**IOSR Journal of Engineering (IOSR JEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 33-35

# Wi-Fi Authentication Method Using Authcoin

Akshay Kumbhar1, Narendra Gupta2, Sourav Mandal3, Amruta Pokhare4
*[1,2,3]B.E Students, [4]Assistant Professor Department of Information Technology*
*Atharva College of Engineering, Maharashtra, India*

***Abstract:*** *Nowadays free Wi-Fi hotspot is available everywhere, and it gives access to user after authentication by the One time password (OTP) send on the user Mobile number. But OTP method of authentication is not so secure as many attacks can be performed to identify user OTP. For this we propose a new method of authentication using Authcoin that use blockchain to store the data which provide more security to the user credentials.*

## I. Introduction

Nowadays internet has become the most important aspect for storing data, obtaining information and many more. To do the work over internet many free Wi-Fi hotspot has been installed[1]. Currently One time password (OTP) method is used to authenticate the user validity. But the OTP method is not so secure as many different types of attacks like Man in Middle Attack, SIM Swap Attack and ways like Wireless interception, mobile phone Trojans etc. to find out the OTP. We proposed a new method of authentication using Authcoin[2] that can solve the above problem. Authcoin is a type of bitcoin that use blockchain to store user data. In our system Authcoin is used as an authentication proof of a user in which user credentials are saved in the form of Hash function which is unique for every single user.

## II. Background

This section discusses about authcoin and conventional authentication methods of access points.

**Authcoin:**

Authcoin is alternative method of authentication[9]. It is a type of Bitcoin[2] that combines validation and authentication process with the advantage of blockchain based storage system. Authcoin authentication method is more secure than OTP method because the data of the user is stored as hash function in the block format and that block is added to the blockchain. Once the data is saved in the block it cannot be changed or modified. But the user modify data can be saved or stored in another block which has different hash function and that block is added to the blockchain this make blockchain more secure than any other data storage method.

**Conventional Authentication Methods:**

Some of the conventional authentication methods are as follows:

- To register e-mail address of users.
- To register cellular-phone number, and authenticate by SMS.
- To authenticate through API of SNS(ex. Facebook, Twitter, etc.)
- To request users to accept the policy.
- To require users to submit their identification card such.

Each method has some problems. The method to register by e-mail address can allow user to make use of fraudulent address for access. SMS authentication is easy to verify users but it has risk of exposure and tampering. The strictest method is to require users to submit their id cards and verification is done at registered centers. But it is not possible every time.

## III. Proposal Method

This system proposes a new authentication method for wi-fi access which makes use of for authentication of user. The method is implemented using and blockchain. The user just have to download the auth wallet application that will provide Authcoin to user. The Authcoin contains asset id that is generated from the data provided by the user. The data can be user name, password, mobile number, email id etc from which the hash function is generated and it is different and unique for each user. Once the user get the Authcoin from the wallet, the user then can access the free wifi hotspot anytime securely as the user credentials are stored in blockchain.

**Wi-fi scanning application :**
It is a simple wi-fi scanning app that scan all the wi-fi hotspots near by the device. In this system the app will redirect the user to the wi-fi registration page when user click on the free wi-fi hotspot.

**Wi-fi registration webpage :**
In this system when a new user want to access the free wi-fi hotspot the user need to sign up with Authcoin to access the wi-fi unless that the user cannot access the wi-fi hotspot. This page is used to verify and authenticate the valid user.

**Authwallet :**
In this system the wallet is the major component as it is responsible for providing authcoin to user and this authcoin have unique asset id to authenticate the user.

## IV. Methodology

**Registration protocol:**

This protocol is executed at users first access. Firstly the user connects to the Access Point (AP). AP then redirects user to URL to download Auth wallet. After that user inputs his informations specifying individual to Auth wallet. Wallet then generates public key Upub and secret key Usec for user. Wallet then sends I and Upub to administrative server. The server then issues authcoin to user and registers users asset id into the database.

**Authentication Protocol:**
In this protocol user first connects to the access point. The access point then issues transaction proxy-tx which sends c to AP. User verifies the transaction and sign it and sends it back to AP. Access point then verifies user using verifying signature protocol using unique asset id of user. On access AP authorizes user and on failure AP nullifies the transaction.

Block diagram of the system is as follows:

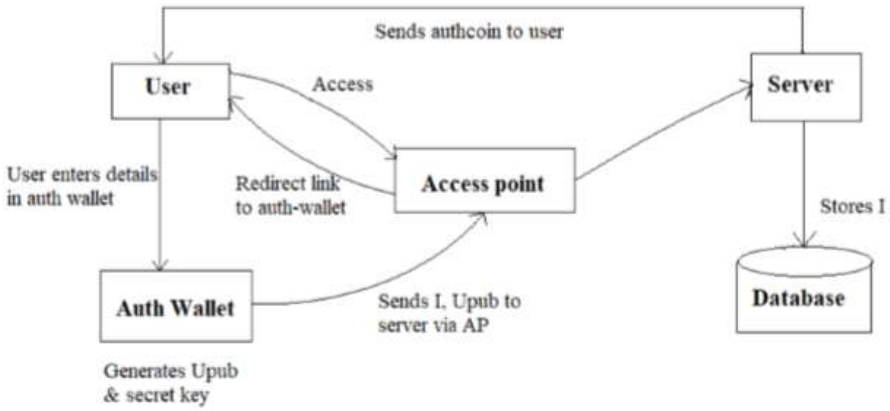


**Fig.1.Block diagram**

## V. Advantages

Some of the advantages of the proposal method are as follows:

1. Users can be authenticated directly after registration as they do not have to send their personal information each and every time.
2. Authcoin can be used only by its owner thus it reduces the risks of spoofing.
3. When user gets access the transaction is broadcasted on blockchain thus it reduces the risk of double spending and coin being stolen.

## VI. Conclusion

In this paper, we have proposed new authentication method using Authcoin. In this method user can access wi-fi by exchanging the authcoin instead of their information. This method will reduce the time and effort of the user as in this method the user don't have to register each and every time.

## References


[1]. Sanda, Tomoyuki, and H. Inaba. "Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0." Consumer Electronics, 2016 IEEE, Global Conference on IEEE, 2016:1-5.
[2]. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system.
[3]. Available: https://bitcoin.org/bitcoin.pdf
[4]. K. Miura and H.Inaba, "Privacy preserving digital contents circulationsystem using bitcoin 2.0," IEICE Tech. Report, vol. 2016-EIP-72, no. 5, pp. 1-4, may 2016 (in Japanese).
[5]. Coloredcoins. [Online]. Available: http://coloredcoins.orgK. Elissa, "Title of paper if known," unpublished.
[6]. Wifi map. [Online]. Available: http://www.wifimap.io/.
[7]. Bitcoin wiki testnet. [Online].
[8]. Available: https://en.bitcoin.it/wiki/Testnet
[9]. A. Cassola, E.-O. Blass, and G. Noubir, "Authenticating privately over public Wi-Fi hotspots," ACM CCS'15, 2015.
[10]. D. He, S. Chan, and M. Guizani, "An accountable, privacy-preserving, and efficient authentication framework for wireless access networks," IEEE Transaction on Vehicular Technology, vol. 65, no. 3, pp. 1605-1614, 2016.
[11]. P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," ACM CCS'07, 2007.