SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Volume 7 No 3
ISSN 2054-7390

Two Factor Authentication Framework Using OTP-SMS Based on Blockchain

[1] Eman T Alharbi, [2] Daniyal Alghazzawi

[1,2] Department of Information System, Faculty of Computing and information technology, King Abdulaziz University, Jeddah, Saudi Arabia;

Etalharbi0125@stu.kau.edu.sa; dghazzawi@kau.edu.sa

ABSTRACT

The authentication process is the main step which should be used to confirm that the user is the legitimate one and give the access only for him. Recently, Two Factor Authentication (2FA) schemes have been used by most of the applications to add an extra layer of security on the login process and solve the vulnerabilities of using only one factor for authentication. OTP-SMS is one of the most common methods which has been used in 2FA. However, attackers found a way to attack this method and gain an access to the user's account without their permission. In this paper, we proposed a new 2FA framework for OTP-SMS method to prevent different attacks, mainly Man In The Middle (MITM) attack and third party attack. The proposed framework is based on the use of Blockchain technology, which add more security and better environment for authentication process. The proposed framework uses an encrypted OTP, which generated by smart contract and uses also its hash value to send it to the application/website to complete the authentication process. We introduced a comparison between our proposed framework and other two frameworks which uses Blockchain to secure OTP-SMS. Our framework found to be secure against MITM and third party attacks and the computation time and complexity are less than other frameworks.

Keywords: Two Factor Authentication, One Time Password, Blockchain, Smart Contract, Ethereum, Man in the Middle Attack, Third Party.

1 Introduction

Authentication is a method and technique that used to construct an association among two parties. This association depends on confidence and certainty that the two parties are the authentic parties to establish the association (connection). The most common authentication method is based on the using of password, which is used on various services, like on social networking, bank accounts, and different website and applications. However, there are many ways to hack the secret password, and the easy ones can be attacked without the need for extensive computation. The best way to prevent password attacks is to add more security and make the authentication process more complex.

One of the most common approaches which used to increase the security of authentication is the use of two factor instead of using only one. Two factor Authentication (2FA) schemes was introduced to overcome the weakness of single password authentication scheme and strength the security side by deploying a second authentication factor. There are several different methods that are applicable to be used in 2FA. The main categories of authentication are [1]:

DOI: 10.14738/tmlai.73.6524
Publication Date: 30th June, 2019
URL: http://dx.doi.org/10.14738/tmlai.73.6524

1. Something you are (user's biometric like fingerprint, voice recognition, retina scanning)
2. Something you know (Password and PIN codes)
3. Something you have (mobile phone, ID card, or an Electronic card)

2FA method requires proving two instances of a knowledge factor (e.g., password, inherent biometric features or generating One Time Password). Using messages based on One Time Password (OTP-SMS) is the most common method of second factor which used in 2FA scheme, as shown in Figure.1. OTP-SMS has been widely deployed in many applications which need an extra layer of security, for example, web based banking and login verification in social media applications [2].

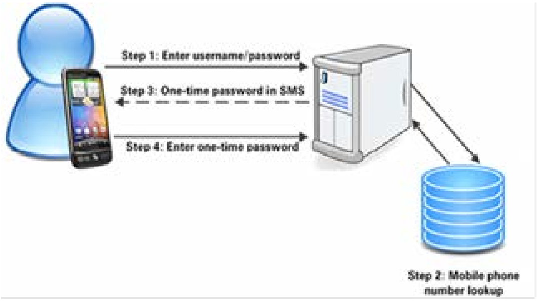
Step 1: Enter username/password
Step 3: One-time password in SMS
Step 4: Enter one-time password
Step 2: Mobile phone number lookup

Fig.1. OTP-SMS as Second Factor of 2FA [3]

There are so many advantages of 2FA method, but attackers were working on breaking this method and they found many ways to hack it and reveal the sensitive information of the users. Breaking 2FA requires the attacker to execute only a single type of malicious action, but multiple times in more contexts – for example, extracting a password (e.g., by a keylogger) and extracting a private token of an application generating OTPs (e.g., by malware). We thus see a need for research on more secure 2FA scheme, specially OTP-SMS, that can withstand today's sophisticated adversary models. In this paper, we explore authentication framework that use Blockchain as a second authentication process instead of the generation of OTP by the third parties. Such approach could eliminate the inherent weaknesses of existing OTP-SMS schemes and preventing the attacks which could reveal the authentication process.

The remaining of this paper is organized as the following: Section II introduces a discussion of the attacks on 2FA scheme, Section III discuss the background and preliminaries, section IV introduce the related work, Section V introduces the proposed framework, Section VI introduces a discussion and finally section VII introduce a conclusion of the work.

2 Attacks on Two Factor Authentication Schemas

Most two-factor authentication (2FA) methods are adopted with online applications or website services, where one-time password (OTP) is created when clients sign in with their username and password. A client gets the OTP by means of a SMS on their enlisted phone number and enters it on the site to finish the login step. While 2FA is a positive enhancement for plain password authentication, it isn't trustworthy [4]. There are many attacks can be occur on 2FA scenario and break down the authentication process.

Jesudoss and Subramaniam [5] introduced an extensive study that investigate and analyze different possible attacks on authentication aspects of security and they placed about 11 possible attack which can reveal a password for attacker . In addition, Certic [6] introduced another study to present forensic evidences that there is a serious breach in the 2FA authentication model, and he confirmed 4 of the attacks that referred by [5]. Moreover, Dmitrienko et.al [2] introduced a study that investigate the security vulnerabilities of the mobile 2FA of many service providers including Dropbox, Google authenticator and twitter. They show that the used mobile 2FA schema has many weakness and attacker can bypass the authentication process simply by intercepting the OTP or capturing the cookies session which can be used for regeneration OTP.

The following is a list of the most common attacks that can reveal 2FA scheme and release the user's credentials:

2.1 Man in the middle attack

A man in the middle (MITM) attack is a general term when an attacker eavesdrops or impersonates one of the parties by positioning himself between two hosts, i.e. website/application and user to steal personal information (e.g. login credential, credit card information). The communication appears as a normal exchange of information, but all the communication between them goes only through the attacker, as shown in Figure.2. So attackers can change, copy or erase the whole or a part of the data traffic between parties. MITM might be used to simply monitor the data (passive attack) or modify it (active attack) [7].

Typically, MITM attack targets the users of financial or e-commerce sites, which require logging in information. 2FA can be revealed by MITM attack, which can tricke the user to visit a fake website, which exactly looks like the legitimate one. The user enters his login information into the fake site, then the attacker get these information and enter them to the legitimate site, which at that point sends an OTP to the user. The user does not have any idea about this movement and he will enters the OTP in the fake site and the attacker sends them to the legitimate site, which allow him to gain full access to the account without anyone's knowledge.

Secure Socket layer (SSL) is one of the main solutions for MITM, which encrypt the traffic and make it impossible to tamper or modify any of the transferred information between two parties [8]. However, using SSL is not enough because there are ways to fake it (by proxy servers), so that the user think that he have a secure connection while he navigated to a non-SSL site. To overcome any revealing or altering in user information, Blockchain technology can be used and an encryption by using the use's public key for OTP should applied. Moreover, the hashed value of OTP can be sent instead of the real value. If the attacker alter the data, then the received hash will be different and the authentication will be failed.

2.2 Session Hijacking

Session Hijacking attack is the abuse of user session, which acquired from his site, to steal his critical information. This attack can occur between a Web server and a Web browser by exploiting the cookies of TCP session. This TCP session contains tokens (in http request header), which including a sign for authentication that sent by the web server to the browser. The attacker can gain an unauthorized access by using this stolen tokens [10]. This attack is common in Web applications. However, even by using 2FA the attacker still able to perform this kind of attack. To overcome this problem, SSL Secure protocol combined with cookie management system should be used.

