Stanford | ONLINE

COURSE CERTIFICATE

10/04/2019

Dhruv Doshi

has successfully completed

Machine Learning

an online non-credit course authorized by Stanford University and offered through Coursera

Associate Professor Andrew Ng
Computer Science Department
Stanford University

SOME ONLINE COURSES MAY DRAW ON MATERIAL FROM COURSES TAUGHT ON-CAMPUS BUT THEY ARE NOT EQUIVALENT TO ON-CAMPUS COURSES. THIS STATEMENT DOES NOT AFFIRM THAT THIS PARTICIPANT WAS ENROLLED AS A STUDENT AT STANFORD UNIVERSITY IN ANY WAY. IT DOES NOT CONFER A STANFORD UNIVERSITY GRADE, COURSE CREDIT OR DEGREE, AND IT DOES NOT VERIFY THE IDENTITY OF THE PARTICIPANT.

Verify at coursera.org/verify/MLXJAK8PAH7F

Coursera has confirmed the identity of this individual and their participation in the course.

NVIDIA DEEP LEARNING INSTITUTE
CERTIFICATE OF COMPETENCY

This certificate is awarded to
DHRUV DOSHI

for demonstrating competence in the completion of
GETTING STARTED WITH AI ON JETSON NANO

Will Ramey

Will Ramey
Senior Director, Deep Learning Institute, NVIDIA

2019
Year issued

NVIDIA. DEEP LEARNING INSTITUTE

Google Cloud

COURSE CERTIFICATE

08/25/2019

Dhruv Doshi

has successfully completed

How Google does Machine Learning

an online non-credit course authorized by Google Cloud and offered through Coursera

Google Cloud Training

Verify at coursera.org/verify/T7WEP5UNK52N

Coursera has confirmed the identity of this individual and their participation in the course.

SUNY The State University of New York

10/26/2019

Dhruv Doshi

has successfully completed

Blockchain Basics

an online non-credit course authorized by University at Buffalo and The State University of New York and offered through Coursera

Bina Ramamurthy
Teaching Professor
Computer Science and Engineering

COURSE CERTIFICATE

EDUCATION FOR EVERYONE · coursera · COURSE CERTIFICATE

Verify at coursera.org/verify/572EE55MFXH2

Coursera has confirmed the identity of this individual and their participation in the course.

International Conference on Mobile Computing and Sustainable Informatics
(ICMCSI 2020)
ICMCSI-2020 23-24, January 2020 | http://icmcsi.com/ | icmcsi.conf@gmail.com

Letter of Invitation & Acceptance

To
Dhruv Doshi,
Silveroak college of Engineering and Technology.

Greetings!!

Institute of Engineering, Tribhuvan University cordially invites you to attend the "**International Conference on Mobile Computing and Sustainable Informatics**" during 23-24 January 2020 in Nepal.

Your research manuscript titled "Blockchain Based Decentralized Cloud Storage" has been accepted after the double-blinded peer review process of ICMCSI 2020 for oral presentation and publication in ICMCSI 2020 proceedings. We are pleased to welcome you to join the conference and share your potential research insights on the conference theme "**Mobile Computing and Sustainable Informatics".** In this regard, ICMCSI 2020 will give an unforgettable experience in exploring new research opportunities in computing and communication paradigms.
For more details, please visit: http://icmcsi.com/index.html

We look forward to welcoming you at Nepal.

VENUE DETAILS:

HOTEL HIMALAYAS 2141, Sahid Sukra Marg, 10, Lalitpur, Nepal.

With Thanks,

Prof. Dr. Subarna Shakya
Department of ECE,
Pulchowk Campus, Institute of Engineering,
Tribhuvan University, Nepal.

Proceedings by

Springer

Blockchain Based Decentralized Cloud Storage

*Dhruv Doshi[1] and Prof. Satvik Khara [2]
[1*]dhru.edu.doshi@gmail.com
[1-2] Silver Oak College Of Engineering and Technology
[2]svkhara@gmail.com

Abstract. A prototype of a multi-user system for access control to data sets stored in a malicious cloud environment is presented. Cloud storage like any other environment needs the ability to securely shared information. The approach here is to provide access control over the data stored in the cloud without provider participation. The main tool of the access control mechanism is a ciphertext-policy attribute-based encryption scheme with dynamic attributes and advanced encryption algorithms. Using a based decentralized ledger, our system provides an immutable log of all meaningful security events, such as key generation, access policy assignments, changes or revocations, and access requests. We propose a set of protocols to ensure the privacy of operations requiring secret or private keys. Only hash codes are transferred through the ledger. The prototype of the system is implemented using smart contracts and tested on the platform..

