ORDERLY SURVEY OF SAFETY WEAKNESSES IN ETHEREUM BLOCKCHAIN BRILLIANT AGREEMENT

[1]Sunkireddy Dileep Reddy, [2]Thummidi Moksha Sri, [3] Vadla Sai Roshan, [4]G.Nagamani
[1,2,3]UG Scholars, [4]Assistant Professor
[1,2,3,4] Department of Computer Science and Engineering
[1,2,3,4]Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India.

***Abstract*: Cloud computing has grown to become an integral part of present as well as future information technologies. This technology has been designed to be used with internet by providing features such as information storage, remote access, etc. Cloud computing has been proved as an effective tool for all the provided services but it also comes with various types of threats. Over the years of its development, different fire attacks and data theft has been reported as a crucial factor since the data stored in the cloud by an organization or an individual user is basically confidential and sensitive. These data are illegally accessed by many hackers and further it will be used to fire attack the user. This paper mainly aims to highlight such attacks and provide suggestions for sorting the data breaching issues**

Keywords: Smart Contracts,Ethereum Blockchain, Decentralized Applications (DApps), Cryptographic Hash Functions

I. INTRODUCTION

Data storage has always been a place for useful information shortage. Even with large scale data storage devices, the space will not be adequate to store the existing huge amount of information. Cloud computing is basically considered as an internet-centric open standard model. This model is full of different types of services which include both hardware and software. The service providers do not require any high management efforts for provision and maintenance of these services. The term “cloud computing” aims to enhance the capabilities of high power computing systems. It also aims to reduce the price by hiking its efficiency as well as performance. Though the benefits and facilities provided are very much effective, the available technical barriers might stop cloud computing from being a ubiquitous service.

One of the main constituents of the cloud computing is security and it also remains as the most significant concern of the system. It usually suffers from various types of security concerns and attacks like malicious codes. In addition, various new concerns like storage and moving of data through the cloud is a big problem for the user. The possibility of locating in a different place with different regulations adds a lot to this problem.

It is also very much important for a cloud service provider to confirm the usability and availability of their services. There are various reasons that could affect the availability and the accessibility of the computing resources like service denial or natural/unnatural disasters. Data privacy is one of the prime concerns associated with the security of cloud computing as the data must be protected from any third party, which is frequently reported by the users. Since, cloud computing is used for sharing data, data theft is remaining remaining as very common and big risk, which is available for both users and service providers.

Though virtualization is brought in application to benefit the consumer but it has its own disadvantages like issues related to the isolation of the data and communication among the viral machines. Through cloud computing, cyberattacks are more likely to happen. Lot of these cyber-crime belongs to the most common as well as potential encounters which has taken place in the wider internet like malicious insider, DDOS attack, nefarious use and abuse of cloud computing, programming interface of insecure application, etc.

Most of the users uses these services on a regular basis. It can be easily explained with the example of email system which is used for exchanging information in forms of text, images videos, etc.; on demand subscription services; various social networking sites and collaboration tools for working along with the people in real time and over same document. The involvement of services of cloud computing does not end here as it is also brought in application within the various types of businesses and it also provides these services on rent to prevent a one-time investment of the companies.

II. EXISTING SYSTEM

Blockchain is a revolutionary technology that enables users to communicate in a trust-less manner. It revolutionizes the modes of business between organizations without the need for a trusted third party. It is a distributed ledger technology based on a decentralized peer-to-peer (P2P) network. It enables users to store data globally on thousands of computers in an immutable format and empowers users to deploy small pieces of programs known as smart contracts. The blockchain-based smart contract enables auto enforcement of the agreed terms between two untrusted parties. There are several security vulnerabilities in Ethereum blockchain-based smart contracts, due to which sometimes it does not behave as intended.

DISADVANTAGES:

- Organizations without the need for a trusted third party.
- Smart contract enables auto enforcement of the agreed terms between two untrusted parties.

III. PROPOSED SYSTEM

In this paper, a systematic review of the security vulnerabilities in the Ethereum blockchain is presented. The main objective is to discuss Ethereum smart contract security vulnerabilities, detection tools, real life attacks and preventive mechanisms. Comparisons are drawn among the Ethereum smart contract analysis tools by considering various features. From the extensive depth review, various issues associated with the Ethereum blockchain-based smart contract are highlighted. Finally, various future directions are also discussed in the field of the Ethereum blockchain-based smart contract that can help the researchers to set the directions for future research in this domain.

ADVANTAGES:

- Smart contract security vulnerabilities, detection tools.
- Ethereum blockchain-based smart contract are highlighted.
- For secure semantic optimal matching on the ciphertext,

IV. LITERATURE SURVEY:

A) TITLE: Review of blockchain technology vulnerabilities and blockchain-system attacks.
AUTHOR: A. Averin and O. Averina.
YEAR: 2019.
Summary:

Blockchain is a relatively young technology. In recent years, blockchain has gained popularity, which keeps growing. Such interest is mainly due to cryptocurrencies, such as Bitcoin and Ethereum. This technology has presented promising prospects of application. With the increasing interest in blockchain from cryptocurrency to smart contracts, there are precedents of attacks on the blockchain platform. This, in turn, encourages consideration of blockchain in terms of security, identifying vulnerabilities and predicting the emergence of new vulnerabilities. That further would allow to find new methods and solutions for blockchain security. In this paper, the known vulnerabilities were considered, as well as the known attacks on blockchain and their successful implementations in recent times.

B) TITLE: From institutions to code: Towards automated generation of smart contracts.

AUTHOR: C. K. Frantz and M. Nowostawski.
YEAR: 2016.
Summary:

Blockchain technology has emerged as a solution to consistency problems in peer to peer networks. By now, it has matured as a solution to a range of use cases in which it can effectively provide the notion of third party trust without the need for a trusted (physical) third party, which makes it an attractive coordination mechanism for distributed systems. To promote the wide adoption of this technology, we yet lack mechanisms that make the specification and interpretation of smart contracts accessible to a broader audience. In this work, we propose a modeling approach that supports the semi-automated translation of human-readable contract representations into computational equivalents in order to enable the codification of laws into verifiable and enforceable computational structures that reside within a public blockchain.

C) TITLE: Semantic-aware searching over encrypted data for cloud compution.

AUTHOR: Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie.**YEAR:**

2019.
Summary:

With continuously changing operational and business needs of the organizations, Decentralized Autonomous Organizations (DAO) is the current need of the organizations. Centralized Autonomous Organization (CAO) lack transparency and are managed by few efficient managers whereas Decentralized autonomous Organization's (DAO) is novel scalable, self-organizing coordination on the blockchain, controlled by smart contracts and its essential operations are automated agreeing to rules and principles assigned in code without human involvement. In this chapter we discuss the needs for Decentralized Autonomous Organizations (DAO) and key efforts in this field. We then introduce a prospective solution employing blockchain Ethereum, which incorporates a Turing complete programming language with smart contract computing functionality. A solution is elaborated that permits the formation of organizations where participants preserve straight real-time check of contributed collects and governance policies are formalized, automatized and imposed using software. Basic code for smart contract is composed to make a Decentralized Autonomous Organization (DAO) on the Ethereum blockchain.

V. METHODOLOGIES

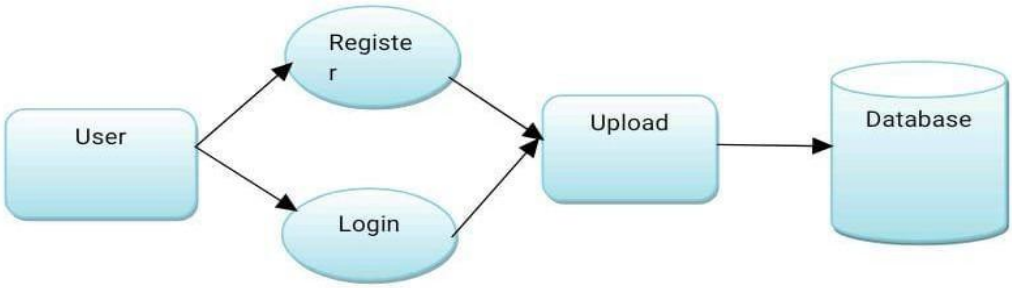
MODULES NAME:

1. User
2. Smart Contract
3. Triggered Manager
4. Ethereum Blockchain

MODULES EXPLANATION

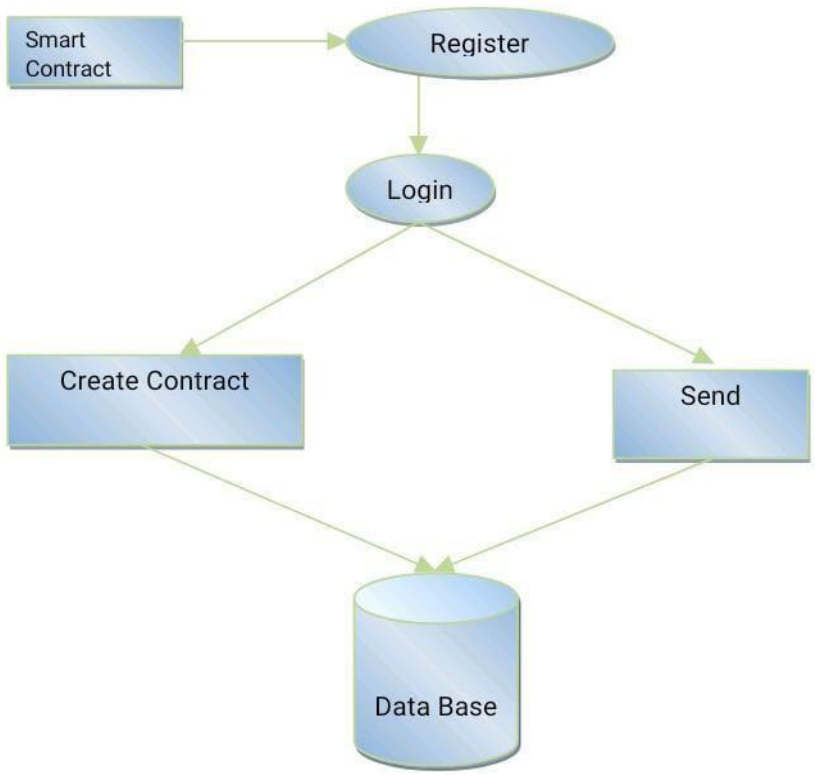
- **User**

  In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



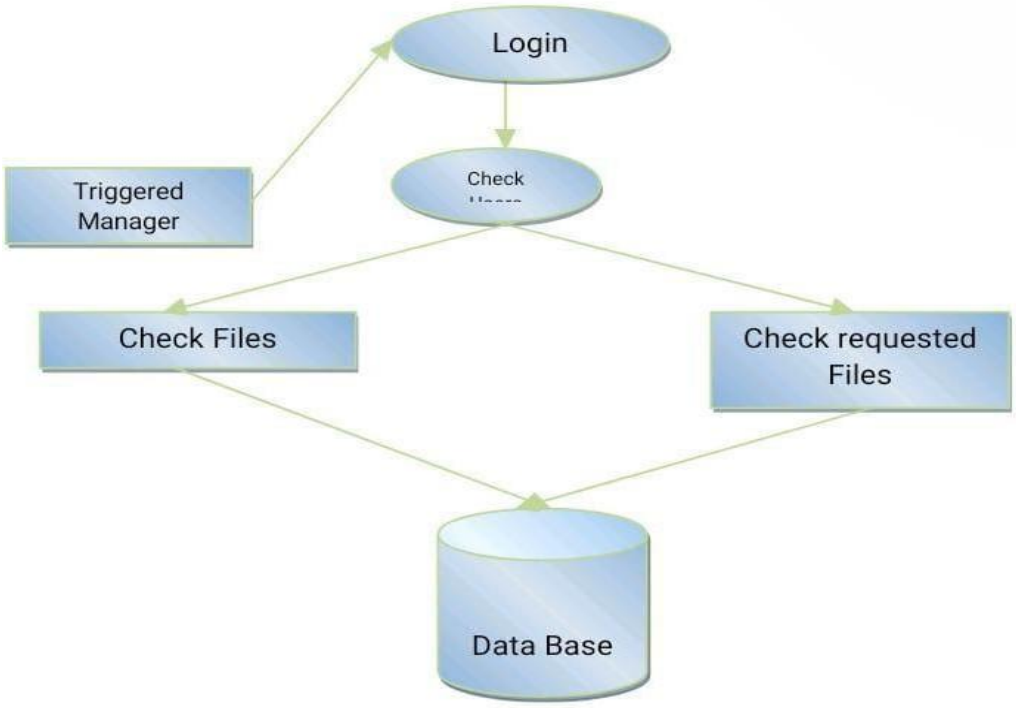
- **Smart Contract**

  This is the first module smart contract can register and Login. After Login This is the first module smart contract can register and Login. After login smart contract have an option to create contract. Smart contract can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the the request and then smart contract can takes permissions from the owner then the file it will downloaded in plain text.



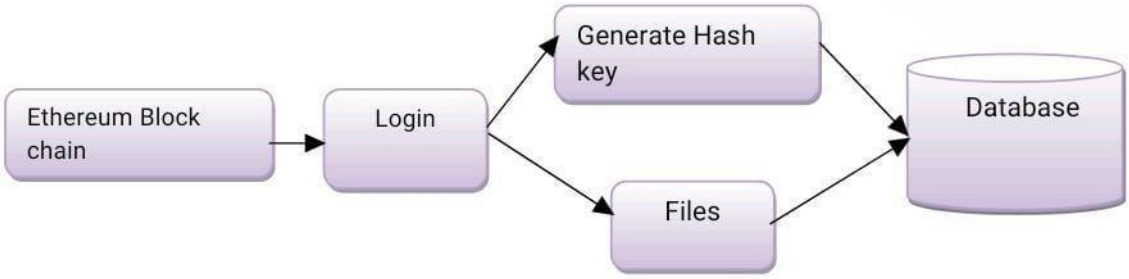
- **Triggered Manager**

  This is the third module of this project. In this module triggered manager did not have any registration and this module have login only. Triggered Manager will check users, check files and check requested files also

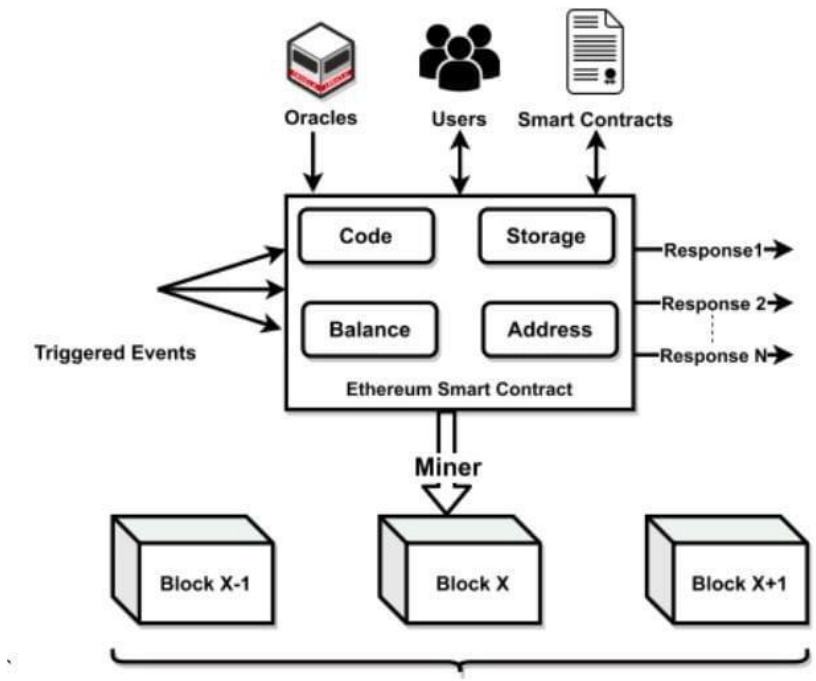


- **Ethereum Blockchain**

  This is the fourth module in this project. This module also have login only and this module will generate hash key and we will see the user files in this module. This is the final module in this project.



VI. SYSTEM ARCHITECTURE



System Architecture Model

VII. CONCLUSION

This paper aims to exhibit the challenges which are faced by the users of cloud computing over the securities issue and it also shows the most threatening factors which are a real matter of concern. There are various issues and challenges in relation to the security of the cloud computing. These issues have been recognized as high impacts over the confidentiality and trust of the users. All the security risks as well privacy risks with the advancing efficiency and impactful solutions are difficult tasks to understand. Availability, reliability, integrity and confidentiality are extensively are the factors which are extensively brought in applications for the security related issues. As the enhancement in the cloud computing is growing.

VIII. REFERENCES

[1] Jensen, M. Schwenk, J. Gruschka, N. Iacono, "On technical security issues in Cloud" IEEE International Conference on Cloud Computing, pp 109-16, 2009.

[2] Mather, T., Kumaraswamy, S., & Latif, S, Cloud Security and Privacy. New York: O'Reilly, 2009

[3] B. Reddy, R.Paturi, "Cloud Security Issues", IEEE International Conference on Services Computing, 2009

[4] J.Viega, "Cloud Computing and the Common Man", IEEE Computer Society, Vol 42, no.8, pp 106-108, 2009.

[5] A.Singh, M.Sharivastava, "Overview of Attacks on Cloud Computing",International Journal of Engineering and Innovative Technology (IJEIT), Vol 1, no.4, 2012

[6] G.Kulkarni, J.GambhirAmruta, " Security in Cloud Computing" International journal of Computer Engineering & Technology (IJCET), Vol3, no.1, pp 258 – 265, 2012

[7] Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M, "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing, Vol 1, no.1, pp 1-18,2012.

[8] Zissis, D., & Lekkas, D,. "Addressing cloud computing security issues". Future Generation Computer Systems, Vol.28, no.3, pp 583- 592, 2012.

[9] Cloud computing Environment against DDoS Attacks", IEEE, , pp. 1- Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing 5,2011.

[10] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, pp. 214-216, 2011.

[11] M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji," Cloud Computing :Research Issues and Implications", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, no.2, pp. 134- 140, 2013.

[12] Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations", Journal of Computing and Information Technology, Vol. 4,pp 235–246, 2008.

[13] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh," A Novel Open Security Framework for Cloud Computing ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, no.2, pp. 45-52, 2012. [14] Ashish Kumar," World of Cloud Computing & Security ", International Journal of Cloud Computing and Services Science (IJCLOSER) Vol.1, no.2, pp. 53~58 , 2012.

[15] Hemraj Saini, T. C. Panda, Minaketan Panda, "Prediction of Malicious Objects in Computer Network and Defense", International Journal of Network Security & Its Applications (IJNSA), Vol.3, no.6, pp.161-171, 2011.

[16] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajaajan, "A survey on security issues and solutions at different layers of Cloud computing", The journal of supercomputing, Vol. 63, no. 2, pp. 561- 592, 2013.

[17] L.M. Vaquero, L. Rodero-Merino, D. Moran, "Locking the sky: survey on IaaS cloud security", Computing, Vol. 91, no. 1, pp. 93- 118, 2011.

[18] Pankaj Patidar and Arpit Bhardwaj, "Network Security through SSL in Cloud Computing Environment", International Journal of Computer Science and Information Technologies, Vol. 2, no.6, 2011.

[19] Insider Threats Related to Cloud Computing, CERT, July 2012. http://www.cert.org/

[20] P. P. Ramgonda and R. R. Mudholkar, "Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud," International Journal of Computer Technology and Applications, Vol. 3, .no. 3, pp. 1217-1224, 2012. [

21] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[22] Z. Wang, "Security and Privacy Issues within the Cloud Computing," in 2011 International Conference on Computational and InformationSciences,pp.175–178,2011.