International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 9, pp 75-81, September-2022

https://doi.org/10.47001/IRJIET/2022.609012

E-Authentication System Using QR Code & OTP

Mohammed Awad Mohammed Ataelfadiel

Department of Computer Science and Information, College of Sharia and Islamic Studies at Al-Ahsa, Imam Muhammad bin Saud Islamic University (IMSIU), Saudi Arabia
College of Computer Science and Information, Open University of the Sudan, Sudan
E-mail: maataelfadiel@imamu.edu.sa

***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.**

Keywords: e-authentication, QR-Code, OTP, One time Password, e-authentication systems.

I. INTRODUCTION

Security is extremely important while accessing services in a web context, more so for the consumer and the supplier. The accessed information must be managed in such a manner that its security is not jeopardized. Passwords are secure if they are kept secret by the user. Not everyone understands the dangers of leaked passwords and other security breaches. Client-side assaults against online banking and electronic commerce have recently increased as a result of a lack of security knowledge among end users. As a result, the end user would be unaware whether their computer or platform had a vulnerability that may lead to attacks on the client-side. Today, the passwords are by far the most used authentication technique. To accomplish any web-based financial exchange, the online user will be required to input his or her password into an online system. The need for more advanced security measures for transaction verification in the online environment grows as technology improvements continue to affect how society pays for products and services. This study proposes a solution to the problem by merging multiple authentications and techniques to give an enhanced and safe online transaction between the client and the server in order to alleviate these security difficulties. Also, this study offers an anti-form snatching strategy that prevents an attacker from "grabbing" sensitive data and altering it as it is given to the server by the client, as well as protecting online content. The system additionally reduces the danger of online assaults by employing One Time Passwords (OTPs), which only validate one login session within a given period of time, as well as the usage of email as a secondary verification channel.

II. LITERATURE REVIEW

To target internet consumers, cyber thieves are employing more and more complex ways. What makes some online attacks difficult to detect from the client side is that any activity appears to originate from the legitimate user's web browser, and as a result, the information of the user's account details is silently changed to the attacker's account details, which is extremely concerning. Financial fraud has resulted in significant losses. On a worldwide scale, the financial services industry has become a key target of cyber-attacks, with losses totaling $54 billion in 2009, up from$48 billion in 2008.[1].

The amount of internet attacks on financial institutions, particularly European consumer banking and corporate banking sectors, has increased exponentially in 2010[2]. Hackers seek the most sensitive data, such as account numbers and amounts, and manipulate it for their own gain. The data supplied to these institution servers must be trusted, that is why an upgraded security program has to be built to combat these security issues.

According to Verizon Communications Inc., New York's Data Breach Investigation Report, 63,000 security events were reported in 2014 from 95 countries across the world, with authentication assaults being the most serious danger to businesses (http://www.verizonenterprise.com/DBIR/). Single factor knowledge-based authentication systems, such as username and password, are insufficient to protect against authentication assaults. The different approaches described in the literature do not provide any one-of-a-kind or general solutions for delivering a reliable and secure authentication system. However, these strategies have several drawbacks, such as lower accuracy and longer processing times. Using biometric features and two-dimensional barcodes, there are various variables for authentication.

Smart cards are commonly used for authentication based on ownership. The widespread use of mobile phones and smart gadgets has necessitated the development of a mobile phone and Quick Response code-based authentication system[3].

For authentication, the biometric template can be integrated in the Quick response code. To allow quicker and more efficient authentication, authentication systems must be integrated with smart devices. One of the biggest drawbacks of biometric systems is the amount of time it takes to register and identify yourself. It takes a long time and is inconvenient to extract biometric characteristics from a group of users. Automatic authentication systems carry out the process without the user's awareness, making them more efficient [2].

Increased cyber assaults during online financial transactions have necessitated the development of safe and efficient authentication methods. For this, encrypted QR codes can be utilized. In the literature, several multimodal biometric systems have been described. Because the modalities used in them are open to spoofing assaults, spoofing is feasible regardless of the type of fusion. Because vein-based modalities are less susceptible, efficient fusion is required.

The majority of current authentication research focuses on the many techniques of obtaining biometric features from the user. With increase in internet users, the number of different types of authentication assaults also increases. As a result, improving the security of authentication systems becomes a critical topic to solve, prompting the author to investigate several forms of authentication systems. Emerging trends in computationally intensive applications need more effective authentication systems.

Despite its widespread use, the existing e-authentication system has a number of security vulnerabilities because it is based on a traditional password-based prototype with no mutual authentication between the user and the financial institution server, which leaves the user vulnerable to spam and phishing, intercepting communication channels, database hackers, and so on. The following authentication method might be effective for making transactions more secure while keeping them simple for the user. By employing https communication between the user and the server, the proposed authentication method guarantees approved certificates that are used for user authentication and digital signatures. The QR-code is produced and shown to the user's screen, decode it with the user's mobile phones to generate OTP using the user's transfer information, desired transfer time, and the serial number of the user's mobile phones instead of a security card. OTP is also created on the server side, and both the OTP generated by the user device and the OTP generated by the server are confirmed before proceeding. To avoid data leaking, the user database should also be secured.

Any authentication method, no matter how good it is, is useless if consumers refuse to use it [4](Karim &Shukur, 2016). As a result, it's critical to investigate the acceptability of e-authentication technologies. Acceptability is a favorable mental image that a user has of a tool before utilizing it [5]. The perspectives of various students give useful information to both the inventors of e-authentication tools and the HEIs that use or plan to employ them. A student may refuse to utilize an e-authentication system that is ineffective or inefficient, poses too many hazards, or is simply inconvenient to use. DLEs should have strong and dependable security systems to ensure their reliability, according to new European regulations [6].

According to [7], trust is a critical component of any new technology's success, particularly in education, and trust in e-authentication appears to be complicated. Biometric authentication, for example, may improve the user experience by reducing the need to establish and remember passwords; but it also introduces new issues, such as privacy concerns [6][8].

According to [7], there are many layers of trust associated with the institution, e-authentication tools, deployment of the tools, usage of the obtained data, and the process' results. Furthermore, according to [9], acceptance is a critical factor in biometric systems since it reveals how eager individuals are to reconcile the use of biometric identifiers in their daily lives.

E-authentication, according to [10], is a unique process at the moment. There is a modest body of literature that deals with the impact of e-authentication systems on different types of end users. Okada, Whitelock, Holmes, and Edwards [10] investigated the perspectives and experiences of 328 Open University (UK) higher education students who utilized an e-authentication system built as part of the TeSLA project [11]. They claim that students in distant education had a generally favourable attitude toward e-authentication technology. However, there were some critical replies as well. Students with disabilities, for example, were more likely to reject e-authentication owing to worries about their specific educational needs, according to the responses. Women were less eager to submit personal data than males, and younger students were less likely to utilize e-authentication owing to worries about data privacy and security. Students' requirements should also be considered in the context of e-authentication, according to [10]. As a result, it's crucial to understand how different pupils react to electronic identification. Researchers, for example, are still learning about SEND students' perspectives on the usage of e-authentication.

III. BACKGROUND

3.1 (QUICK RESPONSE) QR code

The Japanese organization Denso Wave devised a QR-code, which is a Matrix code and a two-dimensional barcode. Information is encoded both vertically and horizontally; allowing it to carry up to a couple of times more data than a traditional barcode. Data is obtained by taking a snapshot of the code using a camera (for example, one integrated with a mobile phone) and then processing the image with a QR scanner [3].

This technology has been around for almost a decade and has evolved into a vehicle for advertisers to reach advanced mobile phone users. QR Codes, or Quick Response Codes, are nothing new. To be honest, they've been employed as a piece of advertising and stock control in Japan and Europe for the previous ten years. One-dimensional (1D) barcodes have a lesser level of security than two-dimensional (2D) barcodes.

Filtering the lines and spaces in 1D barcodes makes them very easy to read. Human eyes have a hard time seeing 2D barcodes in a visual design. One-dimensional barcodes must only output in one direction in order to be relevant. If a scan line's goal did not fit within a range, the data would not be properly examined. 2D barcodes, on the contrary, offer a large selection of scanning options. The quantity of data they can save and convey is the fundamental distinction between the two. QR codes are two-dimensional grid barcode that may hold information in the form of numeric characters, alphabetic characters, and kanji characters. Scanner tags are one-dimensional codes with a maximum capacity of 20 digits [3].

They are appropriate for autonomous companies because of their capacity to hold more information and their comfort. When scanning or channeling a QR-code with iPhone, Android, or other camera-enabled phone, sophisticated content on the web may be connected into, or initiate different phone limits like email, IM, and SMS, and link the phone to a web application.

The QR code as security measure has proven to be of importance in that;

i. Your Online and Offline Media are connected by them

Flyers, brochures, billboards, and business cards are examples of print media that are not linked directly to internet media such as website. That is, unless QR-codes are provided. QR codes are being used by an increasing number of B2B businesses to connect their print media to their websites. This eliminates the addition of website address or phone number in that potential customers can simply scan the QR code and be taken straight to the organization's website.

ii. Quick an error-free

A URL is the only option to link people to internet information if QR Codes aren't available. On a smartphone device, however, inputting a URL is inefficient and cumbersome. Customers are also more likely to to make typing mistakes. Scanning a QR Code, on the other hand, is a significantly quicker and error-free operation.

iii. Rich content engagement

Marketers may share rich material via print marketing by using QR Codes. As a result, they will experience an increase in audience engagement. Chef's Basket, for example, included a QR Code on the container of one of their pasta items. When scanned, the QR Code takes them to a video of the pasta dish's recipe.

iv. Actionable

You may make your promotions interactive and collect feedback from your target audience by using a QR Code. You may hold a contest, solicit registrations for a product or event, get feedback, or allow customers to purchase directly from a newspaper ad or flyer.

v. Trackable

If you're a marketer, you're well aware of the value of analytics. It allows you to learn a lot about your target audience. As a result, you will be able to discover your areas of strength and weakness.

However, unlike digital media, print media has no tracking capabilities on its own. This is where QR Codes come in handy. QR codes allow you to track the scanning activity of print media marketing campaigns, which helps you measure their effectiveness. How many people have scanned it, when they scanned it, and where they scanned it.

It also has a function called event tracking. It describes how users engage with the QR Code's content after scanning it.

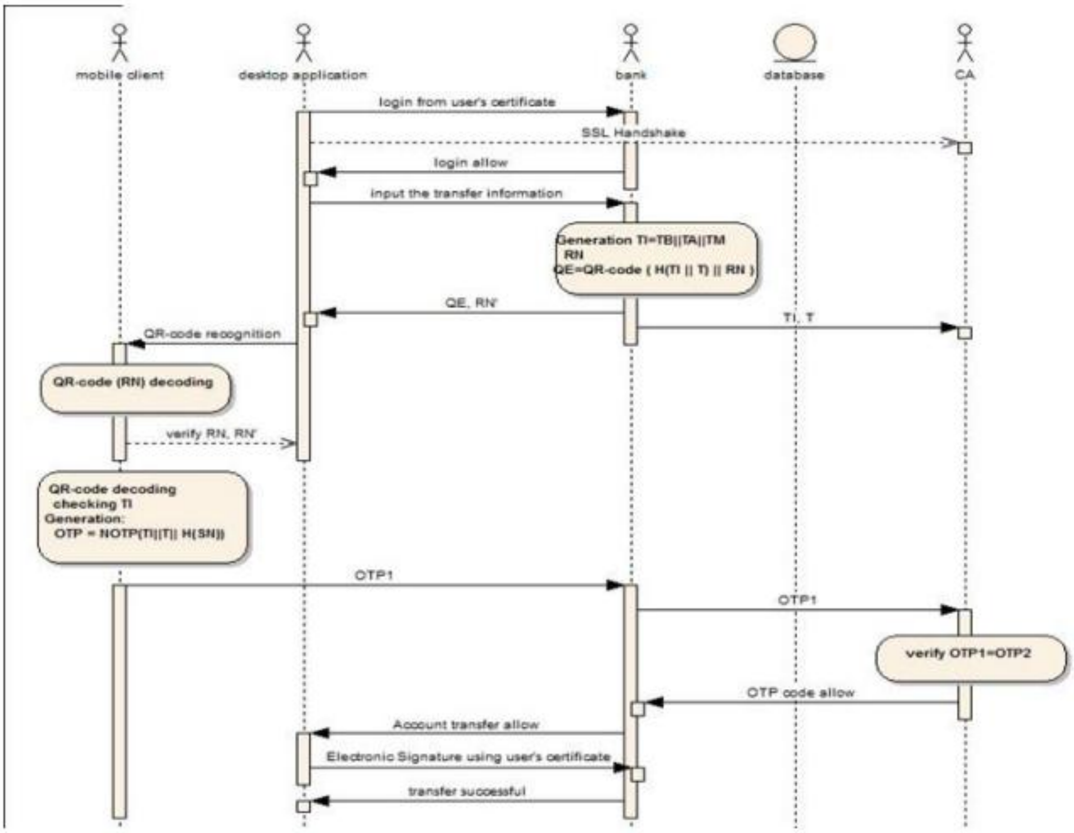

Figure 1: Working scenario for e-authentication system

3.2 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[12].

IV. APPLIED STUDY

4.1 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.

ISSN (online): 2581-3048
Volume 6, Issue 9, pp 75-81, September-2022
https://doi.org/10.47001/IRJIET/2022.609012

4.2 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.

4.3 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.

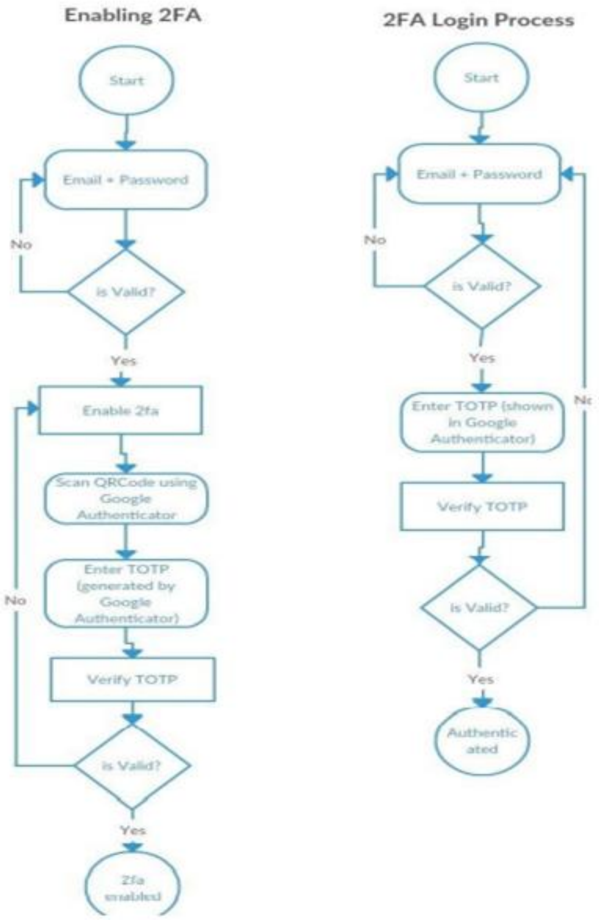

Figure 2: Flow Chart of E-Authentication Login Process

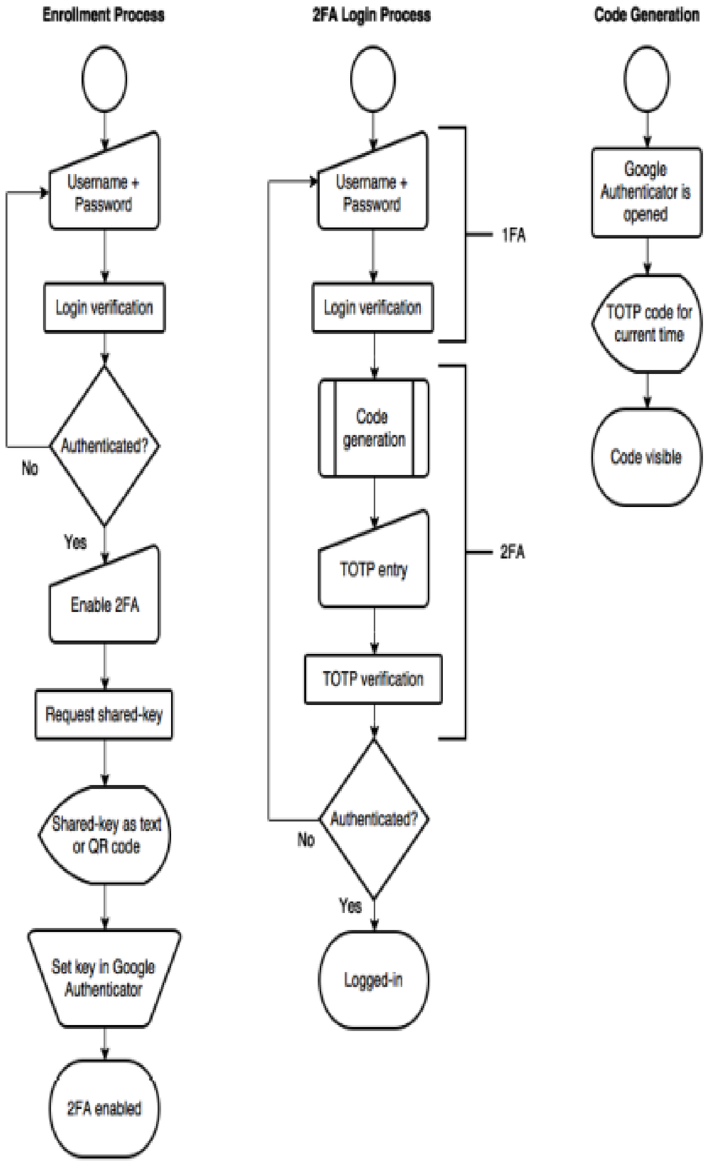

Figure 3: Flow Chart of E-Authentication Login and Code Generation Process

4.4 Data Flow Diagram

Data flow diagrams are visual representations of system. DFD is one of the most brilliant structural analysis tools available. A bubble chart is another name for it.

ISSN (online): 2581-3048
Volume 6, Issue 9, pp 75-81, September-2022
https://doi.org/10.47001/IRJIET/2022.609012

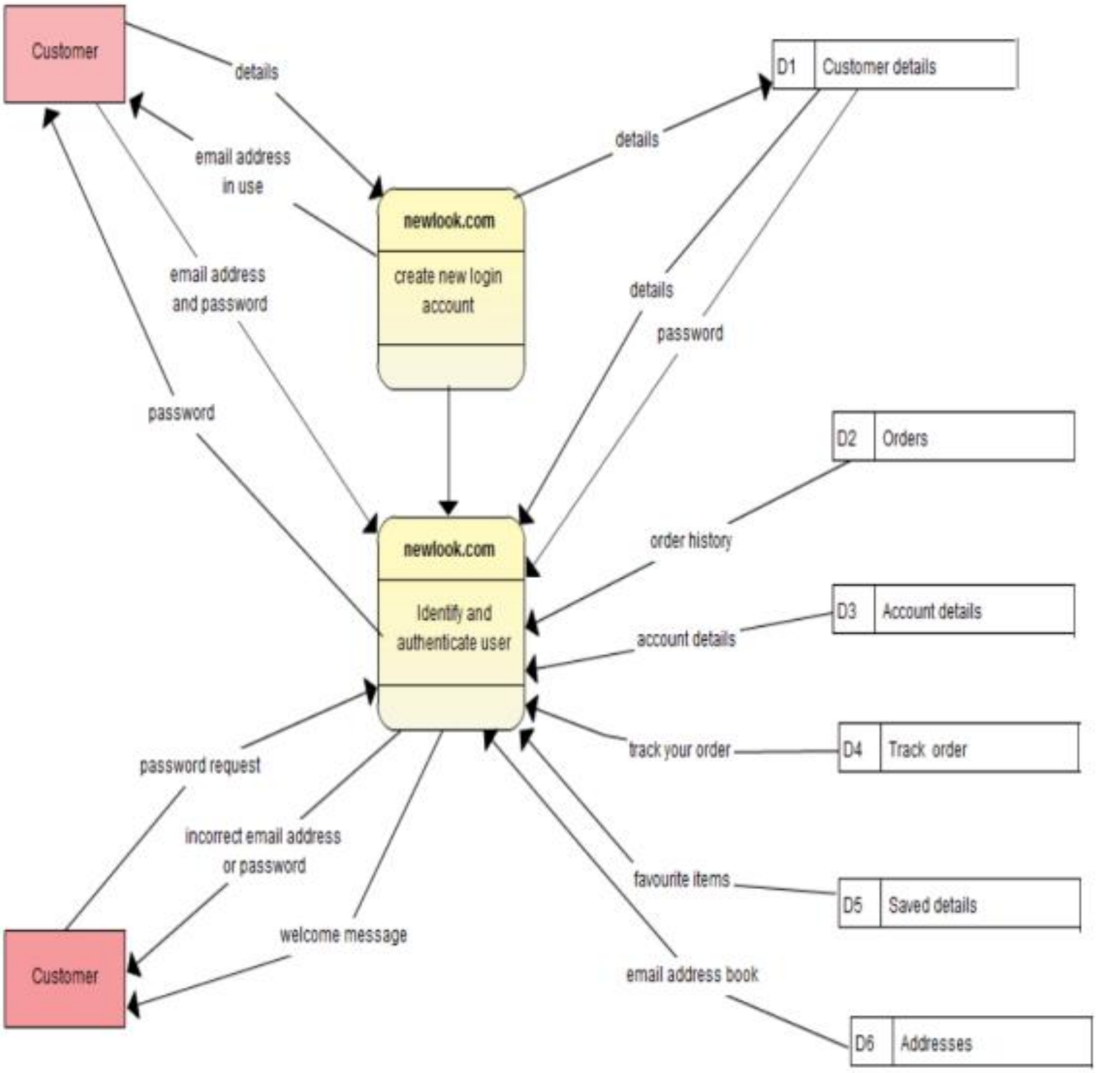

Figure 4: Data Flow Diagram of E-Authentication

V. 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] Edwards, C., Holmes, W., Whitelock, D., & Okada, A. (2018). Student trust in e-authentication. In Proceedings of the Fifth Annual ACM Conference on Learning at Scale, UK, Article No.: 42, 1–4. https://doi.org/10.1145/3231644.3231700.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

Citation of this Article:

Mohammed Awad Mohammed Ataelfadiel, “E-Authentication System Using QR Code & OTP” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 9, pp 75-81, September 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.609012

****