G., Gardiner G., Prabhakar G. P., Abd Razak A., "A comparison of barcoding and RFID technologies in practice," *Journal of information, information technology and organizations*, vol. 2, pp. 119-132, 2007.

[13] Bansode S. Y., Desale S. K., "Implementation of RFID technology in University of Pune Library," *Program: Electronic Library and Information Systems*, vol. 43, no. 2, pp. 202-214, 2009.

[14] Buehrer G. T., Weide B.W. Sivilotti P. A. G., "Using parse tree validation to prevent SQL injection attacks," *Proceeding SEM'05 Proceedings of the 5th international workshop on Software engineering and middleware*, pp. 106–113, 2005.

[15] Ali N. S. "Investigation framework of web applications vulnerabilities, attacks and protection techniques in structured query language injection attacks," *Int. J. Wireless and Mobile Computing*, vol. 14, no. 2, pp. 103–122, 2018.

[16] Al-Mhiqani M. N., Ahmad R., Abdulkareem K. H. Ali N. S., "Investigation study of cyber-physical systems: characteristics, application domains, and security challenges," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, no. 22, pp. 6557–6567, 2017.

[17] Ali N. S., Shibghatullah A. S., Attar M. H. A. L., "Review of the defensive approaches for structured query language injection," *Journal of Theoretical and Applied Information Technology*, vol. 76, no. 2, pp.258–269, 2015.

[18] Bhadauria R., Chaki R., Chaki N. Sanyal S., "A Survey on Security Issues in Cloud Computing, arXiv preprint," [Online], Available: https://arxiv.org/abs/1109.5388, arXiv: 1109.5388, 2011.

[19] Shih K. H., Lee M. F.. "Users' intentions on the mobile securities trading system," *Int. J. Mobile Communications*, vol. 15, no. 3, pp. 252–265, 2017.

[20] Halfond W. G. J., Choudhary S. R. Orso A., "Improving penetration testing through static and dynamic analysis," *Software Testing, Verification and Reliability*, vol. 21, no. 3, pp. 195–214, 2011.

[21] Morris R., Thompson K., "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594-597, 1979.

[22] Shay R., Komanduri S., Kelley P. G., Leon P. G., Mazurek M. L., Bauer L., Cranor L. F., et. al, "Encountering stronger password requirements: user attitudes and behaviors," *Symposium on Usable Privacy and Security (SOUPS)*, Redmond, WA USA, 14–16 July 2010.

[23] Silhavy R., Senkerik R., Oplatkova Z. K., Prokopova Z. Silhavy P., "Software engineering in intelligent systems," *Proceedings of the 4th Computer Science On-line Conference 2015 (CSOC2015)*, vol. 3 (Software Engineering in Intelligent Systems), 2015.

[24] Ali N. S., "Protection web applications using real-time technique to detect structured query language injection attacks," *International Journal of Computer Applications*, vol. 149, no. 6, pp. 26–32, 2016.

[25] Dey S., Nath J. Nath A., "An integrated symmetric key cryptographic method – amalgamation of TTJSA algorithm, advanced Caesar cipher algorithm, bit rotation and reversal method: SJA algorithm," *International Journal of Modern Education and Computer Science*, vol. 4, no. 5, pp. 1–9, 2012.

[26] Das A., Bonneau J., Caesar M., Borisov N. Wang X., "The Tangled Web of Password Reuse," *NDSS*, vol. 14, pp. 23–26, 2014.

[27] Chatterjee D., Nath J., Das S., Agarwal S. Nath A., "Symmetric key cryptography using modified DJSSA symmetric key algorithm," *Proceedings of International Conference Worldcomp*, pp. 18–21, 2011.

[28] Dell' Amico M., Michiardi P., Roudier Y., "Password strength: an empirical analysis," *Proceedings IEEE in INFOCOM*, pp. 1–9, 2010.

[29] Kelley P. G., Komanduri S., Mazurek M. L., Shay R., Vidas T., Bauer L., Christin N., Cranor L. F., Lopez, J., "Guess again (and again and again): measuring password strength by simulating password-cracking algorithms," *IEEE Symposium on Security and Privacy (SP)*, pp.523–537, 2012.

[30] Komanduri S., Shay R., Kelley P. G., Mazurek M. L., Bauer L., Christin N., Cranor L. F. Egelman S., "Of passwords and people: measuring the effect of password-composition policies," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2595–2604, 2011.

[31] Churi P. P., Ghate V., Ghag K., “Jumbling-salting: an improvised approach for password encryption,” *International Conference on Science and Technology (TICST)*, pp. 236–242, 2015.

[32] Bonneau J., Just M., Matthews, G. (2010) ‘What’s in a name? Evaluating statistical attacks on personal knowledge questions,” *Financial Cryptography and Data Security - 14th International Conference*, Springer, Berlin, Heidelberg, vol. 6052, pp. 98–113, 2010.

[33] Menezes A. J., Van Oorschot, P. C., Vanstone S. A., “Handbook of Applied Cryptography,” June, CRC Press, Massachusetts Institute of Technology (MIT), 1996.

[34] Sayanekar P., Rajiwate A., Qazi L., Kulkarni A., “Customized NFC enabled ID card for Attendance and Transaction using Face Recognition,” *International Research Journal of Engineering and Technology*, vol. 3, no. 9, pp. 1366-1368, 2016.

[35] Ali Z., Sonkusare R., “RFID based smart shopping and billing,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 13, pp. 4696- 4699, 2013.

[36] Brian A. L. A., Arockiam L., Malarchelvi P. D. S. K., “An IOT based secured smart library system with NFC based book tracking,” *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, vol. 11, no. 5, pp. 18-21, 2014.

[37] Al Shimmary M. K., Al Nayar M. M., Kubba A. R., “Designing smart University using RFID and WSN,” *International Journal of Computer Applications*, vol. 112, no. 15, pp. 34-39, 2015.

[38] Novotny Á., Dávid L., Csáfor H., “Applying RFID technology in the retail industry–benefits and concerns from the consumer's perspective,” *Amfiteatru Economic Journal*, vol. 17, no. 39, pp. 615-631, 2015.

[39] Rjeib H. D., Ali N. S., Al Farawn A., Al-Sadawi B., Alsharqi H., “Attendance and information system using RFID and web-based application for academic sector,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 1, pp.266–274, 2018.

[40] Alattar M. H., Farawn A. A., Ali N. S., “Anti-continuous collisions user-based unpredictable iterative password salted hash encryption,” *Int. J. Internet Technology and Secured Transactions*, vol. 8, no. 4, pp. 619–634, 2018.

[41] Rahman M. T., Mahi M. J. N., “Proposal for SZRP protocol with the establishment of the salted SHA-256 bit HMAC PBKDF2 advance security system in a MANET,” *International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)*, pp. 1–5, April 2014.

[42] Mc Evoy R., Curran J., Cotter P., Murphy C., “Fortuna: cryptographically secure pseudo-random number generation in software and hardware,” *IET Irish Signals and Systems Conference (ISSC 2006)*, pp. 457–462, 2006.

[43] Castelluccia C., Durmuth M., Perito D., “Adaptiven password-strength meters from Markov models,” *NDSS’12: Proceedings of the Network and Distributed System Security Symposium*, 2012.