ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

MULTIFACTOR AUTHENTICATION USING BLOCKCHAIN WITH SHA-256

Gogineni Krishna Chaitanya[1],

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502, Andhra Pradesh, India.

Uppuluri Lakshmi Soundharya[2]

[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502, Andhra Pradesh, India.

ABSTRACT—

AUTHENTICATION HAS BECOME ONE OF THE MOST IMPORTANT FACTORS IN THE DIGITAL WORLD. SINCE WE HAVE BEGUN TO TRANSFER ALL OF OUR DATA ONTO ONLINE STORAGE DEVICES OR DIGITALIZE THE WORLD AROUND US WE CAN COMPLETE ALMOST ANY TASK ONLINE AS LONG AS WE HAVE A STABLE NETWORK CONNECTION. HOWEVER, ALTHOUGH THIS HAS HELPED US SPEED THINGS UP IN OUR LIVES IT ALSO COMES WITH THE FACT THAT DATA STORED INLINE ISN'T SECURE. DUE TO THIS REASON WE HAVE BEEN ABLE TO OBSERVE LARGE AMOUNTS OF DATA BEING STOLEN BY CRIMINAL ORGANIZATIONS AROUND THE WORLD. HOWEVER, WE HAVE BEEN ABLE TO FOLLOW VARIOUS FORMS OF ENCRYPTION METHODS TO SECURE IT BUT EVEN WITH THIS SOLUTION INTACT WE HAVE OBSERVED MANY CASES UPON WHICH A USER'S CREDENTIALS ARE STOLEN AND USED IN A NEGATIVE MANNER. TO PREVENT THIS, WE HAVE IMPLEMENTED VARIOUS METHODS SUCH AS ONE TIME PASSWORDS AND OTHER FEATURES BUT THESE AT TIMES DEEM TO BE IN EFFECTIVE. THIS IS WHY WE WOULD LIKE TO CREATE AN APP WITH THE HELP OF BLOCKCHAIN TO MAKE THE MOST SECURE AUTHENTICATION SYSTEM POSSIBLE. OUR SYSTEM WILL BE AUTHENTICATED WITH THE IMEI OF A USER'S PHONE. HAVING THE IMEI AS AN AUTHENTICATION MEANS THAT THE USER WILL NOT BE ABLE TO LOG INTO THE WEBSITE FORM ANY OTHER DEVICE EXCEPT FOR THE PHONE IN WHICH THEY HAVE REGISTERED IN.HROUGH THIS PROJECT WE WILL BE USING BLOCKCHAIN TO CREATE AN EFFECTIVE APP WITH THIS METHOD OF AUTHENTICATION.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

1. INTRODUCTION

Over the past decade we have been able to experience the digitalization of almost everything around us. These may be from the memories that we have all the way to the money that we will be using within our bank accounts. We have been able to create various platform for our various requirements which can all be found online. This has been able to help us advance in large leaps compared to the previous era. With the facilities that we are able to avail from all of these modern technologies we have been able to accomplish various things which were once merely impossible. They have also been able to help us out making day to day tasks far simpler and more convenient. However, we have to keep in mind that all of the task or things we digitalize is all stored in the form of data online. Although it may hard to pinpoint the location of the data without any knowledge each set of data has a unique address with respect to its device or server. One of the major problems with data is the fact that it is almost insecure and can be easily corrupted or hijacked. Due to this we have been able to experience various problems in our day to day lives in which the data of an individual is stolen and used in illegal activities. The number of cases that have been dealing with the loss or the theft of data has drastically increased over the past few years. Although the loss of data may seem like a small benefactor in the modern world imagine how problematic it might be if we were to lose data related to our bank accounts or country secrets. Due to this issue we have been coming up with various solutions such as an OTP or one-time password. This feature makes the login process to an account a two-step process. The first step will involve the user entering his credentials while in the second step the user will have to enter a password sent to the users mobile or email. This password is temporary and will change each time the user tries to log into his account. This is one of the most secure forms of authentication due to the fact that even with the loss of a user's credentials without the OTP which is sent to the user a third party will not be able to gain access to an account. Even though this is fool proof modern hackers have been able to identify loopholes to bypass this feature and gain access to the users' account. Due to this reason we have decided to create an application with will use the user's device as mode of authentication. In this process we will be integrating a blockchain structure along with our authentication. The authentication in our project will take place with the use the devices IME number. As we are all aware of the fact that each device has a unique IMEI number, we will be using this unique IMEI number in order to gain

