Improving Security for the Libyan E-Government Portal

A Multi-Factor Authentication Model Utilizing NID-SIM Linkage

Hamdi Ahmed Abubaker Jaber

Faculty of Information Technology, University of Tripoli, Tripoli, Libya
h.jaber@uot.edu.ly

DOI: https://doi.org/10.5281/zenodo.17200545

Abstract. A rapid increase in the use of digital technology by the Libyan government to deliver public services has been observed. As a result, it has become extremely important for these services to be protected from cyber threats and unauthorized access. Government data is required to be protected to ensure people's trust and to support the success of digital projects like Dawlaty, the Libyan e-government portal.

In this paper, an improved method of user authentication, known as Multi-Factor Authentication (MFA), is proposed for Dawlaty. The method is based on the linkage of mobile SIM cards with each citizen's National Identity Number (NID). The verification of mobile users' identities by the Libyan government has already been implemented through SIM-NID linkage. This linkage ensures that important security codes, called One-Time Passwords (OTPs), are received only by the real owner of a phone number.

A real-life case in Libya—the Foreign Currency Management System (FCMS), managed by the Central Bank of Libya (CBL)—has been carefully studied. NID-SIM linkage has already been used successfully in this system. By examining this real system, it has been proven that sending OTPs via SMS using a linked SIM card is a secure and effective way to protect sensitive government services.

In short, a significant improvement in online security for Dawlaty is proposed, and the common problems faced by traditional authentication methods are addressed.

Keywords: Multi-Factor Authentication (MFA), Two-Factor Authentication, E-Government, NID-SIM linkage, OTP, mobile security, Central Bank of Libya.

1 Introduction.

1.1 Background

A global trend has been observed in which governments are increasingly using technology to deliver public services more efficiently. In Libya, this trend has been followed through the Dawlaty project. Dawlaty has been established as a major effort by

the Libyan government to shift its services from traditional, paper-based methods to digital, online solutions [1]. The project is managed by Libya Telecom and Technology Holding Company (LPTIC), a government-owned company.

Through Dawlaty, the simplification of life for Libyan citizens is intended to be achieved by providing them with quick, easy, and secure access to all government services through a single digital platform. The need for people to wait in lines or spend hours filling out forms has been eliminated. Instead, tasks such as applying for documents, paying fees, or accessing government services can be performed from home using the internet.

This project has also been designed to help the Libyan government. Administrative processes have been made faster, clearer, and less expensive. Reducing paperwork saves both time and money, allowing the government to focus on improving services and boosting economic growth. Furthermore, a well-designed digital portal builds citizens' trust in their government by providing transparent, efficient, and reliable services.

However, serious security risks have accompanied the online availability of government services. The storage of sensitive personal information on digital platforms has made them attractive targets for hackers and cybercriminals. If citizens do not trust that their data is safe, they may refuse to use the digital system, causing the project to fail. Several gap analyses of e-government authentication frameworks have identified key weaknesses in existing models and highlighted the need for more robust approaches [1].

Strong cybersecurity measures are therefore considered crucial. Authentication is recognized as one of the most important cybersecurity measures. The verification of users' identities before they are granted access to services or data is ensured by authentication.

1.2 Importance of Authentication

The prevention of unauthorized users from accessing personal data or sensitive services is facilitated by authentication methods. Simple methods such as usernames and passwords are commonly used, but these are easily hacked or stolen. More secure methods, known as Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA), require multiple ways to verify a user's identity, making unauthorized access more difficult [4].

In Two-Factor Authentication, users are typically asked to provide something they know (such as a password) and something they have (such as a phone). However, even two-factor methods can be susceptible to attack. Hackers may intercept SMS messages or steal user information through advanced methods. To increase security further, a third verification method, such as biometrics or ID verification, is sometimes required by governments.

1.3 Libya's NID-SIM Linkage Policy

A policy requiring all mobile phone SIM cards to be linked to users' National Identity Numbers (NIDs) has been introduced by the Libyan government. The registration of

SIM cards by every Libyan citizen using official identity documents has been made mandatory. This policy ensures that every SIM card owner is accurately identified and officially linked to government records.

The linking of mobile SIM cards with NIDs provides strong identity verification because it connects a person's mobile phone number directly to official identity documents. If an attempt is made by someone to use another person's SIM card or identity, the system quickly detects and blocks this unauthorized attempt. Identity theft and fraud are significantly reduced through this process.

The Central Bank of Libya (CBL) has already implemented the NID-SIM linkage successfully in its Foreign Currency Management System (FCMS). By linking users' phones and identities, the FCMS has created a reliable and secure method of verifying identity before allowing financial transactions online.

1.4 Purpose of this Research

The aim of this research is to propose a practical and secure authentication system using Libya's existing NID-SIM linkage policy. The goal is to improve security for Dawlaty, Libya's national e-government portal.

A clear explanation of how this system works and practical evidence from the Central Bank of Libya's experience are provided. The objective is to convince both decision-makers and citizens that the proposed method is reliable, secure, and easy to use. By doing so, trust and wider adoption of the Dawlaty project can be encouraged.

To ensure complete understanding of the topic, a detailed literature review is included, showing how different countries and organizations handle authentication for digital government services. Clear definitions of all abbreviations such as OTP (One-Time Password), MFA (Multi-Factor Authentication), and SMS (Short Message Service) are also provided.

The organization of the paper is maintained in clear sections. Following this introduction, a detailed literature review, methodology, analysis of the Central Bank of Libya's implementation, and a discussion of the proposed authentication system for Dawlaty are presented. Recommendations and conclusions based on the analysis are also included.

2 Literature Review

In this section, the approaches taken by other researchers and countries to secure their online government services are examined. Various types of authentication methods and their implementations are explored. This review is intended to provide an understanding of which ideas have been found to be most effective, and why the NID-SIM method can be considered especially useful for Libya. Several gap analyses of e-government authentication frameworks have identified key weaknesses in existing models and have highlighted the ongoing need for robust, context-appropriate solutions [1].

2.1 Traditional Authentication Methods

At first, simple passwords were used by many online systems for authentication. Usernames and secret words (passwords) would be created by people to log in to a system. This method has been referred to as single-factor authentication because only one method—the knowledge possessed by the user—was used to check identity.

However, many problems have been associated with the use of passwords alone. Weak passwords such as "123456" are often chosen, or the same password is used for many websites. Such passwords can be easily guessed by hackers, or stolen through malware (malicious software) or phishing (fake emails intended to trick users).

It has been stated by Rademaker and Polush (2022) that password-only systems are no longer considered safe for government platforms because of the high risk of password theft [6]. The effectiveness of password managers and commonly used two-factor authentication tools has also been critically analyzed, revealing usability and security challenges that must be addressed for widespread adoption [4].

2.2 Two-Factor and Multi-Factor Authentication

To address these problems, the development of two-factor authentication (2FA) by researchers and companies has taken place. In 2FA, users are required to provide two things:

- Something known by the user (such as a password)
- Something possessed by the user (such as a phone)

This requirement makes hacking more difficult because, even if a password is stolen, the attacker would still need the user's phone to gain access.

For example, when an email account is accessed, a code (OTP – One-Time Password) may be sent to the user's phone, which must be entered to continue. This system is regarded as much more secure than the use of a password alone.

Some systems have gone further and implemented multi-factor authentication (MFA). MFA can include:

- Something the user is (such as a fingerprint or face scan)
- Somewhere the user is (location-based checks)

It has been discussed by Morais et al. (2023) that web applications can employ adaptive MFA to decide when and how to ask for additional verification, depending on the riskiness of the login attempt [5].

2.3 Biometric Authentication

Authentication by biometrics is performed using physical features to confirm a user's identity. These include:

- Fingerprints
- Face recognition
- Iris scans
- Voice recognition

The Aadhaar system in India is regarded as one of the largest examples of biometric use in government services (Ninawe, 2020) [2]. Fingerprints and iris scans are provided by every Indian citizen and stored in a secure database, to be used for identity verification when services are applied for.

However, several problems have been identified in biometric systems. High setup and maintenance costs are associated with such systems. Concerns about privacy and the consequences of data theft have also been raised. If biometric data is stolen, it cannot be changed, unlike passwords.

In addition, some individuals may encounter difficulties when using biometrics—for example, those with worn-out fingerprints or in cases where face scans do not work in poor lighting. For these reasons, Bawany et al. (2013) have warned that biometrics should not be used as the sole method of authentication [9].

2.4 Smart Cards and Government IDs

In some countries, electronic ID cards with embedded chips have been issued. For example, e-IDs are provided to citizens in Estonia, which store identity data and enable digital signatures and secure logins to government platforms. These cards have been found to be effective but require the use of card readers and supporting technical infrastructure.

It was found by Just (2012) that such systems are powerful but require high levels of user training and technical support [3]. The distribution and management of these systems on a national scale have also been reported to incur significant costs.

The integration of Information Security Management Systems (ISMS) into digital government architectures has been recognized as essential for maintaining robust security standards [7].

2.5 SIM-Based Authentication

Another approach, considered simpler and more affordable, involves the use of mobile SIM cards as part of the authentication process. The prevalence of mobile phones, even in remote areas, is high. Governments already possess systems for SIM card registration, and many people are familiar with their use.

Countries such as Pakistan and Bangladesh have implemented SIM-based identity verification to combat fraud in mobile banking and online systems. When a mobile number is applied for, the presentation of a national ID is required. This process creates a verified link between a person's ID and their mobile number.

In Libya, this policy has already been implemented. Registration of all mobile SIM cards with the citizen's NID has been mandated by the government. As a result, a powerful tool for authentication has been created.

It has been argued by Hilowle (2022) that mobile-based identity verification increases the adoption of digital ID systems in countries where the implementation of biometric or smart card systems is difficult [10].

2.6 OTP as a Security Factor

An OTP (One-Time Password) is a temporary code sent to the user, usually by SMS. It expires quickly and can be used only once. This makes it safer than passwords because even if someone sees your OTP, they can't use it again later.

Sending OTPs via SMS is common in two-factor systems. Even though SMS is not perfect (it can sometimes be intercepted), it still offers much better protection than passwords alone.

According to Gauravaram (2012), OTP systems are especially effective when combined with strong encryption and ID validation [11]. For this reason, many banks and governments use SMS OTPs as part of their login systems.

2.7 Cybersecurity Challenges

Constant attacks from hackers are faced by governments. Such attacks are aimed at data theft, disruption of services, or damage to systems. When users do not feel safe online, the use of e-services is avoided.

It has been explained by Chen et al. (2024) that the presence of a secure login system is the first step in protecting all other parts of a digital system [15]. If login is compromised, extensive damage can result. Therefore, strong authentication is not only helpful but essential. Similar operational and security evaluations have been conducted for authentication systems in critical infrastructure environments, providing valuable lessons for public sector applications [8].

2.8 Summary of Literature Insights

From the reviewed research, the following findings have been identified:

- Passwords alone are insufficient for safety.
- Biometric systems, though secure, are costly and raise privacy concerns.
- Smart card systems are effective but require infrastructure and user training.
- SIM-based systems are simple, low-cost, and have already been used in Libya.

For these reasons, the use of Libya's existing SIM-NID linkage is considered a smart and effective means of improving e-government security. By sending OTPs to verified mobile numbers, a strong and easy method for confirming a user's identity is established.

Other works in the field have provided additional context for e-government security frameworks [1], password managers and two-factor authentication analysis [4], and the integration of information security management into enterprise architectures [7]. Operational and security evaluations for authentication in critical infrastructure have been detailed by Fernandez-Saavedra et al. [8], while advanced encryption standards have been analyzed by Boussif [12]. Recent studies have also focused on cloud security strategies [13] and the measurement of cybersecurity awareness among smartphone users [14]. These studies collectively expand the understanding of technical and human factors influencing secure digital government services.

3 Methodology and Case Study

In this part, the development of the proposed system and its applicability to Libya's Dawlaty portal are explained. Additionally, a real example from Libya, where this idea has already been successfully implemented—the Central Bank of Libya's Foreign Currency Management System (FCMS)—is examined.

3.1 Research Design

A case study method has been employed in this study. Through a case study, a real-world system's operation and the lessons that can be learned from it are better understood. In this case, the FCMS from the Central Bank of Libya has been used as a real example of SIM-NID linkage and OTP authentication.
Descriptive analysis has also been applied. This involves a detailed explanation of how things work, such as the sending of OTPs, SIM registration, and user identity confirmation.
Support for this explanation has been provided through data from trusted sources and scientific papers. In addition, a comparison has been made with similar systems in other countries to demonstrate the practicality and realism of the proposal.

3.2 Theoretical Framework

The foundation of this study is the "Security by Design" theory. According to this theory, security should not be added as an afterthought, but instead must be built into the system from the outset.
In digital government systems, it is essential that security be carefully planned before any online operations are launched. Security must be made part of the architecture. In the present proposal, it is not merely suggested that OTPs be added later; rather, the SIM-NID linkage, which already exists in the country, is recommended as the main component of the authentication system.
The integration of Information Security Management Systems (ISMS) into digital government architectures has been recognized as essential for maintaining robust security standards [7]. These are rules and methods used by companies and governments to protect data. One main principle is access control—ensuring that only authorized individuals gain access to the system. Authentication constitutes the initial step of access control.

3.3 FCMS: A Real Libyan Case

The Foreign Currency Management System (FCMS) is a digital service provided by the Central Bank of Libya. It is used by people to apply for foreign currency for medical treatment, study, or business.
In order to use FCMS, the following steps must be taken by users:

- Registration using their National Identity Number (NID)

- Use of a mobile number linked to that NID
- Receipt of an OTP via SMS for login

This system has achieved significant success. Fraud has been reduced because only genuine individuals with real NIDs are permitted to apply. Repeated fake applications from the same individual using different names have been blocked.

Widespread popularity has been achieved by this system, and it is considered a success story. It has demonstrated that:

- OTP via SMS is a practical solution in Libya
- The SIM-NID policy has already proven effective
- The system was accepted by people due to its ease of use

Because of FCMS, it can be claimed that the proposed system for Dawlaty is not simply theoretical, but has already been tested in real life

3.4 System Requirements

For the implementation of this authentication system in Dawlaty, the following are required:

- A reliable user registration system using NIDs
- A database linking NIDs to mobile numbers
- An OTP generator
- A secure SMS gateway for sending OTPs
- A login interface that requests OTP after password entry

All of these components are already available in Libya:

- The General Authority for Information and Documentation maintains citizen data
- Mobile phone companies register SIM cards with NIDs
- The CBL system already utilizes OTP systems and SMS services

Therefore, the building of new systems from scratch is unnecessary for Dawlaty. Most of the necessary components are already in place.

3.5 Sample and Data Collection

A qualitative and descriptive approach has been adopted for this study. The following have been reviewed:

- Government policies regarding SIM registration
- FCMS login procedures
- Technical papers on authentication

A quantitative survey was conducted with 110 FCMS users to assess satisfaction and perceptions regarding the authentication system...

A group discussion was also conducted to collect more information about users' opinions. The meeting was held online using Microsoft Teams on December 14, 2024. Six people were invited to join. The participants were chosen because the FCMS system had been used by them before, and they had different backgrounds in computer science, information security, and government administration. It was made sure that different fields were included, so different opinions could be heard.

During the meeting, the process of logging into the Central Bank of Libya's Foreign Currency Management System (CBL FCMS) was discussed. It was confirmed by most participants that the process was found to be easy. One computer science expert stated, "No problems are faced by me with the login process. It is simple and easy to use." Some concerns about security were expressed by the team. An information security expert said, "I am not sure if two-factor authentication is enough, and maybe more security should be considered." Confidence in secure credentials was mentioned by a government administrator, who said, "Trust is given by me to the system to keep my credentials safe, but I worry if there are any mistakes in it."

Recommendations for other government systems were asked about. It was agreed by most participants that the model could be followed because it is easy to use and simple. However, it was said by some participants that more security measures should be implemented for better protection, especially because there are more cyber threats these days.

Through this group talk, useful ideas were learned about why the system is liked and what improvements are needed. It was agreed by most people that the system is easy and safe to use, but better protection was wanted by some participants.

3.6 Security Flow

The authentication flow for Dawlaty would be as follows:

1. The Dawlaty portal is visited by the user.
2. Username and password are entered.
3. The system checks if the username exists.
4. If valid, the system sends an OTP to the linked phone number.
5. The OTP is entered by the user.
6. The system verifies the OTP.
7. If the OTP is correct, access is granted.

This process remains simple for users but is very difficult for hackers to bypass—especially when the SIM is linked to the user's NID

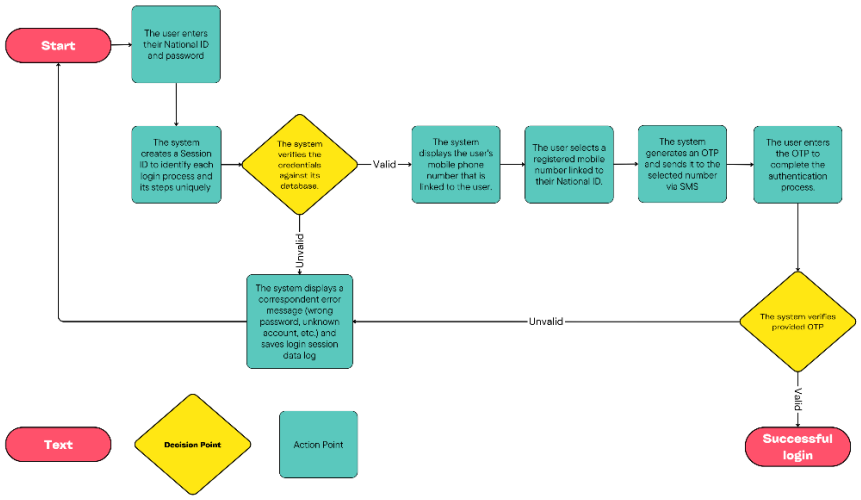


Fig. 1. The authentication process flow

3.7 Advantages of the Method

Numerous advantages are offered by this method:

- No biometrics or special cards are needed; existing phones are used.
- Alignment with existing government policy is ensured; new laws or major changes are unnecessary.
- Cost and speed are optimized, as SMS is already utilized by many government and private services.
- Fraud is reduced, as the registration of multiple accounts by a single person is not easily accomplished.
- Ease of use is ensured, since most citizens are already familiar with receiving OTPs via SMS.

