An Improved Time-Based One Time Password Authentication Framework for Electronic Payments

Md Arif Hassan[1]*, Zarina Shukur[2], Mohammad Kamrul Hasan[3]
Center for Cyber Security, Faculty of Information Technology
National University Malaysia (UKM), 43600 UKM, Bangi, Selangor, Malaysia

***Abstract*—One-time Password is important in present day scenario in the purposes of improving the security of electronic payments. Security sensitive environment or perhaps organization avoid the resources from unauthorized access by allowing different access control mechanism as user authentication. There are several safety issues in one Password based authentication. However, studies show that OTP sent over SMS are causing different causes and issues, which lead to precious time, delay in transaction. User authentication can be raised with more levels within the procedure of multi-factor authentication scheme. Time-based One-time Password and biometrics are one of the widely accepted mechanisms that incorporate multi-factor authentication. In this paper, we approach the Time-based OTP authentication algorithm with biometric fingerprints to secure an electronic payment. This algorithm uses a secret key exchanged between the client and the server and uses a certain password through the algorithm. The shuffle of the TOTP approach better wear by screening the key as being a QR code, as revealed in the majority movable applications are able to read. It offers confidentiality at the application level within the system to protect user credential within equal entities (the user and the server) for preventing brute force and dictionary attacks. Thus, the proposed system design is possible for users because of the lack of the concern of holding its own hardware token or additional charges from the short message service. Our suggested approach has been found to improve safety performance substantially compared to existing methods with regard to authentication and authorization. This research hopes to boost research effort on further advancement of cryptosystems surrounding multi-factor authentication.**

Keywords*—Electronic payments; One Time Password (OTP); Quick Response (QR) code; Time based One Time Password (TOTP)

I. Introduction

Mostly all online services and the websites are today implementing multi step authentication to offer protection to the customers of theirs. Multi-factor authentication is a technique of the digital device access influence that a person is able to pass effectively showing different authentication stages. In this, rather than asking only the individual piece of info as passwords, users are requested to provide a number of extra info and that helps make it harder for any intruder to bogus the identity of the real user. This info could be an OTP that will be delivered by the server on the registered mobile of consumer or perhaps there could be certain security concerns. This particular procedure makes it hard for the opponent to access the internet account even if the assailant understands the username as well as password of the user. This more info is able to consist of different aspects as fingerprints, security tokens [1], biometric authentication, and so on. It has emerged as an alternative means to enhance protection by needing the user to give over one authentication factor instead of just one password. Authentication issues are of those kinds: Knowledge - something which the person knows [2], like a password and a username; Possession - a thing the person has specifically a hardware token [3]; Inherence - a thing verifies the person is, like fingerprints, iris, facial recognition, palm print [4-7]. Biometrics technology enjoys a wider acceptance because of including fingerprint biometrics and more user-friendly applications on digital devices [5]. Two forms of biometric authentication are available, respectively physiological and behavioral approaches [8-9]. Fingerprint is the most popular biometric process. As authentication is highly user friendly, it is increasingly used to login functionality in fingerprints [10]. Among the many other applications of theirs, QR codes are popular for the multi-factor authentication to transmit info through the authenticating device on the mobile device which is accredited as being an AIM Standard, an ISO standard and a JIS Standard [11]. In the beginning, the QR code is created to be utilized in the auto industries. However, these days, it has been popular in the ad so that a customer is able to utilize the smartphone and scan to find out much more info about the marketed products.

The barcode scanner programs are developed that are suitable for smartphones as IOS and android. QR Code is a kind of 2D bar codes that was created by Denso Wave, within 1994 [12]. The symbol things in 2D bar codes include light and dark squares. The 2D specifications set the encoding of the information, the dimensions of quiet zones before and also after the barcode, the finder or maybe place detection patterns, as well as blunder detection and correction of information [12]. Barcodes present an inexpensive and simple way to encode textual info about objects or items in a type which machines are able to read, retrieve, validate, and procedure [12]. The QR code has the increased capacity that will keep 7,089 numeric, 4,296 alphanumeric, and also 2,953 binary characters [13]. Now, QR Codes have forty designs, which range from one to forty, so the scale of each edition is different. The size of QR code is dependent on the vertical and horizontal sizes of the QR version employed [14]. It can be checked out with smartphones equipped by using a digital camera. A software program client placed on the smartphone controls the camera to browse and understand the coded info, letting mobile users to connect to the net with a point and click of the phones of theirs, therefore making mobile surfing easier. It's clear by reasonably equipped mobile cell phones with cameras and also QR

*Corresponding Author

scanners, info like Url, SMS, contact info and plain text could be embedded into the two dimensional matrix [13]. Data can be encrypted inside a QR code to offer the confidentiality of info lodged in the code [15]. The barcode and QR code are presented in Fig. 1, respectively.

One of the more trendy implementations is Google authenticator that is working with QR codes. The shuffle of the TOTP approach better wear by screening the key as being a QR code, as revealed in the majority movable applications are able to read. This is easier and acceptable to utilize in looking at the mechanical input of the same secret. After the TOTP authenticator is enabled, owners are going to be ready to allow MFA individually within their user profile that adds a layer of protection and postulate an added authentication code from a dependable device. Fig. 2 displays the TOTP based QR generation procedure flow diagram [16].