2.3 Third party

In the two-factor authentication systems, the generation and verification of the second factor tokens is done by the third party, which considered as a part of the authentication scheme. Any third-party authentication mechanism is based on the security of the vendors or carriers who generate the second factor token. OTP-SMS authentication process is based on the mobile carrier's practices which assign and reuse phone numbers. If the mobile phone is lost or the attackers convince the carrier that they are the true user and they their phone has been lost, they can intercept phone calls and SMS messages, and get access to the OTP tokens [11]. Nowadays, some applications have been requested to stop using OTP-SMS as a second factor in the authentication process. To overcome this problem, the generation of the second factor should be managed through a decentralized authority which can be implemented securely by using Blockchain technology.

2.4 Account recovery

The attacker is searching for the weakest point in the authentication system to attack. When the user loses the first factor of authentication (or if an attacker pretends to), i.e. password, the two-factor authentication process will be temporarily disabled. In this case, the attacker might be able to social engineer the account recovery process to get access to the account. Moreover, the knowledge-based authentication which used in the account recovery process to ask user for secret question provide much worse security and makes the attacking easier as these answers are often very easy to guess.

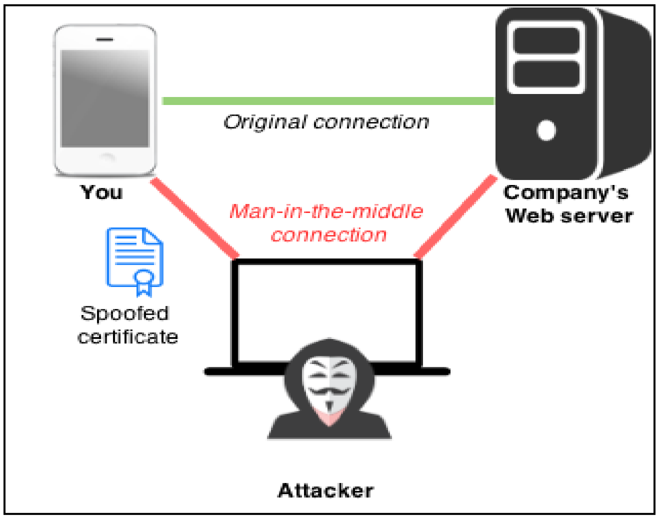

Fig. 2. Man In The Middle Attack Scenario [9]

3 Background and Preliminaries

In order to understand how blockchain can solve the vulnerabilities of 2FA, we have to understand what is Blockchain, how it works and what are its characteristics.

3.1 Blockchain Definition

A blockchain is a distributed database that uses the technology of distributed ledger that preventing the forgery of data records by arbitrary manipulation. Blockchain is a special instance of Distributed Ledger Technologies (DLTs) that records transactions of any value or asset securely. The transaction can be for any type of value between independent parties using a peer-to-peer network, without a central administrator.

3.2 How Blockchain Works

In a blockchain, blocks are linked using a cryptographic hash function, which called Merkle tree, and each new block has to be agreed upon by special participant's node called miners which running a consensus protocol. Each block contains various transactions, which are the interactions between client and Blockchain. These transactions may contain either orders transferring crypto-tokens or calls of smart contract functions, and each one linked with the sender's signature and receiver's public key. The smart contract is a written code for special applications and can encode arbitrary processing logic (e.g., agreements) written in a supported language. All transactions sent to a blockchain are validated by miners who maintain a replicated state of the blockchain. To incentivize miners, blockchain platforms introduce reward and fee schemes. The way how Blockchain is working is displayed and tagged in Figure.3.

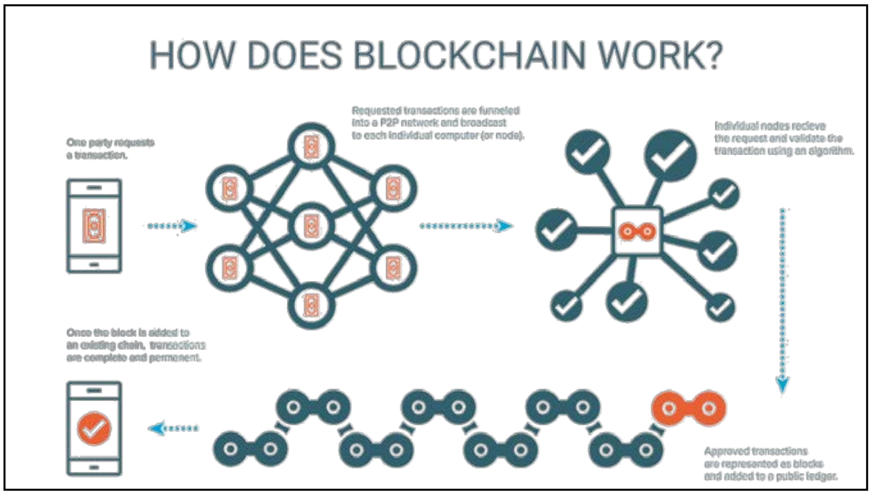
HOW DOES BLOCKCHAIN WORK?
One party requests a transaction.
Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).
Individual nodes recieve the request and validate the transaction using an algorithm.
Approved transactions are represented as blocks and added to a public ledger.
Once the block is added to an existing chain, transactions are complete and permanent.

Fig.3. The way of how Blockchain is working [12]

3.3 Different functionality of nodes in Blockchain

Blockchain is composed of many nodes which create the network itself. These nodes are different and each one has its own functionality. Here we briefly discuss the types of nodes and what are the functions of each type:

- Routing (minimum functionality)
  - Used to discover and connect to other peers in the network, validate and propagate transactions and blocks).
  - Its purpose is to keep the network alive and passing information through the network.
- Storage (full functionality)
  - Store local copy of the blockchain database.
  - Can autonomously and authoritatively verify any transactions without any external references.
- Mining (minor)
  - Runs special mining software to solve a cryptography puzzle to win mining reward.
  - Its purpose is adding the verified transactions to the blockchain.
  - Doesn't necessary to have local copy from the database, they depend on a pool server to get the required information.
- Wallet (simplified payment verification)

- Good for devices with limited storage, security, and power.
- Rely on other trustworthy full node to provide necessary information.

3.4 The Advantages of Blockchain

The blockchain has a number of advantages compared to a traditional centralized system. These advantages including transparency, security, efficiency, and resilience [1], [13].

- Transparency: sharing the resources between all the participated nodes in Blockchain is done in a straightforward fashion and the use of these resources is open by default.
- Security: hacker intrusions can cause catastrophic damage in the centralized data management. However, the case in Blockchain is entirely unexpected and data falsification is almost impossible because hackers need to control all the nodes which contains the distributed data to change any information.
- Efficiency: It is easy to follow the data blocks and get its information in Blockchain. Even if many nodes were participated, the complex processes of system integration can be bypassed.
- Resilience: Centralized data management have a single point of failure (SPOF), while Blockchain does not have SPOF as its devices are decentralized and all data is shared equally between the participated nodes. It is unlikely to receive malicious threats in Blockchain, even if some nodes subject to execution corruption or mistakes.

3.5 Ethereum and Smart Contracts

Ethereum is a platform that provides a customized blockchain to build applications in a distributed environment. It connects each party directly to reach zero-dependency and better transparency. It works on the client-server model and located in the middle of decentralizing computer system.

Smart contracts are programs which created to perform a specific execution. They can be encoded on any blockchain system, Ethereum is the most favoured choice since it gives adaptable handling abilities and allow the programmers to edit and code them as they need [1]. Smart contracts can be used to do the following: managing agreements between users, triggering a claim automatically if certain events occur, and store application's data like health data record.

4 Related Work

Blockchain is an emerging technology that has been used in widely in resent researches. The use of Blockchain in authentication process become an active area and there are many researchers proposed special frameworks to show how this technology can adopted and changes the authentication models to be better than the existed ones. Lin et.al [14] proposed a framework for smart factory which used Blockchain to authenticate the employees in the factory before allowing them to use any device. Ethereum smart contract had been used to request transaction which signed by the employee’s private key. The transaction is validated by decrypting it, using public key for employee, and then allow him to use the device. The proposed framework provides the security that guarantee confidentiality, auditability, and authenticated access to each device. The proposed framework was evaluated, and its security were proved.

In addition, Homoliak et.al [15] proposed 2FA framework which based on the use of a smart-contract cryptocurrency wallet. It consists of three components (i.e., an authenticator, a client, and a smart contract). The proposed framework provides a secure, usable, and flexible way of managing crypto-tokens in a self-sovereign fashion. The authentication process performed by generating one-time passwords (OTPs) by pseudo random function and then aggregate it by a Merkle tree. They proved that this framework is secure against the man-in-machine and quantum cryptanalysis attacks.

Moreover, Park et.al [16] propose 2FA framework to solve the problem of the private Blockchain which is hyperledger. The proposed framework based on the use of TOTP (time based one-time password) which generates a password using the current time information and the secret key shared by a TOTP server and a user. This OTP is generated by the membership function, which is a part of the private Blockchain, based on the user authority. The application will provide the authentication and access for the user when receive the OTP, which is sent to the application rather than send it directly to the user, which guarantee a high level of authentication.

The use of Blockchain with IoT infrastructure can address the issues that confronting the advancement of IoT engineering and security. Wu et.al [17] proposed 2FA framework for out-of-band IoT devices based on Blockchain infrastructure. The implementation of the framework integrates the Blockchain system with multiple devices to simulate IoT infrastructure. All the devices were registered in the Blockchain and each device is connected with the nearest device that able to authenticate each other based on the relationship which stored in the Blockchain nodes. The request for authentication is sent from a devise to the related device which checks in the Blockchain if this device is related and has the ability to authenticate it. This scheme was able to prevent the attack of external malicious devices, even if the adversary was able to steel the first token.

These related works are summarized with their strategies and the problems which solved in Table 1.

Table 1. The Related Work with Their Strategy and Solved Problems

Framework	Strategy	Solved problem
BSeIn: Blockchain for Authentication and Access control for Smart Factory [14]	Authenticate users of factory devices and guarantee secure transactions by using private key to sign the request. The Blockchain smart contract used for authentication process to and to keep tracing of records and connect various factories together.	Secure mutual authentication and provide fine-grained access control.
Smart-contract cryptocurrency wallet framework [15]	Managing crypto-tokens in a secure and flexible way using 2FA based on Blockchain. OTP is generated by the authenticator and aggregated by Merkle tree of Blockchain.	Secure against the man-in-machine and quantum cryptanalysis attacks
OTP Authentication Scheme for Hyperledger Fabric Blockchain [16]	Using 2FA based on Blockchain which generate OTP by the membership function of Hyperledger Blockchain. OTP token is sent to the application rather than directly to the user and then used to access the desired service and make it available to the user.	Prevent third party attack.
An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology [17]	2FA based on Blockchain for devices in IoT network. The authentication steps are: checking the related device in the nearest node then send a verification code to activate the device. Blockchain were used to store the relationships between devices and give access to the related device only.	Preventing single point of failure, and provide secure, reliable and flexible access to the devices of IoT network.

5 The Proposed Framework

The OTP-SMS security and management have turned out to be critical with the recent rise of cyber-attacks. We propose OTP-SMS for 2FA framework based on Blockchain smart-contract to overcome the vulnerabilities of using original OTP which based on using a central authority. The proposed framework gives a flexible, usable, and secure way of generating and validating SMS-OTP which is encrypted and secured against most of the common attacks, which are MITM and third party attacks. The components of our proposed framework are including web application, user, and Ethereum smart contract. The authentication is performed in two stages: the first by providing the username and password to the desired application/website, and the second is by decrypting the OTP which is generated and sent via a smart contract which requested by web application to authorize the user, where the blocks of records are stored in an ever-growing public distributed ledger called a blockchain, which is resistant by design against modifications.

The following steps are descrying how this framework works, as shown in Figure.4:

1. User logs into application/website with the combination of username-password.
2. The application/website asks the user to send a transaction to their Ethereum 2FA contract. The user should be at least a wallet node in the used Blockchain to be able to send contracts and encrypt/decrypt any message. A reasonable waiting time is set for an authenticated event, then login is rejected if no authenticated event is heard for this user's Ethereum address or if the timeout.
3. User sends a transaction to the Ethereum 2FA contract.
4. a. Ethereum checks the validity of the user request through checking the integrity of his transaction with the website/application.

   b. If the request is valid, Ethereum 2FA contract generate OTP.

   c. Ethereum 2FA contract encrypts OTP by user’s public key then send it to the user.

   d. Ethereum 2FA contract computes the hash value of OTP and sent it to the website/application (H1).
5. a. User decrypt the OTP and compute its hash (H2), and send the hash value to the website/application.

   b. Website/application compare the received hash values (H1 form smart contract and H2 form user) to ensure integrity of the user and there is no any alteration on the OTP. If the two values are equal and the process still within the waiting time, Website/application provide the access to the user.

6 Discussion

We proposed a novel framework to provide two factor authentication which based on the use of OTP-SMS. The proposed framework is introducing a solution for the greatest attack which thread the OTP-SMS two factor authentication scheme, mainly the Man In The Middle Attack (MITM) and third party attack. The encapsulation of the OTP message through encrypt it using user’s public key makes such attack impossible and keep the data save. Moreover, the using of hash value by the website/application to authenticate the users instead of the original OTP is s novel method which has not been exposed in researches to our knowledge.

In this section we will compare our proposed framework with the frameworks which introduced by Homoliak et.al in [15] and Park et.al [16]. The comparison is summarized in Table 2.

Homoliak et.al in [15] framework was based on the use of pseudo random function to generate the OTP at the authenticator side (which is the website/application), and send it in plain text to the smart contract in the Blockchain. This step makes it possible for attacker to perform his MITM attack as the OTP is not encrypted while send it through network. Moreover, the computation of the root value, which used later for authentication process, is complex and consuming long time, as multiple OTPs should be generated from the original one, then compute their hash values, and aggregate these values to compute the root value to send it to the user for authentication purpose. The use of hashed value make it impossible for altering the OTP, but in the first place sending the OTP as plain text make this framework still vulnerable for attacks.

Similarly, Park et.al [16] framework solved the problem of third authority attack by generating the OTP via membership function of the Blockchain. However, the OTP is sent as pain text which make it vulnerable to MITM attack. In addition to this attack, there is no any mean to ensure that the OTP is the same generated one and no alteration is performed on it, which considered as another vulnerability in that framework.

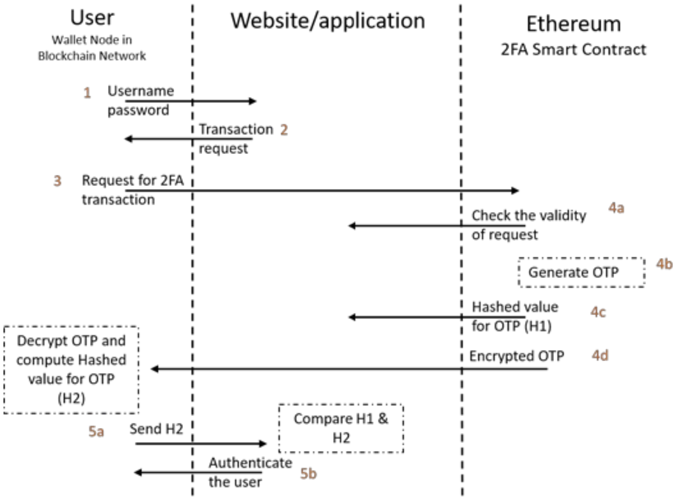
User
Wallet Node in Blockchain Network
Website/application
Ethereum
2FA Smart Contract
1 Username password
Transaction 2 request
3 Request for 2FA transaction
Check the validity of request 4a
Generate OTP 4b
Hashed value for OTP (H1) 4c
Decrypt OTP and compute Hashed value for OTP (H2)
Encrypted OTP 4d
5a Send H2
Compare H1 & H2
Authenticate the user 5b

Fig. 4. The proposed 2FA based on Blockchain Framework

Table 2. Comparison between the Proposed Framework and other two frameworks.