3.8 Risk Considerations

While no system can be considered completely safe, several risks must be acknowledged:

- SIM swap fraud (in which criminals attempt to obtain a new SIM using someone else's ID)
- SMS interception (by advanced hackers if the phone is compromised)
- Inadequate phone coverage in remote areas

However, these risks are smaller than those faced by other systems, and solutions are available:

- ID checks by mobile companies can be enhanced
- Users can be educated to report lost phones promptly
- Offline backup codes can be provided in areas with poor network coverage

3.9 Summary

It has been demonstrated by the FCMS case that the use of NID-linked SIM cards with OTPs is effective in Libya. The required infrastructure already exists. Dawlaty can build upon this experience and improve its security without the need to start from scratch.

In the next section, a comparison of different systems will be presented and the suitability of the proposal within the broader context of secure, accessible e-government will be evaluated.

3.10 User Survey Results

The main findings from the user satisfaction survey are summarized in Table 2.

Table 1. summarizes the responses from 110 CBL FCMS users

Survey question	Strongly Agree %	Agree %	Unsure %	Disagree %	Strongly disagree %
It is easy to log in to the CBL FCMS	39	41	8	11	1
You feel secure when logging into the CBL FCMS	36	48	7	8	1
You feel confident that your login credentials are secure	54	31	8	6	1
Do you recommend similar login processes in other government systems based on convenience?	61	24	9	5	1
Do you recommend similar login processes in other government systems based on security?	69	19	7	4	1

Source: Author's analysis (quantitative method described above).

Most respondents (80%) found it easy to log in, and 84% felt secure when using the system. More than half would recommend the same authentication process for other government services. This supports the usability and trust in the NID-SIM linkage.

4 Evaluation and System Comparison

In this section, an evaluation of the proposed system in comparison to other common security systems is conducted. The suitability of the proposed approach for Libya and its alignment with the Dawlaty project are also discussed

4.1 Evaluation Criteria

The following criteria have been used to evaluate the NID-SIM and OTP system:
- Security – The effectiveness of protection against unauthorized access
- Cost – The expense involved in implementation and maintenance
- Usability – The ease with which citizens can understand and use the system
- Scalability – The capacity for use by millions of users
- Infrastructure Requirements – The need for additional devices or software

By using these five points, a comparison of different authentication methods has been made in the following table.

4.2 Comparison Table

Table 2. Authentication methods comparison.

2FA Method	Security Level	User Experience	Cost
SMS OTP	Medium High	High	Low
Email OTP	Medium High	High	Medium Low
App Based OTPs	High	Medium Low	High
Biometric Authentication	High	Medium Low	High
Token Based	High	Medium Low	High
QR Code 2FA	High	Medium	Moderate

It can be seen that the OTP via SMS with NID-SIM linkage scores highly, offering strong security, good usability, relatively low cost, and suitability for national-scale use.

4.3 Benefits for Libya.

A closer examination of how this system fits Libya is presented below:

1. **Alignment with Existing Laws and Policies**
   It is required by the Libyan government that mobile companies link phone numbers to national IDs. The proposed system leverages this existing rule and strengthens it by applying it to the login process for government services [1].
2. **Affordability and Practicality**

Large investments in new devices or technology are unnecessary for Libya. Mobile phones are already owned by most people, and SMS is both widely available and easy to set up.

3. Consideration of Citizen Limitations

Complex systems such as email or biometric devices may not be easily used by all people. However, reading an SMS and typing a code are skills familiar to the majority of users.

4. Prevention of Fraud and Identity Theft

Major problems in online government services, such as the registration of multiple fake accounts, the use of stolen identities, or the submission of repeated requests with false data, are addressed. NID and SIM linkage make these tricks much harder to carry out. Every login is strongly connected to a real person, as only the number linked to an official identity can be used.

4.4 Drawbacks and Weak Points

Despite its strengths, the proposed method is not without weaknesses:

1. SMS Delivery Failures
   Occasional delays or failures in OTP delivery may occur due to network issues, especially in rural areas with poor signal coverage.
   Solution: Alternative backup methods such as voice calls or offline codes can be introduced.
2. SIM Swap Fraud
   Attempts by criminals to deceive mobile companies and obtain someone else's phone number may be made.
   Solution: The tightening of SIM re-issuance rules and strict ID checks by phone companies should be enforced.
3. Phone Theft or Loss
   If a phone is lost and not reported, an attacker may be able to gain access.
   Solution: Dawlaty should provide a rapid method for reporting lost numbers and blocking access, along with secondary verification options for users.

4.5 User Experience (UX)

It is acknowledged that good security should not degrade the user experience. Systems that are too complex may be abandoned, while those that are too simple may lack sufficient security.

The proposed system is simple:

- Login and password are entered
- OTP is received by SMS
- OTP is entered; access is granted

This method is already familiar to many users through banking and other services, which increases the likelihood of acceptance.

4.6 Compatibility with Dawlaty Goals

The objectives of Dawlaty include:

- Making services easier
- Building citizen trust
- Reducing corruption
- Protecting user data

All these goals are supported by the proposed system:

- Simplicity and speed are provided
- Unauthorized use is prevented
- The method has already been tested in Libya (FCMS)
- User confidence in online services is strengthened

Thus, from technical, legal, and social perspectives, this method aligns well with Dawlaty's objectives.

4.7 Feedback from FCMS Users

Reports and observations from FCMS users have indicated a mostly positive experience:

- The system was perceived as secure
- Its simplicity was appreciated
- The requirement for a real phone number increased trust in the process

This feedback suggests that Libyans are ready for such systems. Given its success with FCMS, similar success for Dawlaty is likely.

4.8 Summary

Upon comparison with other authentication systems used globally, the proposed approach demonstrates strong security and alignment with Libyan policy. It is user-friendly and does not require new devices.

While some risks remain, these are minor and manageable. With proper planning and support, the NID-SIM OTP system can serve as a strong foundation for e-government in Libya.

Additionally, OTPs can be set to expire after a short period (e.g., 5 minutes), which enhances security without adding complexity.

5 Recommendations and Future Work.

In this section, clear suggestions are provided for Libya to implement the proposed security system. Future improvements and areas requiring further study or technical development are also recommended.

5.1 Government Recommendations

1. **Default Use of OTP Login for Dawlaty**
   It is recommended that OTP-based login be adopted as the default for Dawlaty. Password entry should be followed by the sending of an OTP to the user's registered phone number. This additional step can prevent many cyberattacks.
2. **Utilization of the National Identity Database**
   The connection of Dawlaty to the national identity system should be ensured, to verify that each user's SIM card is truly linked to their NID. This connection must be made secure and kept up to date.
   As the General Authority for Information and Documentation already holds this data, cooperation between Dawlaty and the authority should be established to create this link.
3. **Collaboration with Mobile Operators**
   Libya's mobile phone companies (such as Libyana and Almadar) already collect ID information for every phone number. Cooperation with these companies should be undertaken by Dawlaty to:
   - Verify the SIM-to-NID link before OTPs are sent
   - Prevent OTP delivery if a SIM is no longer valid
   - Update numbers promptly when users change their phones
4. **Update of SIM Registration Rules**
   Stricter rules for obtaining new SIM cards should be enforced by the government. Mobile shops should be required to conduct strict checks of ID documents and prevent the registration of fake SIMs. This helps to deter SIM swap fraud.

5.2 Technical Recommendations

1. **Secure Hosting of the OTP Server**
   The OTP generator should be placed on a secure, government-controlled server. The server should:

- Generate random OTPs
- Store OTPs temporarily (e.g., for 5 minutes)
- Automatically delete OTPs after expiration

Verification should be performed to ensure that the phone number receiving the OTP is the one linked to the user's ID.

2. **Limiting OTP Requests**
   Limits on the number of OTP requests a user can make in a given time period (for example, no more than 5 per hour) should be set, to prevent abuse. This helps to deter bots and spammers.
3. **Recording of Login Attempts**
   All login attempts should be recorded, including:
- The time of login
- The IP address used
- Whether the OTP entered was correct or incorrect

This log can be used to identify unusual activity and detect attacks early.

4. **Account Locking**

   If an incorrect OTP is entered multiple times, the account should be locked temporarily. This helps prevent brute-force attacks.

5.3 Citizen Awareness

It is acknowledged that security is not only a technical matter but also a human one. Citizens must:

- Be informed about the importance of OTPs
- Exercise caution with their phones
- Avoid sharing OTPs with others
- Report lost SIM cards immediately

Dawlaty can support this by:

- Sending SMS reminders
- Displaying safety tips on the login page
- Running short TV or social media videos to promote online safety

Raising user awareness is especially critical, as studies have shown that gaps in smartphone users' cybersecurity knowledge can undermine even well-designed technical systems [14].

5.4 Future Improvements

While the current system is strong, the adoption of future technologies could yield even better solutions. The following improvements are suggested:

1. **Backup Verification Methods**
   For users who lose their phones or live in areas with poor coverage, Dawlaty can provide:
   - Voice call OTPs
   - Backup email codes

- One-time printable codes (as used by banks)

2. **Optional Biometric Add-On**
   The future introduction of biometrics for users desiring higher security (such as fingerprint login via smartphones) can be considered. This can be made optional, especially for services requiring extra protection (e.g., financial or health data).
3. **Mobile App with Push Notifications**
   Instead of SMS, a secure Dawlaty app that sends OTPs directly to users can be developed. This is faster and less vulnerable to interception. The app could also offer fingerprint login and display a login history for users.
4. **Continuous Monitoring of Global Trends**
   Because cybersecurity is constantly evolving, it is important that Dawlaty's team stay updated with new threats and solutions by monitoring international reports.

Future expansions may also benefit from best practices in cloud computing security, which have been thoroughly reviewed in recent literature [13].

5.5 Suggested Research Topics

Further academic research is recommended on topics such as:

- User satisfaction with OTP systems in Libya
- Accessibility for older or disabled users
- Technical comparison between OTP and biometric methods
- Cybersecurity readiness in Libyan ministries
- Legal and policy impacts of digital identity

5.6 Long-Term Vision

It should be noted that the proposed method extends beyond mere login processes. It forms part of a broader objective—building digital trust. When citizens feel confident that their data is secure and their identity respected, increased use of government services is encouraged.

This creates a positive cycle:

- Better security leads to more trust
- Increased trust results in more users
- More users enable better systems

The digital future of Libya relies on trust, and trust begins with secure and simple authentication.

5.7 Summary

A clear list of actions for both government and Dawlaty developers has been provided in this section. Most requirements are already in place; what is needed is careful integration.
Additionally, future tools, improved awareness, and topics for further research have been discussed. Dawlaty can begin with OTP authentication and gradually strengthen its approach over time.

6 Conclusion

In this paper, a simple yet robust method to protect the Libyan e-government portal, Dawlaty, has been discussed. The use of Multi-Factor Authentication (MFA) based on NID-SIM linkage and OTP codes sent via SMS has been proposed.
The key points can now be summarized as follows:

6.1 What Has Been Learned

It has been established that passwords alone are inadequate. Many people reuse weak passwords, making it easy for systems to be compromised by hackers [6].

Multi-Factor Authentication has been shown to provide better security. When multiple forms of verification (such as password and phone) are required, system strength is greatly increased [4].

Libya's existing SIM-NID linkage has been recognized as a valuable asset. This linkage allows for a reliable method of verifying the owner of each phone number.

This method has already been implemented by the Central Bank of Libya in the FCMS system, where OTPs must be sent to a phone number linked to the user's ID. This approach has helped reduce fraud and abuse.

It is recommended that Dawlaty adopt the same idea, as it is neither complex nor costly, and the public is already familiar with its operation.

6.2 Why This Matters

Libya is moving towards the provision of digital services. The Dawlaty project is a critical initiative. It has the potential to:

- Make life easier for citizens
- Save time and money
- Combat corruption

However, the success of these benefits depends on the public's sense of security while using such services. If concerns exist that accounts may be hacked or stolen, system usage will be avoided. Therefore, robust authentication is recognized as the foundation of success [1][8][15].

6.3 Simple, Safe, and Local

It has been noted that some countries employ technologies such as fingerprints, face scans, or smart ID cards. While these tools are effective, they are costly and may be difficult to deploy everywhere [2][3][9].
Libya already possesses the necessary resources:
- National IDs
- SIM registration regulations
- Widespread mobile phone use
- SMS network infrastructure

It is thus logical to utilize what is already available. The proposed system is:
- Simple for users
- Inexpensive for the government
- Resistant to most forms of attack

6.4 Call to Action

It is strongly recommended that the Libyan government:
- Implement OTP login for Dawlaty
- Integrate Dawlaty with the national ID system
- Cooperate with mobile service providers
- Educate citizens about OTP security [14]

This is not simply a technical adjustment, but a step toward building trust.

6.5 Final Words

It must be understood that cybersecurity is not solely about blocking hackers, but about safeguarding individuals. The implementation of a secure login system ensures that:
- A mother can safely obtain a birth certificate online
- A student can apply for a scholarship without concern
- A business owner can pay taxes with confidence

The future of public service in Libya lies in Dawlaty. Its protection should be ensured not with complex foreign tools, but through intelligent use of what is already present in Libya [12][13].
This represents an opportunity to establish a digital Libya that is secure, trustworthy, and ready for the challenges of tomorrow.

References

1. H. Almagwashi, H. Almagwashi, W. A. Gray, "E-government Authentication Frameworks: A Gap Analysis," in The 5th International Conference on eGovernment, Boston, USA, Oct. 2009.
2. S. S. Ninawe, "A Method of Designing Authentication Scheme for Aadhaar User," J. Inf. Syst. Eng. & Manage., vol. 10, no. 11s, pp. 97-108.