Several authentications methods have been developed to ensure the security of electronic transactions. Until now, there are many methods used for authentication in electronic payment. Onetime passwords (OTP) are produced on demand by Internet centralized party and delivered to the customer via a correspondence channel in which a registered getting device is assumed to have the client's possession. Probably the most prominent illustrations will be the SMS OTPs given by banking apps [17]. The majority of the OTP authentication methods are network reliant. The issue is that network-dependent devices provide a secure network connectivity between the device and the authentication server. For instance, SMS based program is going to need to transmit onetime password via an SMS within the user device. As in deep SMS primarily based two-step verification methods, the server will send out an SMS on the user's device, the person might have to purchase the price of SMS. The issue with SMS based OTP is it is just and the SMS network the cell phone is subscribed to? Recent studies show that OTPs over SMS are causing different causes and issues, which lead precious time, delay in transaction [18]. SMS OTP might also have financial problems in case the carrier charges the subscriber for having SMS communications. In this paper, we approach the Time-Based OTP Authentication Algorithm for electrical payment. There will be no spoofing or perhaps tempering of the transmitted information in between. In this manner, only legitimate user will gain a chance to access the account. The entire program will operate with absolutely no system expecting the registration stage. The proposed system maintains zero SMS policy with no additional charges for SMS. It will encrypt and secure the information inside the system from any misuse.

We structure this paper into seven sections. Section 1 discussed above together with introducing the multi-factor authentication techniques. Section 2 offers a brief knowledge of the literature review with OTP techniques. Section 3 points out the part of the proposed method architecture. Section 4 presents the system architecture of the proposed system and result and implementation are presented in Section 5. Section 6 discussion on performance key factor and Section 7 concludes the paper.

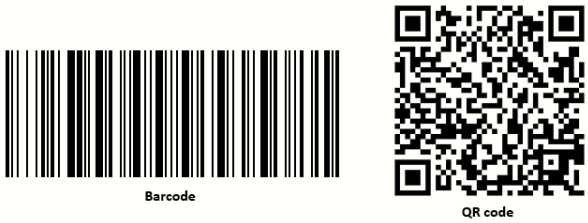

Fig. 1. Barcode and QR Code.

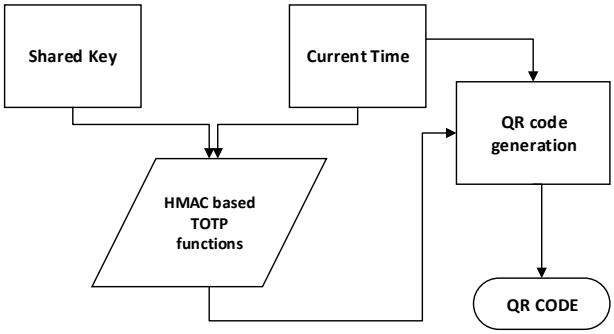

Fig. 2. TOTP based QR Generation Procedure Flow Diagram.

II. Literature Review

To preserve details on the net as protected as servers and possible, many clients implement different kinds of cryptographic methods to encrypt sensitive details and authenticate individuals at the opposite end of the connection [19-20]. Today that much more confidential information is stored virtual [21], it is supreme that community security oak updated with modern threats [22]. The bulk of sites in use today use the conventional verification pattern of supplying a password and a username more than a secure interconnection. The user name is used-to find what online account a client would like to access, even though the password is accustomed to confirming the identity of the customer. However, it seems secure in concept several passwords even now wind up being affected [23-24]. This is because of two things: vulnerable passwords and also quicker password cracking hardware [25-26]. In order to stop these attacks, two-factor authentication contemplated solving securing online transactions and also identifying the authentic individual and logging them right into a method or even the program.

The most used method of boosting the protection of an account is asking for additional info out of the computer user. Rather than asking only one piece of info out of the person, the server can ask for additional info, making it a lot harder for an assailant to bogus the identity of the person. With the hand of the fantasy, they have approached the OTP primarily based authentication [27-28], do the related work approach by [29]. A onetime password (OTP) method depends on the capability for just a unit to make a onetime code that will be delivered towards the server for verification. If the code is discovered to be accurate, subsequently that consumed is provided a chance to access the account. A onetime Password (OTP) is the one of the important part of the mobile networking [30]. OTP is a password or maybe code that is effective just for one login session or maybe transaction holding a computer or maybe

some electronic device. OTPs had been released to stay away from the flaws, which are connected with fixed passwords. Even though they are legitimate for a little time and they also instantly expire after the specified time span. A technological mechanism to reduce the risk of an unauthorized person getting to access the account. The most important advantage of OTP is in contrast to a static password. OTP, security technique shield for the various password-based attacks, specifically password sniffing and reply attack [31]. TOTP is one of the principal requirements for the onetime password. In generally, TOTP, the token creates a numeric code, typically six or maybe eight digits [25]. TOTP makes use of time in increments known as time action, and that is typically thirty or maybe sixty seconds. What this means is that every OTP is legitimate for the duration of the precious time action. The TOTP is regarded as a much more safe Onetime Password remedy. A high-level diagram of TOTP enrolment process are shown in Fig. 3 [23].

A Time-based authentication of multi-factor tokens improved cryptocurrency security approach by [32]. Tahar et al. (2019), in their research, they developed the protection and enhancement algorithm for MFA Crypto-monetary (CR) to set up an additional safeguard layer when looking for the target through the onetime password (TOTP) technology in time. The user first requires a username and password for logging into every 2FA-enabled entity; as a second factor, the user will then create a TOTP virtually through the token. A similar concept based TOTP based challenge response protocol for e-commerce approach in [33]. Aina et al. (2018) on their paper, they approached Scan2Pass payment for banking system. The system is depended both server side and client side. After the registration in server side, the user needs to input their username and password and generate a QR code. In client side, the user has to open; his mobile application to screening the QR code after input the user authentication details. Do the similar work proposed by [34]. Abhishek et al. (2020), in their article they proposed TOTP Based Authentication Using QR Code for payments. The QR code is read, and the system tracks the TOTP on the server side. The consumer is permitted to join whether this TOTP matches in the QR code. Moreover, Chowdhury et al. [35] suggested the usage of OTP and QR code for payment transfers in the online banking system.

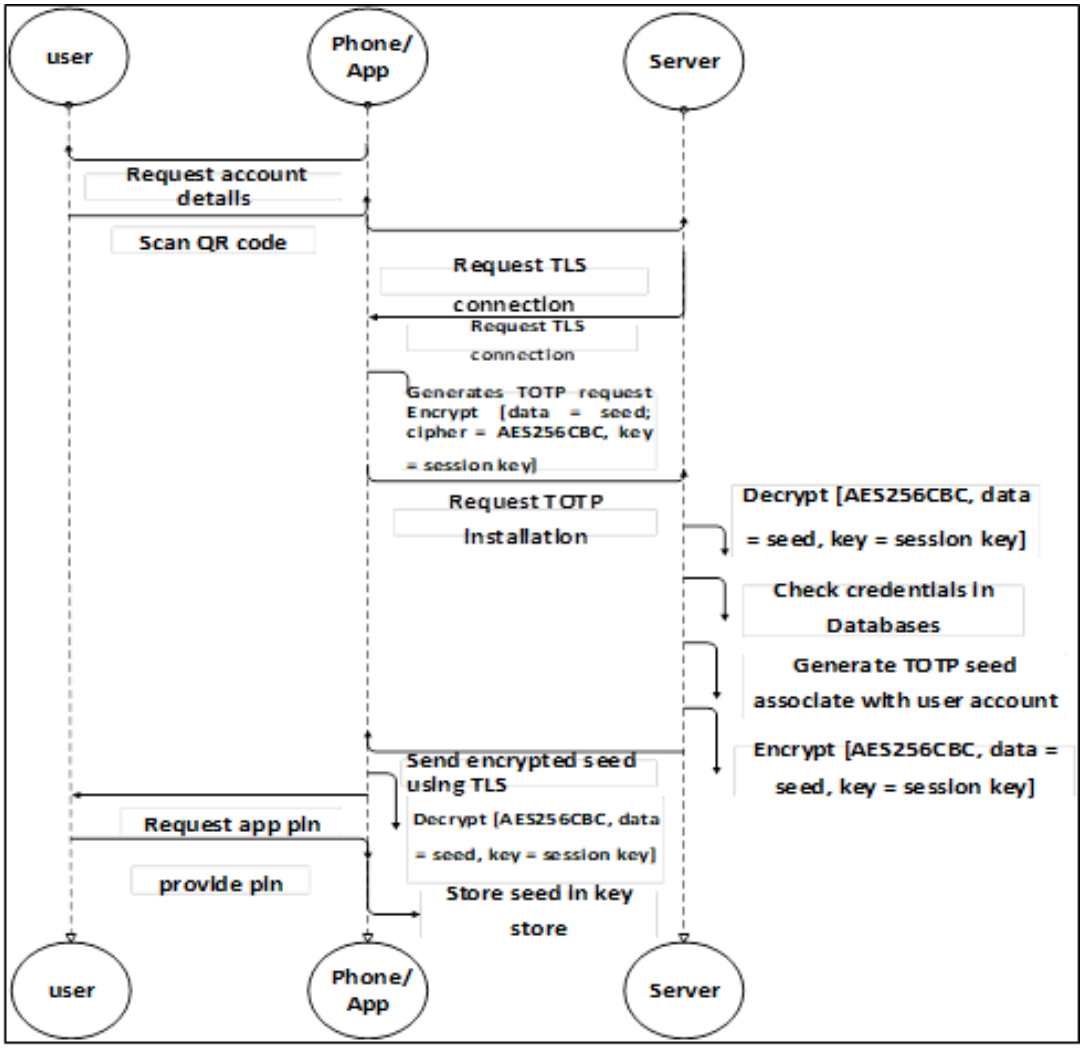

Fig. 3. A High-Level Diagram of TOTP Enrolment Process.

A QR code along with a secret key shared between the client and the server is generated in this system and is used to generate an OTP, which is integrated into the QR code. For the transaction to be completed, this QR code is then checked to verify the OTP. A new OTP must then be created for every session to provide additional protection. In addition, a TOTP based two-factor authentication using smart phones as software tokens proposed in [36]. The proposed system would use mobile phones to create software tokens that will be used to authenticate an Internet Banking application, using specific onetime passwords (OTPs). The user ID, IMEI phone number, timestamp and PIN of the server compute the mutual secret of the TOTP algorithm on their device. After the analysis of the previous study, it can be found that most of the study proposed username and password based authentication system along QR code. Furthermore, the can be improved using biometric features for client side authentication. Authentication techniques, which hinge on much more when compared to one component, typically are tougher to compromise as opposed to just one element system. There is a strong need to produce the strategy powerful and efficient a multi-factor authentication component is necessary to boost protection for electronic transactions. Table I lists the existing systems and their proposed properties.

TABLE I. RELATED METHODS WITH THEIR PROPERTIES

Author	Method	Finding	Drawback
Tahar et al. [32]	Password /TOTP	This study proposed a framework for the security enhancement of the Cryptocurrency using time based token. The user first needs username and password, then user the TOTP token for authentication.	In password-based authentication, many security issues exist. Intruders may try different methods to steal passwords using password-based attacks.
Aina et al. [33]	Pin/TOTP	This study has proposed a challenge–response protocol for enhanced e-commerce security using time based token. The proposed Scan2Pass method used pin for authentication.	In pin -based authentication, various security issues exist. Intruders may try different methods to steal passwords using password-based attacks.
Abhishek et al.[34]	Password /TOTP	This study has proposed TOTP Based Authentication Using QR Code for Gateway Entry System. The proposed technique used username and password for TOTP authentication.	In password-based authentication, many security issues exist. Intruders may try different methods to steal passwords using password-based attacks.
Choudhary et al. [35]	Password /OTP	This proposed technique used Mobile OTP with the combination of QR-code, which is a variant of the 2D barcode. The proposed method used username and password for OTP verification.	Security challenges with password-based authentication are many. Intruders may use password-based attacks to attempt various ways of stealing passwords.

III. PROPOSED SYSTEM

In the proposed method, we have utilized TOTP as a starting algorithm to produce needed onetime passwords. TOTP is dependent on HTOP; However, HTOP is used counter whereas TOTP is a time-based algorithm. TOTP is going to generate an innovative worth after a determined period. This particular occasion is known as the time step. TOTP supports HMAC-SHA2 and HMAC-SHA1 hash functions [37]. The proposed system has two phases, namely: registration stage, an authentication phase. A comprehensive explanation of each phase is provided below. Before making use of this service, the user should register the information of theirs during a procedure known as the registration phase. Verification of that information may just be achieved by a procedure known as an authentication phase. Each of the suggested materials and strategies are completed in the system during both registration process as well as the login procedure, their process flow is reviewed in this area. In Table II, we provided the symbol used in the proposed technique.

$$ENTOTP = EN\ (PKIDi\ (TOTP)) \quad (1)$$

$$ENTOTP = QRDEC\ (QR\ (ENTOTP)) \quad (2)$$

$$TOTP = DEC\ (ENTOTP) \quad (3)$$

A. Registration Phase

After the registration is done, the client app creates an eight digit onetime password (OTP) that may be utilized for the authentication aim. The registration process of the proposed system can be seen in Fig. 4. However the registration process of the proposed system as working as follows.

Step 1: The user input his credential information *IDi* on the server.

Step 2: The server determines the client's info and recovers the client's public key *PKIDi*

Step 3: the server then choices an arbitrary string TOTP, have a period slot, and encrypts it together with the public element to get (1)

Step 4: The server generates the *QR* code in the payment side.

Step 5: The client decodes the QR code with (2)

Step 6: The arbitrary string is encrypted together with the client's public key *PKIDi*, the client is able to read the *T*OTP string just over the device of user by (3) and type in the *T*OTP within the terminal with an actual keyboard.

Step 7: Registration Successful.

TABLE II. LIST OF THE SYMBOLS USED

Notation	Description
IDi	Client details identification
PKIDi	Client's public key
EN	Encryption string
*T*OTP	Times based one-time password
QR	Quick Response
DEC	Decryption

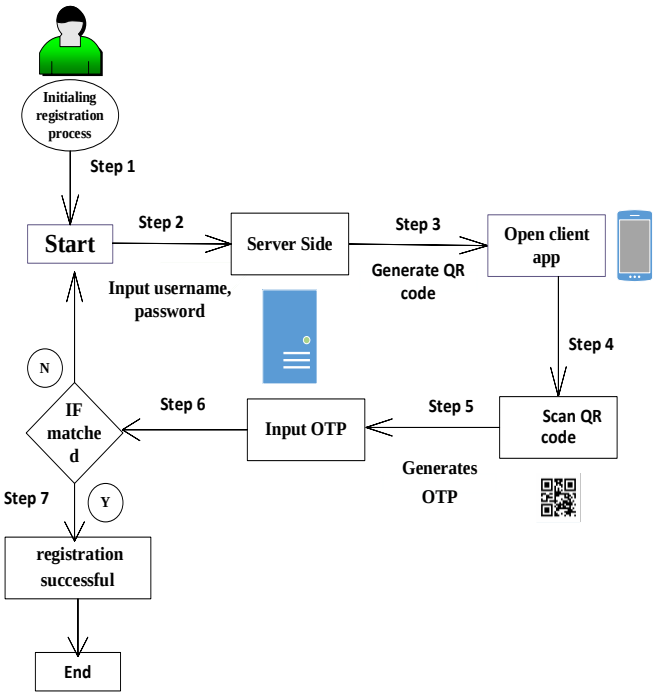

Fig. 4. Registration Phase.

B. Authentication Phase

The authentication service has to authenticate the client whenever the client wants to access the system. The authorization service checks server data and database identification Identities. The value submitted by the client would be compared to the current value of the server. When the values are both identical, the authentication is successful; the new value will be used to change the old value for the server. Otherwise, the authentication of the client will fail. Fig. 5 illustrates the method of authentication of the proposed system. The details authentication steps of the proposed system are mentioned below:

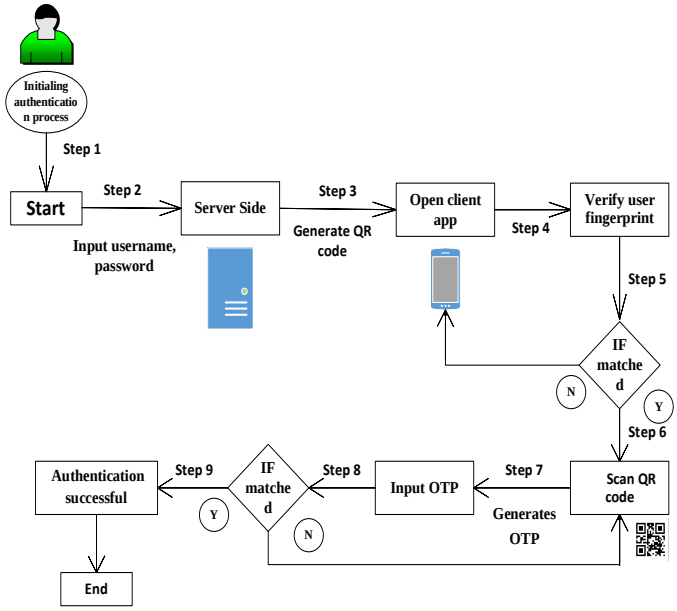

Fig. 5. Authentication Phase.

Step 1: The user input his credential information on the server.

Step 2: The server determines the client's info and regains the client's public key

Step 3: The server generates the *QR* code in the payment side.

Step 4: In user side, the user will open the application.

Step 5: The client input his fingerprint to verify

Step 6: Once the app verify the registered user, then the app ready for decode the QR code.

Step 7: the user will get TOTP number after decode the QR code.

Step 8: the user will input the TOTP number in the server side, if matched,

Step 9: Authentication successful.

IV. System Architecture

In this paper, we proposed TOTP based on authentication for enhanced electronic payments authentication security. The system design includes various entities, like a prospect, a smartphone, a user's PC and a server. The user is an individual with little to no knowledge of cryptographic codes, such as passwords and complicated mathematical equations. The terminal of a user is a computer of a user that is used to connect to a server for money transfers [38]. The user has a smartphone that stores the public key certification of the digital certificate or the server furnished with a camera. The server is the method entity belonging to the monetary institution that interrelates with the user by carrying out all the back end operations. In deep agreement with the present moment, TOTP uses a secret shared between client and server to produce a onetime use code [39]. Through executing the disgust secret through the algorithm, the client experiences the code with the server being able, during the whole algorithm, to confirm the published chip with a similar secret. The cipher is equally relevant for an imbued amount of time, usually thirty seconds [32]. The flow looks like firstly operator logs directly into an application program with username as well as the password, now view a text field asking to type in the newest launch and code TOTP client on their cell phone. Fig. 6 displays the proposed framework architecture of the proposed system.

The user gets a TOTP token by scanning the QR code. In the first phase, users open the Internet browser for login their account details getting a username password together with TOTP. Within the next stage, it provides an authentication need on the identity authentication server. In the last stage, verification on the request is used by confirming the allowed individual through identity authentication server. The request may be accepted in the last stage and maybe denied. The onetime password is made on the subject of the server using seed exchange, after which provided via a Transport Layer Security (TLS) tunnel about the client mobile program. The client will solely be authenticated whether it suits the password on the server on the server part. It is moreover secure than the SMS solution, since the transmission of the cipher is not intermediate. The function is the algorithm. To stay behind safe, mutual confidentiality should be reserved for this process.

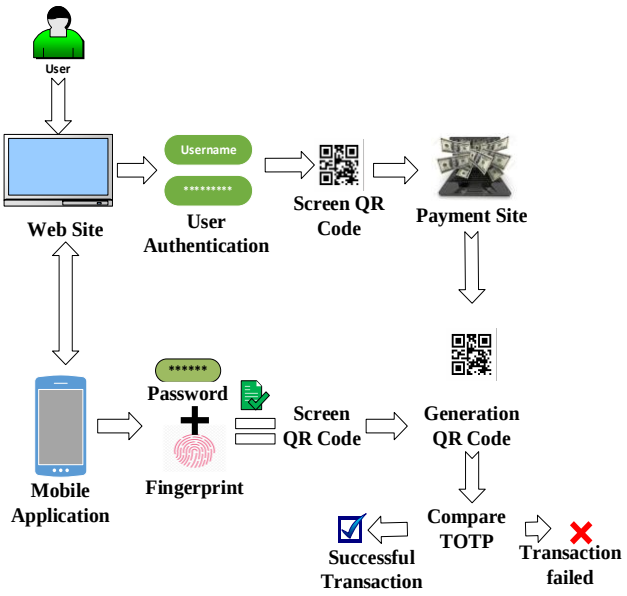

Fig. 6. Proposed System Architecture.

V. Design Consideration

The suggested solution works with a smartphone on the person's side. The smartphone plays a significant part within connecting the breach between the server and the user. In order to offer secure user authentication device, which works mutual authentication in between entities, thus, the proposed method uses the TOTP algorithm of RFC 6234 to compute the OTP required authenticating the user and finishing the login process [27]. The android application syndicates three components: the shared secret, timestamp and server challenge [33], in the mobile to make a token of 8 or more 8 digits so long as it applies the TOTP algorithm. Random details are essential, and they are utilized by the 8 bytes utilizes tokens and the shared secret. The system is depended both server side and client side. Some parameters are needed for the establishment of a TOTP authentication. The following steps are descrying how this framework works:

- For the TOTP generation, users and servers will know or be able to measure the current UNIX period.
- A secret key must be shared between user and server. The hidden key may be used as a pre-existing key between the parties. On the other side, the secret key may be produced by means of a main agreement protocol during agreement between the parties. This is a secure communication.
- The HMAC-Based One Time Password (OTP) will be the main component for the algorithm.
- The same time value is required for both the user and the server.
- For each user there must be a single specific private key.
- The key must be generated randomly or by key derivative algorithms and the keys should be protected from unauthorized access.
- In order to login, first-time users must register. At the registration stage, the user from the server will provide the QR code for authentication with the username and password.
- The user application runs on their device and needs user registered fingerprints on their phone to authenticate it.
- The registered device should only be used for a transaction, so each time a valid fingerprint needs to be checked.
- In order to access the system, the user is compulsory to input the approved fingerprints.
- Once users successfully enter the username and password, then the user side application needs to open a QR scan request. Remember that the user must encrypt their application via fingerprint before logging on the services.
- Complete after registration. The QR code scan page will be sent to the user with the same hidden key once the login is done and stored in the database. This key will produce the TOTP encoded in the QR code. Therefore, the QR code is verified using a QR code reader. The TOTP is then compared with the server TOTP.
- The user is permitted to enter if both TOTP match, otherwise access is not permitted.

VI. Discussion and Analysis

In this paper, we use the Time Based onetime password authentication algorithm to secure an electronic payment. The TOTP method is generally utilized in applications, which have to limit time like mobile banking and applications transactions. This section summarizes the key functionality and discussing regarding the OTP authentication system their methods. In the earlier methods found there are already various stages in the authentication task, as there they have worn SMS OTP Authentication within the authentication phase. Right here we have used TOTP its combat with specific QR Code of user that could be a fruitful method for supplying great protection on the authentication procedure. Here we have compared the usability considerations of SMS OTP and TOTP. The comparison of existing methods with the proposed system outcome is shown in Table III, where the usability considerations are discussed in Table IV for both SMS OTP AND TOTP.

The important paradigm of SMS OTP that is the Mobile Transaction Authorization Number, that's put on to authorize transactions of the person. In this particular mechanism, the OTP is delivered as a text message on the user's mobile device. Nevertheless, the protection of SMS OTP depends on the confidentiality of SMS, which is trusted by the security of movable networks [40]. While authenticator Apps count during a shared secret, which both the server and the App have to store. This "seed" is mixed with the period to produce the multi-factor authentication code. In our method, the TOTP based onetime password authentication for secure electronic payment process aims to be raised by utilizing TLS connection

between server and client Apps. Because the seed is discussed making use of the secure link, therefore it is never, exposed.

User verification has become more and more important than ever for electronic payments. Various authentication stages were described in previous approaches, as they did with the knowledge-based methods in the authentication stage. The security mechanism for usernames and passwords that can easily be accessed through guessing and password based attacks [41-42]. There is also a possibility to develop user authentication methods for multi-factor implementations. This study suggested a user authentication framework focused on TOTP for electronic payments that are concrete with biometric features. In addition, the proposed study recommends the possibility of biometric fingerprints verification during user authentication. The fingerprint method appears to be one of the most secure means for authentication in the electronic payments world in order to reduce future security vulnerabilities [43-44].

However, the proposed system is free of cost. The program-offering site likewise should make use of this product to improve the protection of the program, charging no extra cost. Because user have no SMS, services associated with the device so there will be absolutely no cost of SMS to user and server. This method could be lodged in a broad range of applications to provide multi factor authentication.

TABLE III. COMPARING THE RESULT OF EXISITNG AND PROPOSED METHODS

Attribute	**Tahar et al.** [32]	**Aina et al.** [33]	**Abhishek et al.**[34]	**Choudhary et al.** [35]	**Our method**
Authentication technique	TOTP	TOTP	TOTP	TOTP	TOTP
Method	Password	Pin	Password	Password	Fingerprint
Methods type	knowledge	knowledge	knowledge	knowledge	Biometric
Authentication type	Two-Factor	Two-Factor	Two-Factor	Two-Factor	Multi-Factor
Password based Attack	Yes	Yes	Yes	Yes	No