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

access into an account. Once the user registers into our application the IMEI of the user will be stored into our blockchain network and will only allow the user to login to his account from that mobile device. This implies that a user will not be able to log into his account from any other device other than theirs. However, the most important factor in our project will be creating our application with the use of blockchain. This is a newly developed technology which is well known for its implementation within the various cryptocurrency markets around the world. Blockchain is nothing more then a storage of blocks in a public database which is referred to as the chain. The advantage of using this type of technology is the fact that our data will be irretraceable. Although all of the blocks within our blockchain network are created within our database the integrity of these blocks will be constantly changing and almost random in nature. Due to this even if one were to hack into our application and gain access to the backend servers the data would be completely random and they would be unable to trace it back to an account or an individual user. Although it is one of the most recently formed methods of data storage the security which is being offered by blockchain networks can't be compared with the modern methods. Through our project we will take you through how our application has been implemented from the registration of an individual all the way to the Hash OTP's generated by our blockchain and the authentication of users.

PREVIOUS CITATIONS

These days, banks vary substantially in their structure and purpose. They face complex issues in designing effective governance policies for each of their major functions and to accommodate their many differences. As a monetary authority, they sometimes fail to contain macro economic crises that could stem from incentivized excessive risk-taking for example via unconventional monetary policy tools such as negative rates or quantitative easing. These, in times of financial distress and high volatility, exacerbate negative outcomes. Further problems result from large numbers of financial intermediaries. In addition to high fees, service charges paid for financial intermediation and cost of regulatory compliance, there are delays, onerous paperwork and opportunities for fraud and crime. Multifaceted linkage between banks and a variety of central intermediaries adds to current incomplete understanding of the post- crisis financial system.; in particular, this relates to

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

the concentration of the rest management of credit and liquidity risks in those intermediaries and the impact on systemic risks.

So to over come these risks we propose Blockchain privacy protection scheme based on ring signature. This scheme mainly introduces the use of ring signature technology to design a completely anonymous user data storage protocol under the blockchain architecture to ensure the privacy of user information in the blockchain. A smart contract is deployed in the blockchain network to monitor the dynamics in the network, and when preset conditions are met, a preset instruction is triggered to execute transaction T. A secure ring signature scheme should meet the three aspects of correctness, unconditional anonymity, and unforgeability.

Correctness Analysis: The verifier verifies the transaction signature Tσ according to the formula, and if it is true, the verification is passed.∑i=1nci=H1(h,γ1,γ2,…,γn,δ1,δ2,…,δn)

When i≠s , the conversion of γi , δi is as follows:

a. γi=δi=di∗G+ci∗pki=ui∗G+(vi+wi)∗pki=Lidi∗H0(pki)+ci∗Is=ui∗H0(pki)+(vi+wi)∗Is= Ri Therefore, according to the above relationship, the correctness of the ring signature scheme proposed in this paper can be verified as follows:

=H1(h,γ1,γ2,…,γs,…γn,δ1,δ2,…,δs,…,δn)H1(h,L1,L2,…,Ls,…,Ln,R1,R2,…,Rs,…,Rn)cs+∑ i=1,i≠snci1nci