3. M. Just, K. Renaud, "Trends in Government e-Authentication," in Digital Democracy, Information Resources Management Association, 2012.
4. M. Jubur, P. Shrestha, N. Saxena, "An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools," ACM Comput. Surv., vol. 57, no. 5, Jan. 2025.
5. D. Morais, A. Zúquete, A. Mendes, "Adaptive, Multi-Factor Authentication as a Service for Web Applications," in 2023 7th Cyber Security in Networking Conference (CSNet), Oct. 2023.
6. L. L. Rademaker, E. Polush, "Qualitative Data Collection and Quantitative Data Collection," in Evaluation and Action Research, Oxford University Press, 2022.
7. V. Hensel, K. Lemke-Rust, "On an Integration of an Information Security Management System into an Enterprise Architecture," in 2010 Workshop on Database and Expert Systems Applications (DEXA), 2010.
8. B. Fernandez-Saavedra, I. Tomeo-Reyes, F. J. Diez-Jimeno, R. Sanchez-Reillo, "Operational and security evaluation of authentication systems in critical infrastructures," in Proc. Int. Conf. Experiments/Process/System/Modeling/Simulation/Optimization (IC-EPSMSO), vol. 2, July 2011.
9. N. Bawany, R. Ahmed, Q. Zakir, "Common Biometric Authentication Techniques: Comparative Analysis, Usability and Possible Issues Evaluation," [no conference or journal name given], May 2013.
10. M. Hilowle, "Towards Improving the Adoption and Usage of National Digital Identity Systems," in Proc. Pacific Asia Conference on Information Systems 2022, Apr. 2022.
11. P. Gauravaram, "Security Analysis of salt||password Hashes," in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Nov. 2012.
12. M. Boussif, "On The Security of Advanced Encryption Standard (AES)," in 2022 8th International Conference on Engineering, Applied Sciences, and Technology (ICEAST), Jun. 2022.
13. A. Odeh, Q. Abu Al-Haija, T. Alhajahjeh, R. Mesleh, "Navigating Cloud Computing Security: Strategies, Risks, and Best Practices," in Proc. 8th IET SMART CITIES SYMPOSIUM, Bahrain, Dec. 2024.
14. E. Sala, E. Martiri, "Assessing Cybersecurity Awareness Among Smartphone Users: Designing a Comprehensive Survey," in Proc. 2nd International Conference “Creativity and Innovation in Digital Economy” (CIDE2023), Ploiesti, Romania, Nov. 2023.
15. Y.-J. Chen, C.-L. Hsu, T. W. Lin, J.-S. Lee, "Design and Evaluation of Device Authentication and Secure Communication System with PQC for AIoT Environments," Electronics, vol. 13, no. 8, p. 1575, Apr. 2024.

تحسين أمن بوابة الحكومة الإلكترونية الليبية

نموذج مصادقة متعدد العوامل باستخدام الربط بين الرقم الوطني وبطاقة الهاتف المحمول

حمدي أحمد أبوبكر جابر

كلية تقنية المعلومات، جامعة طرابلس، طرابلس، ليبيا
h.jaber@uot.edu.ly

الملخص: أدى التوسع في الخدمات الرقمية في ليبيا إلى جعل تأمين الوصول إلى الخدمات الحكومية الحساسة ضرورة ملحة. تقترح هذه الدراسة نظامًا محسّنًا للمصادقة متعدد العوامل (MFA) لبوابة الحكومة الإلكترونية الليبية، مستفيدًا من سياسة الحكومة الليبية التي تقضي بربط بطاقات الهاتف المحمول (SIM) بقاعدة بيانات الرقم الوطني (NID) لجميع مستخدمي الاتصالات من المواطنين في ليبيا. يضيف هذا الربط طبقة إضافية من الأمان، مما يضمن أن المستخدمين الموثوقين فقط يمكنهم تسجيل أرقام هواتفهم لتلقي كلمات المرور لمرة واحدة (OTPs) .

يهدف النظام المقترح إلى الحد من الوصول غير المصرح به، وهو أحد التحديات الشائعة في أنظمة المصادقة الثنائية التقليدية. بالإضافة إلى ذلك، تسلط هذه الورقة الضوء على التنفيذ الناجح للربط بين الرقم الوطني وبطاقات SIM من قبل مصرف ليبيا المركزي (CBL) في نظام إدارة العملة الأجنبية (FCMS) ، مما يوفر دليلًا عمليًا على فعاليته.

تُظهر التحليلات المقارنة لطرق المصادقة أن آلية المصادقة الثنائية القائمة على الرسائل النصية القصيرة(SMS) ، عند دمجها مع الربط بين الرقم الوطني وبطاقات SIM ، تُعد حلاً آمنًا وفعالًا من حيث التكلفة وسهل الاستخدام لضمان سلامة الخدمات الحكومية الحساسة.

الكلمات المفتاحية: المصادقة متعددة العوامل، المصادقة الثنائية، الحكومة الإلكترونية، الربط بين الرقم الوطني وبطاقاتSIM ، مصرف ليبيا المركزي، كلمة المرور لمرة واحدة.