Keywords: Cloud storage, attribute-based access control, ciphertext-policy attribute-based encryption, ethereum based contracts.

1 Introduction

Today, the requirement of each cloud user is not the same as it used to be, some users need better storage capacity, some need lower storage with better plans hence this paper is the complete solution of unique cloud storage which is completely decentralized to provide utmost transparency. The major security problem with the existing system is that it is unidirectional, hence the user can only rent the storage from the big service providers. Instead of that one can develop an ecosystem in which some users could put their unused resources on rent and others could rent them.

Initially, a huge chunk of the amount in buying the resources is not invested to start extreme servers at one point and pile up all the user data in a single space. This would reasonably reduce the security of the system and also this huge investment upfront, so to get this thing up a better solution based on Blockchain

Technology along with ERC-20 token based on Ethereum for payment systems is presented.

2 Existing systems(Centralized Cloud)

2.1 The vulnerability of Existing Cloud Systems

Currently, most of the cloud systems which are being used are Centralized Cloud System in which a lot of resources are at a single place on which consumers can rent and save their data on those servers. The problem with it is that it has only have one encryption and decryption key as shown below in the figure.

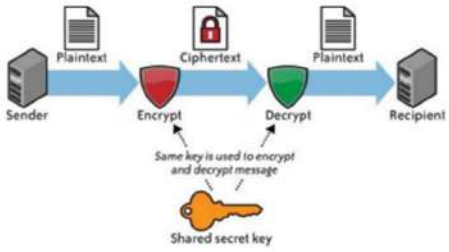

Fig. 1. Centralizsed approach for the cloud storage

With the loss of that encryption key, anyone could decrypt the data and access it. Along with that the initial head cost for implementing the system is quite high which results in higher rent costs. Still, with these higher rent costs, the utmost security of our data is not guranteed.

2.2 Praposed Cloud System(Decentralized Approach)

The distributed network: peer to peer network is the proposed solution for the problem which is based on the blockchain system which is further elaborated down. For a basic overview reference of the following figure is taken which shows how decentralization of cloud would be working on peer networks.

The major tasks to be done are: Encrypting the file, fragmenting it into multiple parts and maintaining the log file in the form of Blockchain to have a record of the system.

This approach enhances the ability to have extremely redundant data bytes which results in enhanced security divisions and contracts which could be developed with the help of ERC-20 blockchain contracts based on Ethereum main network.

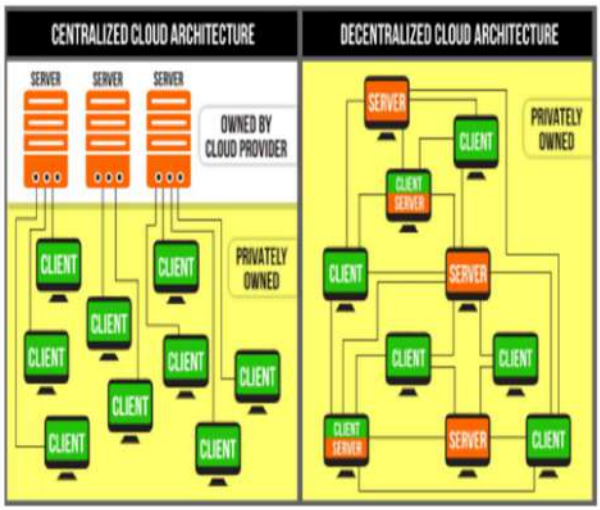

Fig. 1. Centralizsed approach for the cloud storage

The redundancy of the saved data regardless of the amount of data saved compensates when there is any sort of failure in the systems

3 Implementing Cloud Peers

To implement the system on decentralized network there is a need to have data dependencies and complete parity sections for the system in which there is a raid 60 parity system in which each data file could be divided up to 512 distributed peers and each peer could work as an independent ledger. In case of disk failure from host we can retrieve the data with the help of raid systems. This comes up with the complete diversity of the user data for the host systems.

They have to set the minimum amount of resources they put on the platform through which we could have a stable system and equation between the host and the consumer. Each host will be directly connected to a special Blockchain in which consumers would be a part of and consumers would also have their private blockchain network with all of the hosts. Their data is divided in this will lead to better peer to peer transfer of data and better success rate and this will also

enhance the speed of the transaction of the data in the blockchain systems. For the development of this blockchain, we need to work on the hashing algorithms to make dual passkeys to authenticate the host and consumer and this will also lead us to no cross-connection and perfect ledger.

4 Encryption

4.1 Encryption Overview

Blockchain is completely about Encryption and the biggest key you can make with the fastest response time so for this system we need to have dual encryption and decryption system with 4 keys in which we will have one module encryption for our platform to the host platform keys and other set of keys for the user of the system to have his privacy furthermore for the blockchain cryptocurrency which we are going to develop we will be using specially made algorithms which would be based on SHA512 level encoded private keys and public keys,these are the best possible algorithms which would be designed on the top of predefined encryption algorithms in python hashlib libraries and with a bit of modification on those algorithms we can have drastic upstream in performance. For the development of the two-way encryption, metamask key method is the best method to have a secret sequence of random words which would be the backup if the private key gets lost. Whole secret key would be saved in different hardware of the users system itself and at the time of loss we can generate the system bypass key with the help of the master key software which needs to check all of the combinations possible from the user code of CPU and GPU along with the cryptographic hash code given by the platform. Logically to bypass this algorithm we have to make a total of 512**512 which is logically infinite and if we combine the total power of all top 500 supercomputers still it will take more than 320 million years, so logically we can't get into the blockchain.

4.2 Encryption Module

To develop customized algorithms we need to deal with a lot of complex mathematical solutions instead of that we can just deploy our algorithm on top of the SHA512 algorithm which is defined in the hashlib library of python3. We just need to import the sha512 algorithm and update the chip size of the algorithm and along with that, the alphabet consideration to 37 instead of 26 there will be a usage of numbers along with alphabets and the whole system and functions could be inherited as itself. To develop a signature and public key for new users the algorithms which is used is RSA which is defined in a crypto package under Public key PKCS1_v1_5 algorithm will be used from Crypto package under Signature these algorithms are capable of completely generating 512 string length

public key and signatures. The complete algorithm will be working on back end systems with database checking for the database systems we will be using Google Datalabs and BigQuery systems which is one of the fastest for the blockchain systems.

5 Payment

5.1 Payment Systems

Here as the host is letting us use his resources we need to pay them for that dual-mode payment system would be implemented in which each host is potentially a miner, To run the ecosystem we have created one cryptocurrency DCS Coin this will be deployed individually on another Blockchain with the same private and public keys so that both cloud authentication and Cryptocurrency authentication would be same which would make system lot more lightweight. For the development of the complete new coin, we came up with python code on the back end. For another payment gateway we came up with ERC-20 tokens on Ethereum network these are the mini ethereum coins which are worth the same as ethereum and we can also trade them for the development of ERC-20 contract ,Truffle Framework is implemented and on truffle framework we use Ganache to define some user for the scripting language we came up with Solidity with compiler pragma 0.4.23, executable on a remix engine. For inter-platform transactions, we came up with payment gateways that are in use, we are just taking them as they are. Each time any host mines a coin some defined percentage of that transaction is carried forward to that host blockchain account and now that could be reverted into Ethereum coins. To maintain the flow of the coin in the ecosystem the major platform can change the rates of the gas price per transaction of the data uploading and download. This is how the ecosystem and the market of the coin would be controlled.

5.2 Payment Module

It will be defined at the extreme point of Data Transfer while uploading and downloading and prices will differ depending on the available maximum bandwidth to upload and download the data instead of putting a barrier on the amount of the data here we just give unlimited storage access to the consumer and let them pay for the faster download and upload speeds technically to put large chunks of data on same peer network they need to have higher bandwidth speeds. The whole payment module system will be dependent on Blockchain systems in which the host has a different contract with the platform and the user will have different contracts with the platform. Just for example uploading 1Tb file on the peer network with the free basic speed of 128Kb/s user have to wait for 218 years which is logically impossible, for that user have to get into the premium plans and get the higher bandwidths.

6 Performance Boost

For a system to pile up data in a single centralized server it puts up a hell of a lot of strain on it which result in limited bandwidth compare to this multiple ledgers which work as servers with comparatively low resource power works more efficiently and generates more bandwidth capacity for the whole system for an example just think to upload 1Tb file on the existing cloud storage with 50Mbps speed would take 2 days whereas putting that 1Tb file divided into 500 pieces and upload it with same 50Mbps bandwidth will take just 5minites and 43Seconds this shows the drastic performance boost we still need to add 1-2 minutes of performance gap for the allocation of the host and the consumers.

7 Conclusion

The major problem with an existing cloud service provider is the mediator and centralized system which could be solved by including blockchain and having peer to peer decentralized systems and implementing specialized cryptocurrency for payments module and specialized algorithms for encryption and decryption of the data and generation of the public and private keys. After the implementation of the complete ecosystem of hosts(miners) and consumers, we can manipulate the cryptocurrency for the flow of coins in the ecosystem.

References

1. Daniel Drescher Blockchain Basics: A Non-Technical Introduction in 25 Steps (2017)
2. Roger Wattenhofer Distributed Ledger Technology-blockchain (2016)
3. Alan T. Norman Blockchain Technology Explained: The Ultimate Beginner's Guide(2017)
4. Andreas Antonopoulos Mastering Ethereum: Building Smart Contracts and Dapps(2018)
5. Chris Dannen Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners(2017)
6. Kevin Werbach The Blockchain and the New Architecture of Trust(2018)
7. John tromp Cuckoo Cycle: A memory bound graph-theoretic proof-of-work
8. Bela Gipp, Norman Meuschke, Andre Germant Decentralized Trusted Timestamping using the Crypto Currency Bitcoin

Springer

ICMCSI-2020

CERTIFICATE OF PRESENTATION

This certificate is awarded to

Dhruv Doshi

has successfully presented a paper entitled

Blockchain Based Decentralized Cloud Storage

in the International Conference on Mobile Computing and Sustainable Informatics (ICMCSI 2020) organised by Pulchowk Campus, Institute of Engineering, Tribhuvan University, Nepal on 23-24 January 2020.

SESSION CHAIR

ORGANIZING SECRETARY
Dr. Jennifer S. Raj

CONFERENCE CHAIR
Prof. Dr. Subarna Shakya

AHMEDABAD UNIVERSITY | School of Engineering and Applied Science

Ingenium
where innovation is education

This certificate is presented to

Dhruv Doshi

for participating in Ingenious Hackathon 2019 during Ingenium 2019 held at School of Engineering and Applied Science, Ahmedabad University.

George Varughese
Sr. Manager -Administration

Dr. Sanjay Chaudhary
Associate Dean

NUTECH 2018

A NATIONAL LEVEL TECHNICAL COLLOQUIUM

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

Certificate of Participation

This is to certify

that Mr./~~Ms.~~ DHRUV DOSHI *has participated in* HACKNUTHON *under National Level Technical colloquium NU-Tech organized on March 7-8, 2018 at the Institute of Technology, Nirma University.*

Prof. Ath Singhal
Faculty, Co-ordinaator
NU-Tech 2018

Dr. Ankit Thakkar
Faculty, Co-ordinaator
NU-Tech 2018

Dr. Alka Mahajan
Director
ITNU

DCB BANK

Innovation carnival 2017

DEV ACCELERATORS

Certificate of Participation

This certificate is awarded to

DHRUV DOSHI

for

participating in

DCB Bank Innovation Hackathon, 2017

Date: 17/09/2017

Place: AHMEDABAD

Prasanna Lohar

Chief Innovation Officer

DCB Bank Ltd.

INNOVATE > IDEATE > SHOWCASE

Talaash 2018
In search of excellence

CERTIFICATE OF MERIT

SILVER OAK
Education to Innovation

This is to certify that

Mr./Ms. DHRUV DOSHI , PRACHI KADAM

of SILVER OAK COLLEGE OF ENGG. & TECH. *has secured* THIRD *Position in* PAPER PRESENTATION *event in Techfest organized by Silver Oak Group Of Institutes during 13th-14th Feb 2018.*

Talaash 2018 In search of excellence

IEEE SOCET SB

Dr. Saurin Shah
Principal SOCET

Dr. Siddharth Jadeja
Principal ASOIT

Dr. Sweta Khandwala
Director

BitDegree

VERIFIED
2019

CERTIFICATE
OF COMPLETION

07 August, 2019

Dhruv Doshi

Has successfully completed **Space Doggos - Interactive Learning Solidity Course For Beginners**

BitDegree Foundation VSI ©

INSTRUCTOR

ID-1410989

Spoken Tutorial

Certificate for Completion of C Training

Talk To A Teacher

This is to certify that **DHRUV DOSHI** has successfully completed **C** test organized at **Silver Oak College of Engineering & Technology** by **Satvik Khara** with course material provided by the Talk To A Teacher project at IIT Bombay.

Passing an online exam, conducted remotely from IIT Bombay, is a pre-requisite for completing this training. **UMANG THAKKAR** at **Silver Oak College of Engineering & Technology** invigilated this examination. This training is offered by the **Spoken Tutorial Project, IIT Bombay, funded by National Mission on Education through ICT, MHRD, Govt., of India.**

September 23rd 2017

Prof. Kannan M Moudgalya
IIT Bombay

1365248YWA

Spoken Tutorial

Certificate for Completion of Cpp Training

Talk To A Teacher

This is to certify that **DHRUV DOSHI** has successfully completed **Cpp** test organized at **Silver Oak College of Engineering & Technology** by **Satvik Khara** with course material provided by the Talk To A Teacher project at IIT Bombay.

Passing an online exam, conducted remotely from IIT Bombay, is a pre-requisite for completing this training. **UMANG THAKKAR** at **Silver Oak College of Engineering & Technology** invigilated this examination. This training is offered by the **Spoken Tutorial Project, IIT Bombay, funded by National Mission on Education through ICT, MHRD, Govt., of India.**

February 26th 2018

Prof. Kannan M Moudgalya
IIT Bombay

1792410JER

BitDegree

VERIFIED
2019

CERTIFICATE
OF COMPLETION

09 August, 2019

Dhruv Doshi

Has successfully completed **The Complete Nmap Ethical Hacking Course : Network Security**

Access Academy (Nathan House)

INSTRUCTOR

ID-1413915

IGNITE 3.0 | TECHNICAL COUNCIL
Indian Institute of Technology Gandhinagar
Palaj, Simkheda, Gujarat- 382355
E-mail- ignite@iitgn.ac.in

Certificate of Participation

This certificate is awarded to **Dhruv Doshi** for participating in ***Technical Mashup*** held in IGNITE 3.0 at Indian Institute of Technology Gandhinagar.

Date: 11/03/17

Prof. Nihar Mohapatra
(Faculty Advisor - IGNITE 3.0)

Certificate of Completion

This is to certify that Dhruv Doshi successfully completed 2 hours of Build with Blockchain: Deploy your own private blockchain online course on Aug. 11, 2019

Edward Burton — Edward Burton, Instructor

Keir Finlow-Bates — Keir Finlow-Bates, Instructor

&

Udemy

#BeAble

Certificate no: **UC-X0H1PZ02**
Certificate url: **ude.my/UC-X0H1PZ02**

IGNITE 4.0 | TECHNICAL COUNCIL
Indian Institute of Technology Gandhinagar
Palaj, Simkheda, Gujarat- 382355
E-mail- ignite@iitgn.ac.in

CERTIFICATE OF PARTICIPATION

This is to certify that

Dhruv Doshi

participated in CONFERRAL in IGNITE 4.0 at
Indian Institute of Technology Gandhinagar on
11th March, 2018.

Prof. Atul Bhargav
Faculty Advisor
Technical Council

Certificate of Completion

This is to certify that Dhruv Doshi successfully completed 8 hours of Python Core and Advanced online course on June 17, 2019

Bharath Thippireddy

Bharath Thippireddy, Instructor

&

Udemy

#BeAble

Certificate no: **UC-6F70B1E4**
Certificate url: **ude.my/UC-6F70B1E4**

Certificate of Completion

This is to certify that Dhruv Doshi successfully completed 8 hours of Code Your Own Cryptocurrency on Ethereum (ERC-20 Token) online course on May 7, 2019

Gregory Mc Cubbin

Gregory McCubbin, Instructor

&

Udemy

#BeAble

Certificate no: **UC-5X7OVNXU**
Certificate url: **ude.my/UC-5X7OVNXU**