PROBLEM STATEMENT

In Existing system, the documents are stored in centralized system which is not much secure. May be it will hack and break the security which harms whole user data. So the disadvantages of this system are significant technology cost associated with mining bitcoin, low transactions per second, history of use in illicit activities, susceptibility to being hacked. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and provide officials with instant results. So there would be improved accuracy by removing human involvement in verification, cost reductions by eliminating third-party verification, decentralization makes it harder to tamper with so the transactions are secure, private and efficient as blockchain is a transparent technology.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

PROCEDURE

There are three major parts that will take place within our project. The first step within our application is to make sure that the user registers themselves into the database using their own device. Once this has been done, they will be able to login with a hash OTP. Once this is done this data will be stored into a newly created block within our blockchain network.

Now that we have a vague idea upon how this works lets take a closer look into these steps:

b. User Registration

Once the application is properly downloaded on the user's mobile device the user will now be able to open the application and navigate through its home menu. From this menu the user will be able to select one of the two options of either logging into their account or registering themselves. Since we are new to this application the user will now select the register option and enter their desired credentials consisting of their username as well as password. The user must keep in mind that once they have registered in a specific mobile device, they will not be able to access their account from any other mobile device as the IMEI will change. Once the user is registered the user's credentials along with the IMEI of the mobile phone will be stored into our database and these will be used in the future for the user to access his account within our blockchain. Once you have registered yourself on your device our application will now prompt you to login using your credentials to gain access to your account.

c. Logging Into your Account

Now that the user has successfully registered themselves onto our platform, we will now be able to log in. Once the user has entered their credentials there will be 2 steps before they are able to access their account. The first step will verify the IMEI of the device that the user is using during the time of login. If the IMEI of the device is not the same as the IMEI of the user when they registered the user will not be granted access into their device. However, if the user is using the same device and the IMEI of the device match that of the registered data we will now proceed to the next step. The user will receive an 8-digit Hash OTP generated by our blockchain which will be used as our second form of authentication. If the user is able to pass these two forms of authentication, they will be able to successfully log into their account and access all of their details. The most important point to note during the user login stage is to make sure that the device used by the user is the same device used for registration as our application will focus upon the devices IMEI.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

d. Block Creation in our Blockchain Network

Every time a user logs into his account a block will be created within our blockchain network. This newly created block will note down all the details such as the time of login along with the duration of the session so that all of these can be referenced in the future if there are any problems. This block of data will also take into account all the activity of the user on our application and will only be called back once the user logs in again. If we were to think about this there would be a several block in our chain and all of them would be combined when the proper credentials are met.

e. SHA-256 Cryptographic Hash Algorithm

A cryptographic hash is a kind of signature for a text or a data file. SHA-256 generates an almost-unique 256-bit signature for a text. SHA-256 is one of the successor hash function to SHA-1, and is one of the strongest hash functions available. SHA-256 is not much more complex to code than SHA-1, and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. It is defined in the NIST standard 'FIPS 180-4'. NIST also provides a number of test vectors to verify correctness of implementation. The JavaScript is oriented toward hashing text messages rather than binary data. The standard considers hashing byte-stream messages only. Text which contain characters outside ISO 8859-1 (i.e accented characters outside Latin-1 or non-European character sets – anything with Unicode code-point above U+FF), can't be encoded 4-per-word, so this script defaults encoding the text as UTF-8 before hashing it.

2. RESULTS

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

Homepage

Registrationpage

Login page

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

i.

