e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

ONLINE FRAUD DETECTION USING BLOCKCHAIN

Mr. Maghade Rahul Ratan*1, Mr. Dhakne Balaji Sambhaji*2, Mr. Patil Ganesh Raju*3, Mr. Gaidhane Akshay Sanjay*4, Prof. S.D.Jondhale*5

*1,2,3,4,5B.E Computer Engg. Dept, P.R.E.C. Loni, Ahmednagar, Maharashtra-413736., Savitribai Phule Pune University, India.

ABSTRACT

India is transforming rapidly from a developing country to developed one. Due to which many companies and big corporate entities are established yearly which gives employment to millions of people. Human resource is the backbone of any company. For a company to be successful employee assessment is done by the company at regular intervals. This assessment helps the company in giving appraisal to the employees according to the performance. These assessments are handled directly by providing a questionnaire to the employee and then assess by manager of that specific level in a company. Sometimes managers help the employee close to them get better assessment by tempering or changing the answers for the questionnaires given by the employee. Thus, wrong or underperforming employee gets same bonus and facilities as better performing employees. This will demoralize an efficient employee which will affect the company performance if not handled properly. So, to solve this problem of fraud or tampering of an assessment system of a company we propose a secured assessment framework which will use latest technology named blockchain with a distributed ledger system. First employee answer questionnaire using mobile application. The manager at a specific level will assess the employee under his level from a desktop application. Then comes the final entity admin which will have access to all manager and employee. The data of all the communication will be saved using blockchain where a block will be created for each data entry containing the hash code of next block i.e., primary key of the data entry. The data in the block will be encrypted using AES algorithm. Each table will have a ledger i.e., which operations have been done on the table. Thus, if a manager favours an employee and tampers with employee assessment, he can be caught by doing audit on the blockchain ledger with primary keys in each block. If a block is tampered the original data will not be shown which will be a sign of fraud. Thus, our system will be secured and tamper proof assessment system for employees of a company.

Keywords: Blockchain, Hashing Function, AES, Mobile Computing, Cloud Com-Puting, Distributed Ledger, Employee Assessment.

I. INTRODUCTION

In Blockchain and Cloud Computing are hot topics. Today a lot of things can be achieved in many organizations like a company to achieve data integrity and avail-ability using these two technologies together. It can detect frauds or favoritism at every level in the company and help admin in detecting frauds at each level and increase the productivity and profit making of a company. Thus, these two technologies will deter unwanted use of posts as their misdoings can be detected and stemmed at admin level. Currently, there is need for a modernized approach in handling and assessing employee performance. In the traditional approach the manager plays an important role in employee assessment. The manager can change the assessment of an employee at any stage if necessary. It is quite good but it also gives rise to fraud where a manager gives importance to incompetent employees and hide their incompetence. Thus, this kind of a behavior can keep decision making body of a company in the dark and they will not know the correct assessment of an employee. Thus, this kind of fraud has to be detected and stopped for a company to prosper and develop. In order to solve this problem, there should be a system which can detect these kinds of frauds and increase employee confidence. So, in other words the main objective of this paper is to:

Thus, the rest of the paper is structured as follows:

- Section II. explains literature survey which studies various techniques with their advantages and drawbacks.
- Section III. explains the methodology i.e., mathematical model and algorithms to be used by the system.
- Section IV. explains proposed system with block diagram or system architecture and working of the system.
- Section V. shows the results of how the application are implemented and how they can be used.

II. LITERATURE SURVEY

This section describes the fundamentals of various security and cloud computing techniques that can be used in designing a new more reliable online fraud detection in employee assessment to help a company to get best performing employee list correctly. It helps in understanding various ideas put forward by various technical papers published by various authors and how they put forth a more accurate and concrete techniques. Some of the ideas with technique and drawbacks are mentioned below:

1. Paper: - SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities. Year: - 2020.

Author: - MANAF ZGHAIBEH , UMER FAROOQ , NAJAM UL HASAN AND IMRAN BAIG.

Technique: - Healthcare system using blockchain.

Drawback: - This paper gives is quite good and handles all the concepts needed for a secured healthcare system but it does not explain or give insights of how this system can be used in other fields than healthcare.

2. Paper: - A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing.

Year: - 2018.

Author: - Tian Wang , Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu and Yang Liu. Technique: - Cloud storage using Fog Computing.

Drawback: - This paper is quite good and explain how to use distributed cloud technology in designing our system but it lacks the explanation of how to use blockchain technology with it.

3. Paper: - Employee Performance Assessment with Profile Matching Method.

Year: - 2018.

Author: - Safrizal, Lili Tanti, Ratih Puspasari and Budi Triandi. Technique: - Employee assessment using profile matching.

Drawback: - This paper is quite good and the questionnaire used in it can be used in our system but it lacks the explanation of how to use blockchain and cloud computing technology with it.

III. METHODOLOGY

This section will study the mathematical conditions and algorithms to be used for designing a secured and multilayer malicious URL detection framework. These are explained as follows:

A Mathematical Model Our projects mathematical perspective can be put and described as given below. Set Theory Applied to the Project.

1. Employee: -

Set(E)=fE0, E1, E2, E3, E4, E5, E6g E0 2 E = Register.

E1 2 E = Answer assessment questionnaire.

E2 2 E = Submit assessment.

E3 2 E = Save assessment by distributing fields data on different clouds.

E4 2 E = Get primary keys of data and embed them as data in block of a blockchain. E5 2 E = Create a block in blockchain using hash and encryption.

E6 2 E = Save block of blockchain in the ledger.

2. Manager: -

Set(M)=fE0, M0, M1, M2, E3, E4, E5, E6g E0 2 M = Register.

M0 2 M = fetch assessment.

M1 2 M = retrieve and view assessment from different clouds. M2 2 M = Update and save assessment on manager side.

E3 2 M = Save assessment by distributing fields data on different clouds.

E4 2 M = Get primary keys of data and embed them as data in block of a blockchain.

E5 2 M = Create a block in blockchain using hash and encryption. E6 2 M = Save block of blockchain in the ledger.

Probability, NP-Hard and NP-Complete

So, by studying the sets as defined above we come to notice that elements E0, E3, E4, E5, E6 are common in both modules and used in coordination in both sets which can be placed as

$$x\ 2\ E \setminus M\ i\ f\ \ x\ 2\ E\ \ \text{and}\ x\ 2\ M$$

Thus, the probability of intersection of elements in both modules can be given as

$$P(E \setminus M) = P(E) + P(M)$$

So, intersection of common elements can be shown as

$$E \setminus M = fE0;\ E3;\ E4;\ E5;\ E6g$$

The conditional probability of both modules using the same elements can be shown as

$$P(E\ M) = \frac{P(E \setminus M)}{P(M)}$$

j

Thus, we conclude that our project "Online Fraud Detection in E-Assessment Using Blockchain" success and failure will depend upon the internet as it sends assessment answers from employee to cloud, i.e., if the internet connection is not good or not present the answers will not be fetched and sent and the project won't work, thus this is a case of failure, so our project supports NP-Hard and not NP-Complete.

IV. PROPOSED SYSTEM

This This section is mainly divided in 3 main modules with other sub parts in them. The text that follows explains the modules with a block diagram or system architecture as shown in Fig.2. to illustrate them. The working of the framework is explained as:

- Blacklist URL dataset:

In this module we are proposing to use Google Drive as Cloud. The Google Drive sub cloud Google Sheets will be used to store blacklisted URL's and feature keywords. The google sheets is free cloud where the information can be stored and retrieved at any time anywhere. To store URL and keywords we will have a form in desktop application which will use google sheets as backend. The communication with the cloud and desktop application will be done using Google Drive and Google Sheets API. This cloud model will be used by both techniques i.e., Malicious URL detection using SVM and R-CNN.

- SVM:

In this module we first propose to fetch the backlisted dataset from google cloud. Then feature extraction will be done on blacklisted URLs using OPEN-NLP. The extracted feature keywords will be used to create a training dataset which will train SVM. Then a testing URL will be passed from which a testing dataset will be created. Both training and testing datasets will be passed to SVM algorithm which will give a classification results in the form of two classes i.e., safe and malicious.

- R-CNN:

This this module we also first propose to fetch the backlisted dataset from google cloud. Then feature extraction will be done on blacklisted URLs using OPEN-NLP. The extracted features will be used to create a text vector which will be used to train a R-CNN model. The R-CNN model will have all the layers necessary to predict the results properly. The layers will be fine-tuned for better predictions if necessary. Then after training the R-CNN a URL from dataset or any other URL will be passed to it for prediction. The prediction will be in the form of two labels i.e., safe or malicious

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

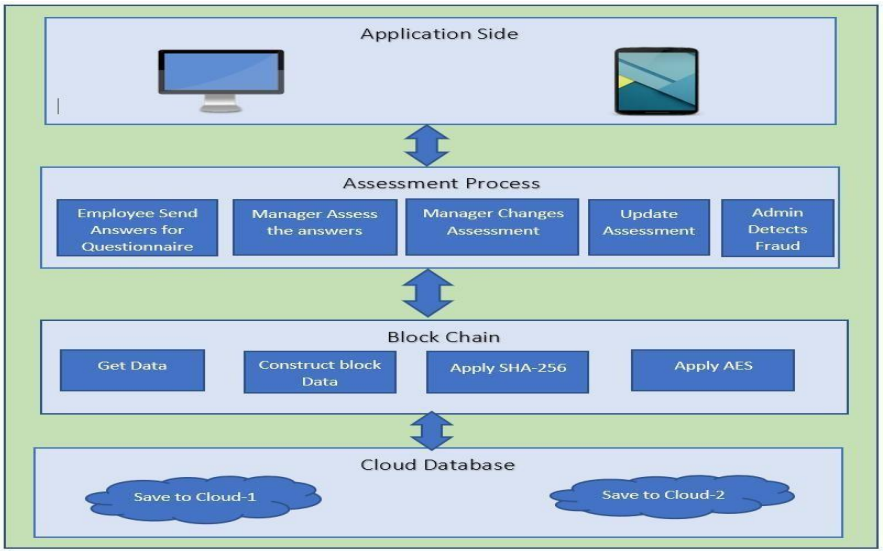

Fig.1: System Architecture Diagram.

V. RESULTS AND DISCUSSION

The system can be explained using following screenshots:

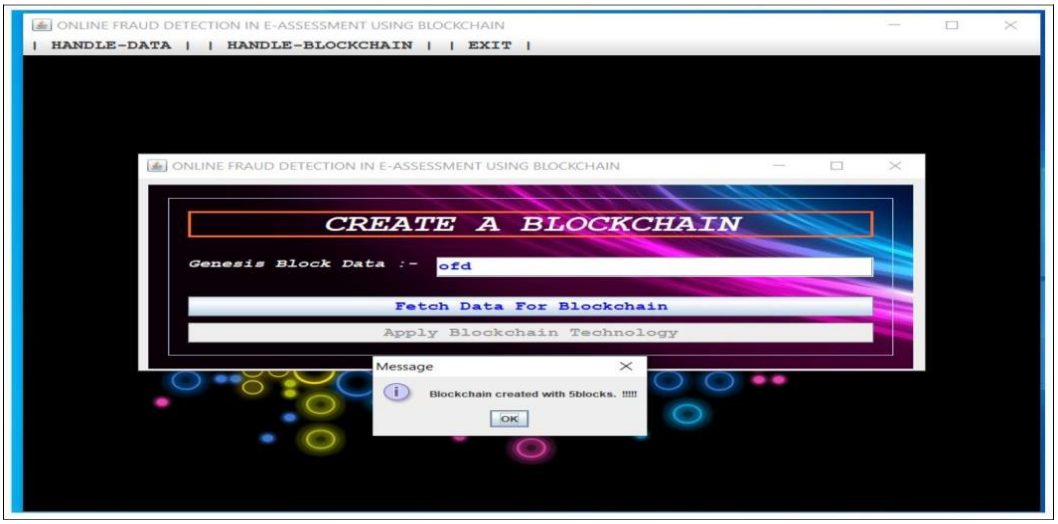

Fig.2: Create a blockchain.

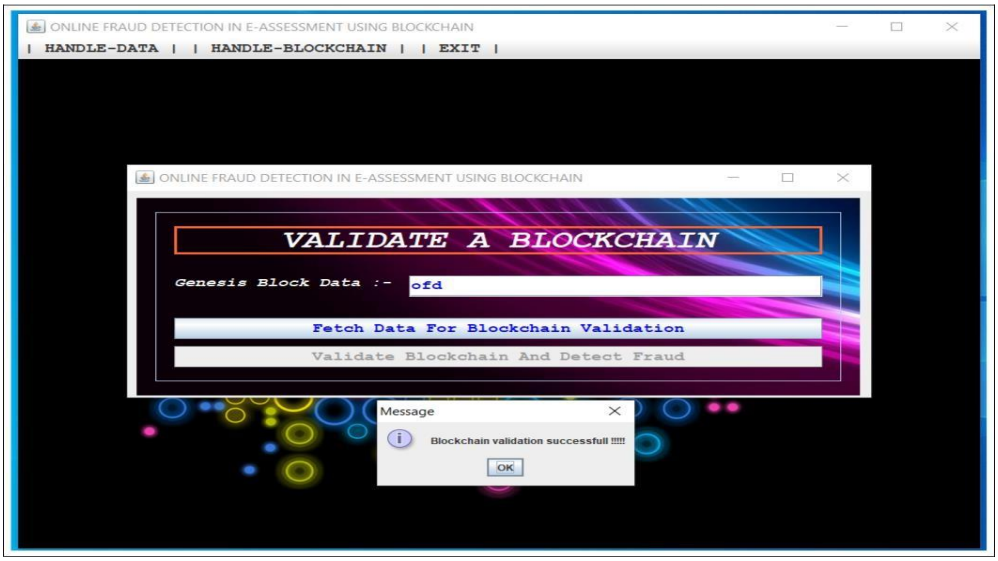

Fig.3: Validate a blockchain.

VI. CONCLUSION

In this project, we are developed novel collaboration of cloud and blockchain together to create a more secured employee assessment system for a company. The basic idea of the project was to design a tamper proof employee assessment system for a company to get correct and untampered assessment. While designing the project we incorporated ideas from [1][2][3] to fit different ideas in one framework. We have implemented blockchain technology properly using SHA-256 and AES algorithms. We also have used multiple clouds to create a distributed system required for blockchain. We have a designed a block authenticity technique for blockchain to detect tampering and catch employee assessment fraud. Thus, we conclude that our project will be very helpful for a company to get tamper free and correct employee assessment.

VII. REFERENCES

[1] IMRAN BAIG., " SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities." IEEE-2020.

[2] Tian Wang , Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu and Yang Liu., "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Com-putational Intelligence in Fog Computing." IEEE-2018.

[3] Safrizal, Lili Tanti, Ratih Puspasari and Budi Triandi, "Employee Performance Assessment with Profile Matching Method." IEEE-2018.

[4] H. Ahvenniemi, A. