Government of Karnataka

Department of Collegiate and Technical Education

GOVERNMENT ENGINEERING COLLEGE

KARWAR, MAJALI-581345

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

A
Technical seminar report
on

"E-Authentication System Using QR Code & OTP"

Submitted In the Partial Fulfilment for the Degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

RISHAB MANJUNATH REVANKAR **2GP21CS033**

Under the Guidance of

Prof. PRACHI KUDTARKAR

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELAGAVI -590002

GOVERNEMENT OF KARNATAKA

DEPARTMENT OF COLLEGIATE AND TECHNICAL EDUCATION

GOVERNEMENT ENGINEERING COLLEGE, KARWAR, MAJALI -581345

(Affiliated to Visvesvaraya Technological University)

Department of Computer Science and Engineering

2024-2025

Certificate

This is to certify that the Technical seminar report entitled "**E-Authentication System Using QR Code & OTP**" carried out by Mr. RISHAB MANJUNATH REVENKAR, USN:2GP21CS033 are bonafide student of Government Engineering College, Karwar in partial fulfilment for the award of Bachelor of Engineering in Computer Science and Engineering of the Visvesvaraya Technological University, Belagavi during the year 2024-2025. The Technical seminar report has been approved as it satisfies the academic requirements prescribed for the said Degree.

.....	.....	.....
Signature of the Coordinator	Signature of the H.O.D	Signature of the Principal

ACKNOWLEDGEMENT

While presenting this Technical Seminar on “E-Authentication System Using QR Code & OTP” I feel that is our duty to acknowledge the help rendered to us by various persons.

I take this opportunity to thank Prof. D CHAUHAN, HOD of Computer Science and Engineering Dept, GEC Karwar providing the inspiration for taking the Technical Seminar to completion.

I will be falling in my duty if I don’t thank our principal Dr. Shanthala B for providinghealthy environment in the college that helped in concentrating on the task.

I take this opportunity to thank Mr. Devdatt Attender of Computer Science and Engineering Dept, GEC Karwar providing the inspiration for taking the Technical Seminar to completion.

Then I would also thank all teaching and nonteaching staff of the department who directly or indirectly contributed in accomplishing this task.

Last but not the least I express my sincere thanks to all persons who have directly or indirectly assisted my endeavour.

RISHAB MANJUNATH REVANKAR 2GP21CS033

ABSTRACT

With the fast expansion of wireless communication technology, user authentication is becoming increasingly vital in order to assure the system's security. Passwords serve a vital part in the authentication process. The user's password will be submitted with the traffic to the authentication server during the authentication procedure, allowing the server to provide access to the authorized user. The invaders will take advantage of the opportunity to try to sniff out other people's passwords in order to carry out illicit acts under the guise of someone else's identity, keeping them out of danger. Many methods have been offered to improve the security of wireless communication technologies as a result of the challenges. The recommended approach will be utilized to improve the system's security in this study. One time passwords, hashing, and two-factor authentication were chosen as the solution. There will also be a new solution that uses the QR code to assist preserve more data. The system outcome's goal is to improve the present login authentication mechanism. It proposes ways to make password cracking more difficult, as well as persuade people to pick and use tough-to-guess passwords**.**

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This passage discusses the importance of security in web-based services, particularly for online transactions. It highlights that passwords, though commonly used for authentication, can be vulnerable if users don't take proper precautions. Client-side attacks, such as those targeting online banking and e-commerce, have increased due to a lack of security awareness among users.

The study suggests improving security by combining multiple authentication techniques to make online transactions safer. One such method involves using One-Time Passwords (OTPs), which are valid only for a single session and for a limited time, to reduce the risk of attacks. Additionally, the study proposes an anti-form snatching strategy that prevents attackers from intercepting and altering sensitive data as it is sent from the client to the server. Another recommendation is to use email as a secondary verification method for added security.

In summary, the study focuses on enhancing online security by combining multiple authentication methods, preventing data tampering, and using short-lived passwords (OTPs) and email verification to protect both the user and the server from cyberattacks.

CHAPTER 2

LITERATURE SURVEY

This passage discusses the increasing complexity of cyberattacks targeting internet consumers, especially in the financial sector, and the challenges in detecting such attacks from the client side. Cyber thieves can manipulate user account details without the user noticing, leading to significant financial losses. In 2009, global financial services losses due to cyber-attacks reached $54 billion, up from $48 billion in 2008. The rise in these attacks, especially on European banks, necessitates stronger and more reliable authentication systems.

The text highlights the weaknesses of traditional single-factor authentication methods (like usernames and passwords), which are insufficient in protecting against modern cyber threats. It suggests integrating more advanced systems, such as biometric authentication, smart cards, and QR codes, to improve security. However, biometric systems have drawbacks, such as longer processing times, and QR codes need encryption to prevent spoofing.

The passage also mentions the importance of mutual authentication between users and financial institutions to protect against phishing and other attacks. A proposed solution is to combine HTTPS communication, digital certificates, and OTPs generated from QR codes for secure transactions.

However, the adoption of these security methods depends on user acceptance. If an authentication method is inconvenient or has privacy concerns, users may refuse to use it. Research shows that trust and acceptance of e-authentication systems vary among different groups, such as students, with some individuals hesitant due to privacy or disability concerns. Therefore, the success of these systems depends not just on their security features, but on how well they are accepted and trusted by users.

In summary, while new authentication methods like biometrics and QR codes could enhance security, their effectiveness relies on addressing privacy concerns and ensuring user trust and ease of use.

CHAPTER 3

METHODOLOGY

3.1 System Analysis and Planning

The practice of assessing a company condition with the goal of changing it via improved procedure and technique is known as system analysis and design. The two primary components of system development are system analysis and design. System design is the process of creating a new system, as well as replacing or enhancing an existing one. However, before we can plan, we must first do a thorough analysis of the current system and determine how the computer might be used to improve its performance. System analysis is the process of gathering and analyzing data, diagnosing problems, and using the data to provide recommendations for system improvements.

3.2 Requirement Analysis

Requirement analysis is a process in system engineering and software engineering that involves establishing the need or conditions that must be satisfied for a new or changed product while taking into account the often-conflicting requirements of numerous stack holders, such as beneficiaries or users. The ability to assess requirements is important to the success of any development project. Executable, measurable, testable and documented requirements for known business requirements or prospects must be stated in sufficient depth for system design. Requirements describe how a system should work, as well as its traits and attributes. It might also be a description of what an app is meant to do.

3.3 Flow Chart

A flowchart is a sort of diagram that shows representations of an algorithm or process by portraying the steps as different types of boxes and connecting them with arrows to show their order. These boxes and arrows do not represent process operations; rather, they are suggested by the sequence of events operations.

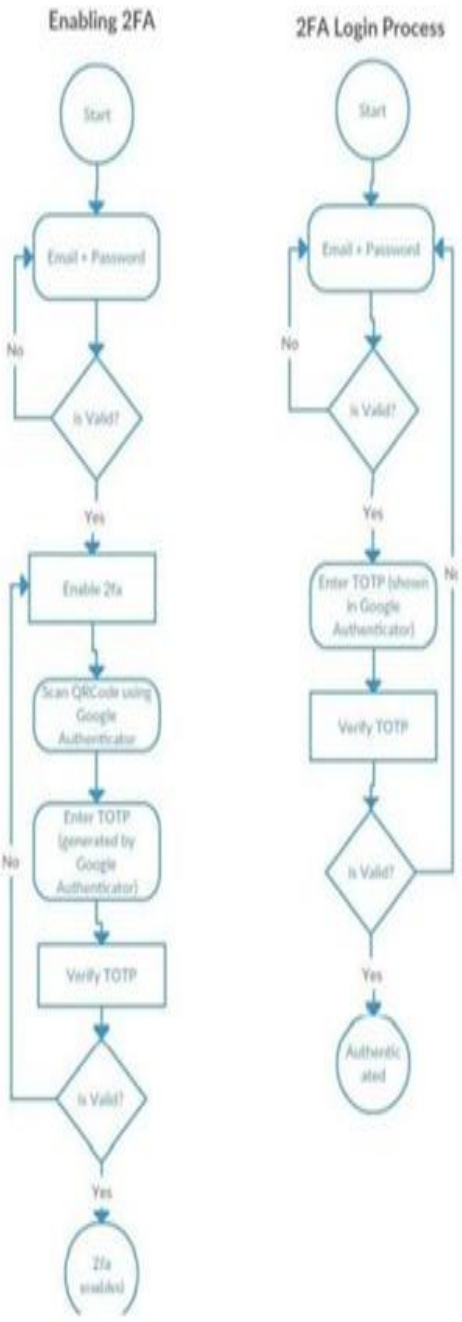

Figure : Flow Chart of E-Authentication Login Process

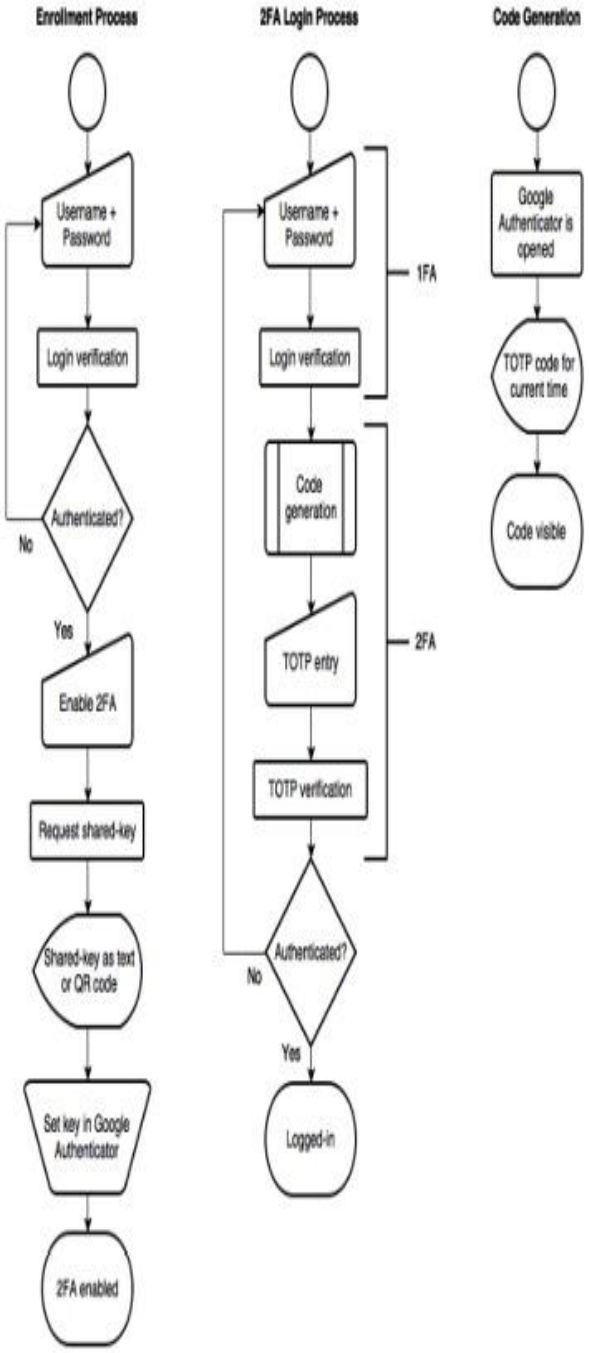

Figure : Flow Chart of E-Authentication Login and Code Generation Process

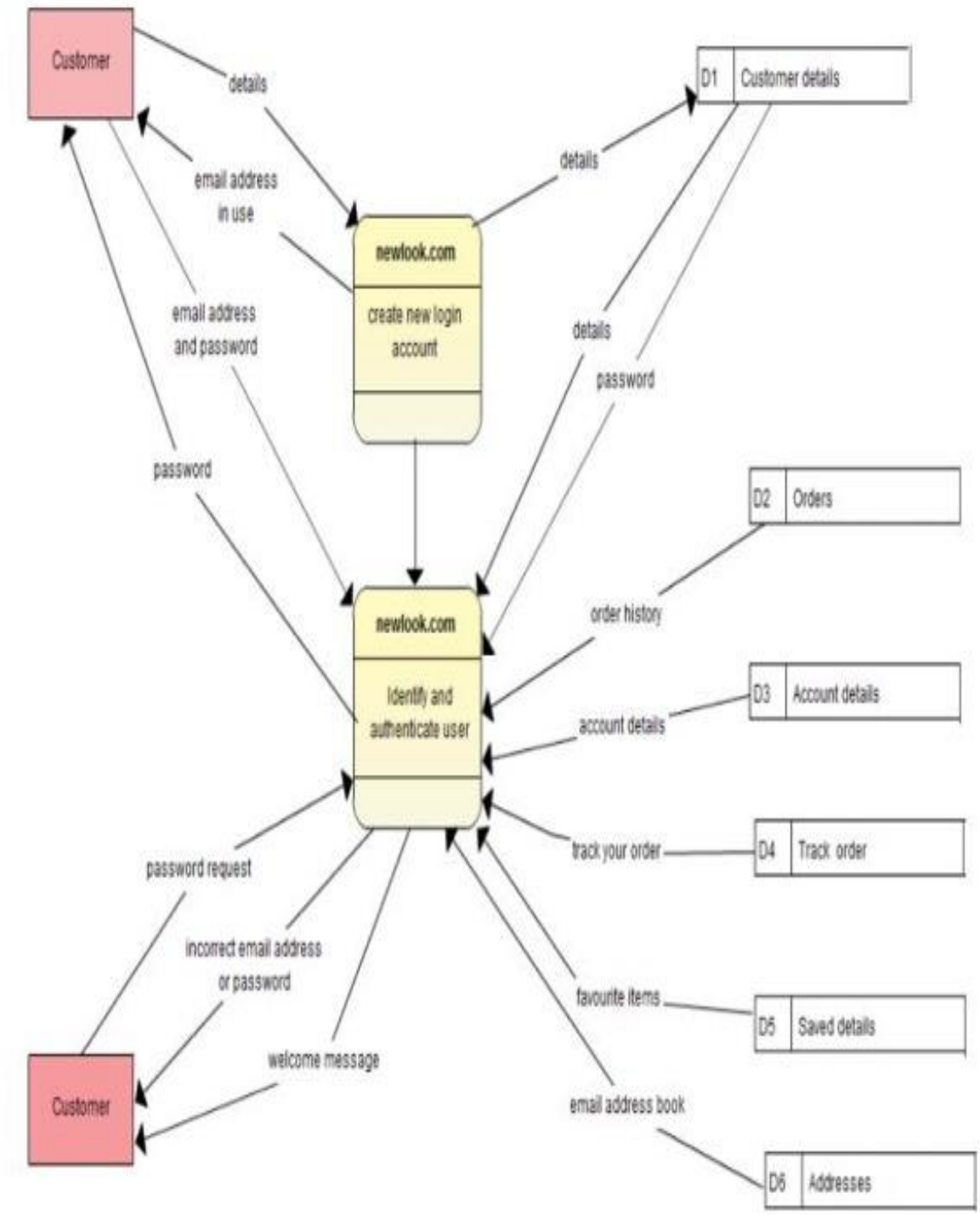

Figure : Data Flow Diagram of E-Authentication

CHAPTER 4

BACKGROUND

4.1 (QUICK RESPONSE) QR code

QR codes, developed by Denso Wave, are two-dimensional barcodes that store information both vertically and horizontally, allowing them to hold much more data than traditional one-dimensional (1D) barcodes. QR codes can be scanned with mobile phone cameras and processed using a QR scanner, enabling users to access web content or perform other actions on their phones.

Unlike 1D barcodes, which only store limited data and are scanned in one direction, QR codes are more versatile, allowing for multiple scanning options and supporting alphanumeric, numeric, and kanji characters.

QR codes offer several advantages as a security measure and in marketing:

1. **Connection Between Online and Offline Media**: QR codes link printed media (like flyers, brochures, and business cards) to websites, making it easier for customers to access online content directly.
2. **Quick and Error-Free**: Scanning a QR code is faster and less prone to errors compared to manually typing URLs.
3. **Rich Content Engagement**: QR codes enable marketers to share interactive, multimedia content (e.g., videos or recipes) through print media.
4. **Actionable**: QR codes allow businesses to make promotions interactive, collect feedback, or facilitate purchases directly from print ads.
5. **Trackable**: QR codes provide valuable analytics, allowing businesses to track how often, when, and where a code is scanned, helping measure the effectiveness of marketing campaigns.

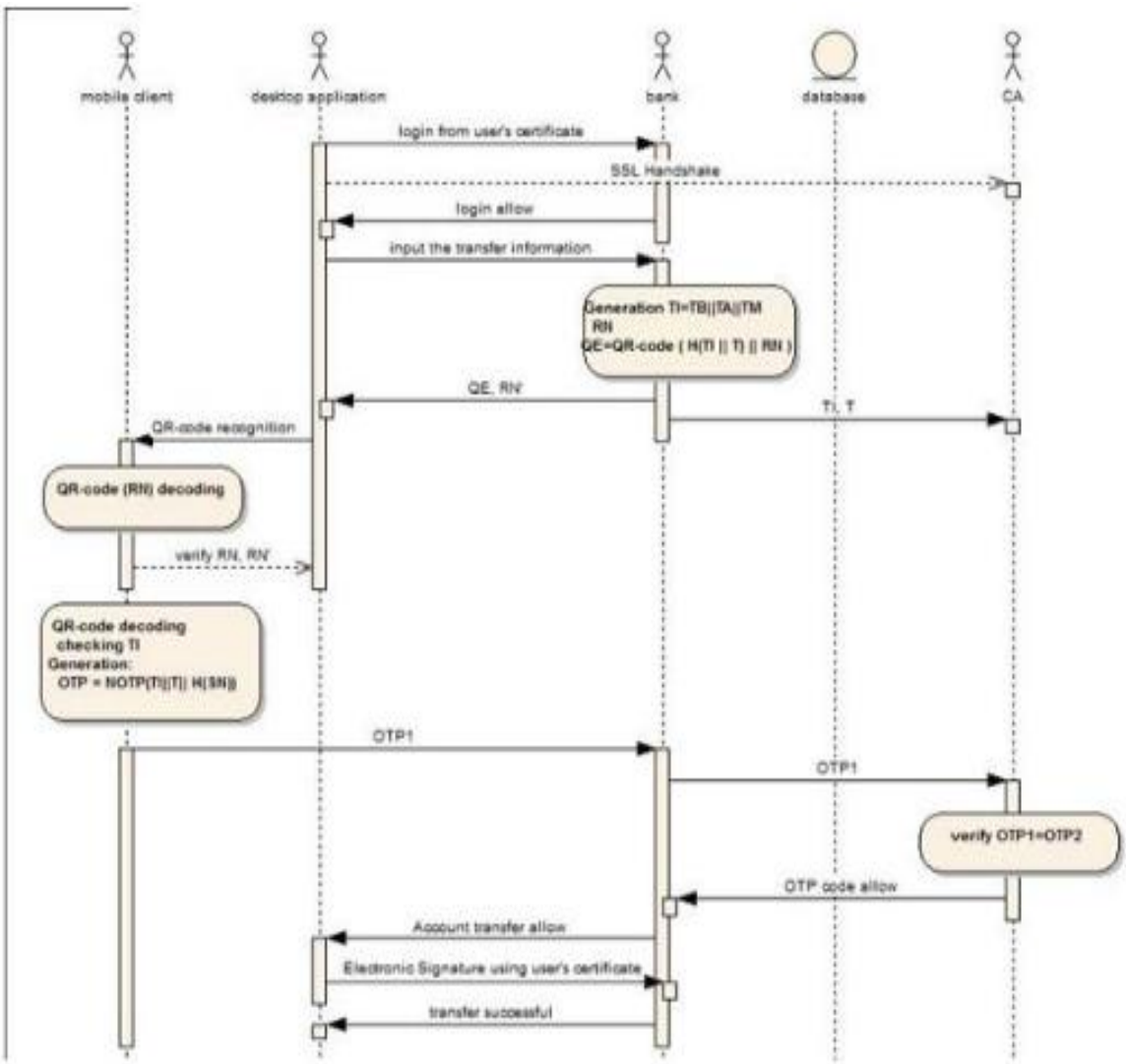

Figure : Working scenario for e-authentication system

4.2 One Time Password

One-time password (OTP) is a type of security measures that allows one to log into a network or service once per session. This aids in the stoppage of identity theft by safeguarding the username or password and authentication is not used more than once. The user's login name is normally the same for each login, but the one-time password is different. As a consequence, the user will be verified for each session using a new OTP. They can also be used to avoid replay assaults, phishing attempts, and other types of attacks on standard passwords[12]. They also provide additional benefits like as anonymity, portability, and extensibility, as well as the ability to prevent information leak. Text messages sent over a

gateway, unique symbols, web-based methods, Secure Code devices, and Grid files are all examples of OTP transmission mechanisms. The most recent Grid file uses a hash type file to confirm the user's authentication request, which raises the possibility of manipulation. They all, however, deal with globally recognized text-based approaches. One-time passwords are a type of strong authentication that may help safeguard business networks, online financial accounts, and other systems with sensitive information.

OTPs solve a lot of the problems that come with regular passwords. One of the most severe flaws that one-time passwords solve is the fact that they are not subject to replay attacks or phishing attempts, unlike standard passwords. An intruder who collects an OTP that has already been used to enter into a service or execute a transaction will be unable to exploit it since the OTP has already expired. On the negative, OTPs are difficult to remember for humans

CONCLUSION

In conclusion, the system fulfills the high security demands of online users and protects them from a variety of security threats. Furthermore, the system does not require any technical knowledge, making it incredibly user-friendly. As a result, the E-Authentication system shows to be adaptable while also being useful to both consumers and vendors in terms of enhancing efficiency. As a result, most businesses utilize it to advertise and market their products. OTPs are sent in the form of a picture, making it difficult for an intruder to identify the presence of sensitive data. An email message with the OTP is sent to the concerned individual. Net-banking customers may easily access their email accounts and retrieve the encrypted OTP by scanning a QR code. As a result, only software installed by the financial institution with the QR image may understand the QR code in a secure transfer. The use of the AES method to encrypt one time passwords adds to the system's security. The system is more sophisticated than any other system now in use, and it is evident that the time necessary to crack it will be longer than the usable lifetime of OTPs. OTPs are only created once each session and have a limited lifespan. After the OTP has expired, it is not able to utilize it. The widespread usage of QR-code makes the process more user-friendly. Even a novice user with a basic understanding of how to use a computer system can familiarize.

REFERENCES

[1] Tiwari, S. (2016, December). An introduction to QR code technology. In 2016 international conference on information technology (ICIT) (pp. 39-44). IEEE.

[2] Sharma, M. K., & Nene, M. J. (2020). Dual factor third- party biometric- based authentication scheme using quantum one-time passwords. Security and Privacy, 3(6), e129.

[3] Saranya, K., Reminaa, R. S., &Subhitsha, S. (2016, March). Modern applications of QR-Code for security. In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 173-177). IEEE.

[4] Karim, N. A., &Shukur, Z. (2016). Proposed features of an online examination interface design and its optimal values. Computers inHuman Behavior, 64, 414 422. https://doi.org/10.1016/j.chb.2016.07.013.

[5] Alexandre, B., Reynaud, E., Osiurak, F., & Navarro, J. (2018). Acceptance and acceptability criteria: A literature review. Cognition, Technology & Work, 20(2), 165– 177. https://doi.org/10.1007/s10111 018-0459-1.

[6] Karim, N. A., &Shukur, Z. (2015). Review of user authentication methods in online examination. Asian Journal of Information Technology, 14(5), 166–175.

[7] Srivastava, S., &Sivasankar, M. (2016, August). On the generation of alphanumeric one time passwords. In 2016 International Conference on Inventive Computation Technologies (ICICT) (Vol. 1, pp. 1-3). IEEE.

[8] TeSLA. (2016). The TeSLA project home page. https://tesla-project.eu/. Accessed 18 Feb 2018.

[9] Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019). E-authentication for online assessment: A mixed-method study. British Journal of Educational Technology, 50(2), 861 875. https://doi.org/10.1111/bjet.12608.

[10] Jain, A. K., Ross, A., &Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4 20. https://doi.org/10.1109/TCSVT.2003.818349.

[11] Moini, A., &Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems perspective. IEEE Systems Journal, 3(4), 469 476. https://doi.org/10.1109/JSYST.2009.2038957.