Attribute	Our Proposed Framework	Homoliak et.al [15]	Park et.al [16]
Used authentication factor	OTP	OTP	OTP
Complexity of computation	Easy	Complex	Easy
Time of computation	Low	High	Low
MITM attack	Secure	Not Secure	Not Secure
Third party attack	Secure	Secure	Secure
Alteration on OTP	Secure	Secure	Not Secure

7 Conclusion

In this paper, we introduced OTP-SMS framework as a second factor of the authentication process. Our framework based on using the Blockchain technology to add extra layer of security and solve the vulnerabilities in the login process. We used Ethereum smart contract to generate OTP instead of a third party, and encrypt this OTP with the public key of the user, meanwhile, it sends the hash value to the requested website/application. The user will decrypt the received OTP by his private key and then compute the hash value and send it to the website/ application. The website/ application will authenticate the user after comparing the received hash values from both entities. These processes are preventing MITM attack from getting access to the OTP or altering its value. Moreover, the Blockchain solve the problem of third party attack as well. Our framework provides more security for users in less time and low computation power. For future work, we plan to implement this framework with real applications and prove its ability to preventing different attacks and measure the exact time which required for authentication.

REFERENCES

[1]. R. Gupta, Hands-on cybersecurity with blockchain: implement DDoS protection, PKI-based identity, 2FA, and DNS security using blockchain. 2018.

[2]. A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, “Security Analysis of Mobile Two-Factor Authentication Schemes,” vol. 18, no. 4, p. 24, 2014.

[3]. “Setup two-factor authentication with OTP sent as SMS.” [Online]. Available: http://www.sms-integration.com/setup-two-factor-authentication-with-otp-sent-as-sms-80.html. [Accessed: 30-Mar-2019].

[4]. “Do two-factor authentication vulnerabilities outweigh the benefits?,” SearchSecurity. [Online]. Available: https://searchsecurity.techtarget.com/answer/Do-two-factor-authentication-vulnerabilities-outweigh-the-benefits. [Accessed: 18-Mar-2019].

[5]. A. Jesudoss and N. P. Subramaniam, “A Survey on Authentication Attacks and Countermeasures in A Distributed Environment,” Indian J. Comput. Sci. Eng. IJCSE, vol. 5, no. 2, pp. 71–77, 2014.

[6]. S. Certic, “Two-Factor Authentication Vulnerabilities,” SSRN Electron. J., 2018.

[7]. “What is MITM (Man in the Middle) Attack.” [Online]. Available: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html. [Accessed: 19-Mar-2019].

[8]. C. Onwubiko and A. P. Lenaghan, “Managing Security Threats and Vulnerabilities for Small to Medium Enterprises,” in 2007 IEEE Intelligence and Security Informatics, 2007, pp. 244–249.

[9]. “Man in the Middle Attack | How Can You Prevent MITM Attack?,” Comodo Securebox. [Online]. Available: https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack. [Accessed: 30-Mar-2019].

[10]. I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, “One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials,” Georgia Institute of Technology, Technical Report, 2011.

[11]. “Five Most Common Security Attacks on Two-Factor Authentication.” [Online]. Available: https://www.itbusinessedge.com/slideshows/five-most-common-security-attacks-on-two-factor-authentication.html. [Accessed: 18-Mar-2019].

[12]. S. Shankland, “Why should you care about blockchain? It’s the ultimate trust builder,” CNET. [Online]. Available: https://www.cnet.com/news/blockchain-explained-builds-trust-when-you-need-it-most/. [Accessed: 30-Mar-2019].

[13]. Z. Gao et al., “Blockchain-based Identity Management with Mobile Device,” in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock’18, Munich, Germany, 2018, pp. 66–70.

[14]. C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” J. Netw. Comput. Appl., vol. 116, pp. 42–52, Aug. 2018.

[15]. I. Homoliak, D. Breitenbacher, A. Binder, and P. Szalachowski, “An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets,” ArXiv181203598 Cs, Dec. 2018.

[16]. W.-S. Park, D.-Y. Hwang, and K.-H. Kim, “A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain,” in 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018, pp. 817–819.

[17]. L. Wu, X. Du, W. Wang, and B. Lin, “An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology,” in 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, 2018, pp. 769–773.