TABLE IV. COMPARING THE USABILITY CONSIDERATIONS OF SMS OTP AND TOTP METHOD

System	**SMS OTP**	**Our proposed method**
Token	Cellphone	Smartphone
Client App	No	Yes
Enrollment	SMS	QR Code
Derivation	SMS	Offline
Resettable	N/A	Yes
Cost	Not Free	Free
Service Access	Restricted	Worldwide
Service Provider	Cellular Network	Not Required
Secure Seed	Fixed	Dynamic
Availability	No	Yes

VII. CONCLUSION

Strengthened multi-factor authentication guarantees the protection of personal data for internet companies and protects them from collapsing or losing money. With Time-based multi-factor authentication algorithm, we improved protection of electronic payments. Our proposed methods uses mechanisms of TOTP, where it facilitates the user device authentication creating the onetime codes. Enabled MFA and worked with the TOTP method to include an additional level of protection for an electronic payment program. We presented our proposed method is building an additional biometric authentication layer that is going to provide additional is safe against famous attacks such as spoofed, MITMF and tempering. The real information of the user is saved anomalously in database. In addition, the algorithm is used to operate an identical secret via the algorithm using a shared secret key between the client and the server. Our system has the benefit to authenticate the only legitimate user will acquire a chance to use the account where the system is free of cost. Our suggested solution has shown that security efficiency for authentication and authorization has been improved significantly compared to the existing method. Finally, the effort could be put on using modern environments such as cloud computing, banking systems, e-commerce, and mobile devices. In the future, we will apply in actual time as a potential task. In addition, we have focused on incorporating other protection elements into the approaches suggested.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful feedback. We are also grateful to Prof. Dr. Zarina Shukur for helping to perform this research. This research was funded by a research grant code from Ya-Tas Ismail - University Kebangsan Malaysia EP-2018-012.

REFERENCES

[1] V. Khattri and D. K. Singh, “Implementation of an Additional Factor for Secure Authentication in Online Transactions,” J. Organ. Comput. Electron. Commer., vol. 29, no. 4, pp. 258–273, 2019.

[2] H. Venugopal and N. Viswanath, “A robust and secure authentication mechanism in online banking,” Proc. 2016 Online Int. Conf. Green Eng. Technol. IC-GET 2016, pp. 0–2, 2016.

[3] K. Skračić, P. Pale, and Z. Kostanjčar, “Authentication approach using one-time challenge generation based on user behavior patterns captured in transactional data sets,” Comput. Secur., vol. 67, pp. 107–121, 2017.

[4] M. A. J. Kartini Mohamed, Fatemah Sidi, “Strengthening User Authentication for Better protection of mobile application system,” J. Theor. Appl. Inf. Technol., vol. 85, no. 3, 2016.

[5] O. Ogbanufe and D. J. Kim, “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment,” Decis. Support Syst., vol. 106, pp. 1–14, 2018.

[6] N. A. Karim and Z. Shukur, “Review of user authentication methods in online examination,” Asian J. Inf. Technol., vol. 14, no. 5, pp. 166–175, 2015.

[7] A. Hassan, Z. Shukur, and M. K. and A. S. A.-K. Hasan, “A Review on Electronic Payments Security,” Symmetry (Basel)., vol. 12, no. 8, p. 24, 2020.

[8] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, “Surveying the development of biometric user authentication on mobile phones,” IEEE Commun. Surv. Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[9] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, “A Survey on Multi-Factor Authentication for Online Banking in the Wild,” Comput. Secur., no. February, p. 101745, 2020.

[10] O. S. Okpara and G. Bekaroo, "Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras," IEEE Int. Conf. Environ. Electr. Eng., 2017.

[11] Q. Code, "QR Code Standardization | QRcode.com | DENSO WAVE." [Online]. Available: https://www.qrcode.com/en/about/standards.html. [Accessed: 31-Mar-2020].

[12] M. H. Sherif, Protocols for Electronic Commerce, vol. 53, no. 9. 2016.

[13] T. S. & R. A. Sharvil Shetty, "QR-Code based Digital Wallet," Int. J. Adv. Res. Comput. Sci., vol. 5, no. 7, pp. 105–110, 2014.

[14] A. Alhothaily, A. Alrawais, T. Song, B. Lin, and X. Cheng, "Quickcash: Secure transfer payment systems," Sensors (Switzerland), vol. 17, no. 6, pp. 1–20, 2017.

[15] A. A. Lezhebokov, Y. A. Kravchenko, and V. V. Bova, "Support system for QR-code-based educational processes," 8th IEEE Int. Conf. Appl. Inf. Commun. Technol. AICT 2014 - Conf. Proc., pp. 4–7, 2014.

[16] J. Physical, "Physical presence verification using TOTP and QR codes," Int. Conf. ICT Syst. Secur. Priv. Prot. - IFIP SEC 2019, Lisbon (Portugal), 2019, 2019.

[17] E. Esiner, S. H. Hanley, and A. Datta, "DMZtore: A dispersed Data Storage System with Decentralized Multi-factor Access Control (Demo)," Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2016–Augus, pp. 757–758, 2016.

[18] S. P. Dhanashri Ghosalkar, "OTP over SMS: Time Delay Issues and Causes," pp. 1–7, 2019.

[19] L. Xuanzhi and K. Ahmad, "Factors Affecting Customers Satisfaction on System Quality for E-Commerce," Proc. Int. Conf. Electr. Eng. Informatics, vol. 2019–July, no. July, pp. 360–364, 2019.

[20] S. S. Alam, M. H. Ali, N. A. Omar, and W. M. H. W. Hussain, "Customer satisfaction in online shopping in growing markets: An empirical study," Int. J. Asian Bus. Inf. Manag., vol. 11, no. 1, pp. 78–91, 2020.

[21] M. A. Hassan and Z. Shukur, "Review of Digital Wallet Requirements," 2019 Int. Conf. Cybersecurity, ICoCSec 2019, pp. 43–48, 2019.

[22] P. Aigbe and J. Akpojaro, "Analysis of Security Issues in Electronic Payment Systems," Int. J. Comput. Appl., vol. 108, no. 10, pp. 10–14, 2014.

[23] A. O. Alsayed and A. L. Bilgrami, "E-Banking Security: Internet Hacking, , Analysis and Prevention of Fraudulent Activities," Int. J. Emerg. Technol. Adv. Eng., vol. 7, no. 1, pp. 109–115, 2017.

[24] J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler, and S. Rizvi, "Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication," Procedia Comput. Sci., vol. 114, pp. 93–99, 2017.

[25] M. L. T. Uymatiao and W. E. S. Yu, "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore," ICIST 2014 - Proc. 2014 4th IEEE Int. Conf. Inf. Sci. Technol., pp. 225–229, 2014.

[26] A. Hassan, Z. Shukur, and M. K. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," computers, vol. 9, no. 3, p. 13, 2020.

[27] M. Harish, R. Karthick, R. M. Rajan, and V. Vetriselvi, A New Approach to Securing Online Transactions—The Smart Wallet, vol. 500, no. January. Springer Singapore, 2019.

[28] K. Vengatesan, A. Kumar, and M. Parthibhan, Advanced Access Control Mechanism for Cloud Based E-wallet, vol. 31, no. August 2016. Springer International Publishing, 2020.

[29] R. Mohan and N. Partheeban, "Secure Multimodal Mobile Authentication Using One Time Password," Int. J. Recent Technol. Eng., vol. 1, no. 1, pp. 131–136, 2014.

[30] S. Islam, A. H. A. Hashim, M. H. Habaebi, and M. K. Hasan, "Design and Implementation of a Multihoming-Based Scheme to Support Mobility Management in NEMO," Wirel. Pers. Commun., vol. 95, no. 2, pp. 457–473, 2017.

[31] R. Idayathulla, "Enhanced adaptive security system for SMS – based One Time Password," vol. 5, no. 4, pp. 538–541, 2019.

[32] K. A. Taher, T. Nahar, and S. A. Hossain, "Enhanced cryptocurrency security by time-based token multi-factor authentication algorithm," 1st Int. Conf. Robot. Electr. Signal Process. Tech. ICREST 2019, pp. 308–312, 2019.

[33] F. Aina, S. Yousef, and O. Osanaiye, Design and Implementation of Challenge Response Protocol for Enhanced e-Commerce Security, vol. 3. Springer International Publishing, 2018.

[34] Abhishek Arvind, Pradyumna Mahajan, and Rishikesh Chalke, "TOTP Based Authentication Using QR Code For Gateway Entry System," Int. J. Eng. Comput. Sci., vol. 9, no. 05, pp. 25023–25028, 2020.

[35] A. Choudhary, S. Rajak, A. Shinde, S. Warkhade, and P. G. F.S., "Online Banking System using Mobile-OTP with QR-code," Ijarcce, vol. 6, no. 4, pp. 657–661, 2017.

[36] C. A. Soare, "Internet Banking Two-Factor Authentication using Smartphones," J. Mobile, Embed. Distrib. Syst., vol. 4, no. 1, pp. 12–18, 2012.

[37] C. Sudar, S. K. Arjun, and L. R. Deepthi, "Time-based one-time password for Wi-Fi authentication and security," 2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017, vol. 2017–Janua, pp. 1212–1215, 2017.

[38] R. Divya and S. Muthukumarasamy, "An impervious QR-based visual authentication protocols to prevent black-bag cryptanalysis," Proc. 2015 IEEE 9th Int. Conf. Intell. Syst. Control. ISCO 2015, 2015.

[39] V. Shukla, A. Chaturvedi, and N. Srivastava, "A new one time password mechanism for client-server applications," J. Discret. Math. Sci. Cryptogr., vol. 22, no. 8, pp. 1393–1406, 2019.

[40] R. M. Ibrahim, "A Review on Online-Banking Security Models , Successes , and Failures," Int. Conf. Electr. Electron. Comput. Commun. Mech. Comput. (EECCMC)" IEEE EECCMC, no. February, 2018.

[41] Mohammed and Yassin, "Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device," Cryptography, vol. 3, no. 3, p. 24, 2019.

[42] S. F. Tan and A. Samsudin, "Enhanced Security of Internet Banking Authentication with EXtended Honey Encryption (XHE) Scheme," pp. 201–216, 2018.

[43] A. Gupta, D. Kaushik, and S. Gupta, "Integration of Biometric Security System to Improve the Protection of Digital Wallet," SSRN Electron. J., no. Icicc, pp. 1–6, 2020.

[44] A. S. Robert Hunt, Jeremy Kalas, Patrick Lowe, "Biometric security," Biometrics Concepts, Methodol. Tools, Appl., pp. 1399–1418, 2016