Logging into Your Account retrieving data from our Blockchain Network

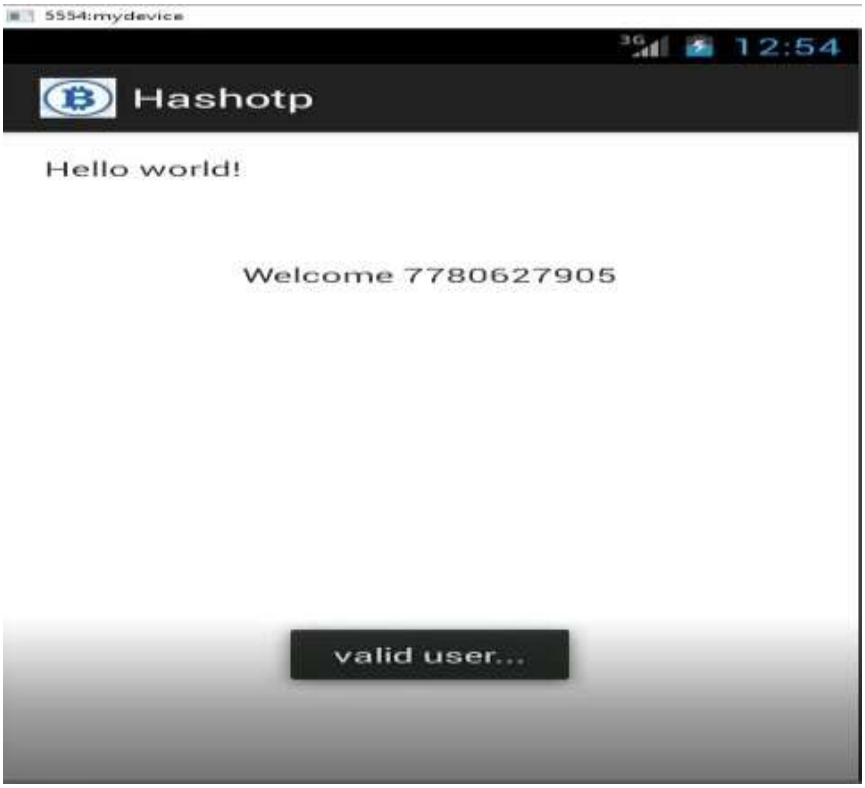
Enter HOTP for Authentication

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

Successfully Logged Into our Application



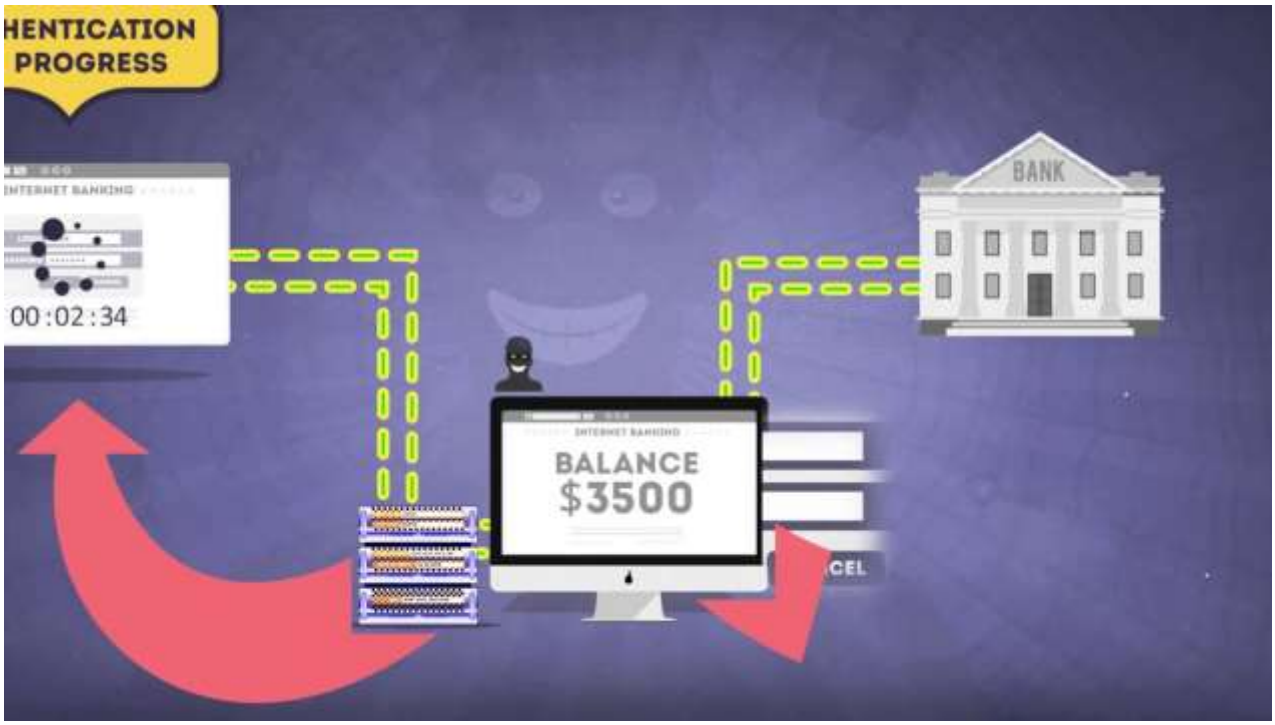
ISSN PRINT 2319 1775 Online 2320 7876

© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

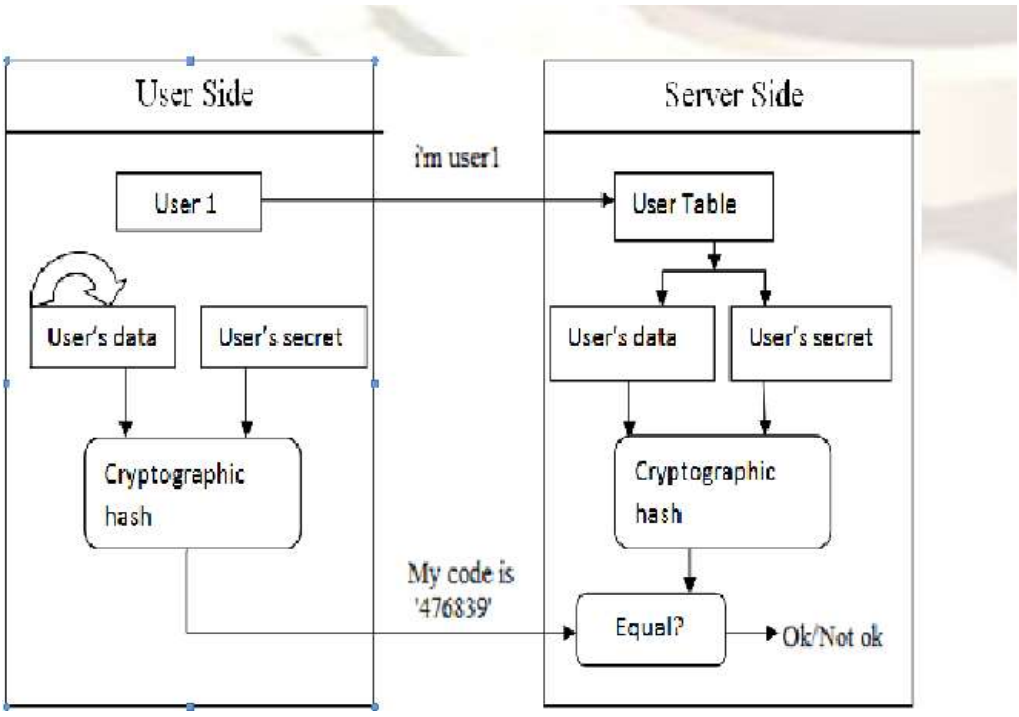
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

RESULT ANALYSIS



ii. Figure 1:How the Hackers get the OTP



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 2, 2019

Figure 2: Proposed System.

3. REFERENCES

1. C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.
2. A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.
3. Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
4. Chris Dannen, Introducing Ethereum and Solidity.
5. J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.
6. L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489– 502.
7. M. Carvalho and R. Ford, "Moving-target defenses for computer networks,"IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.
8. Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE.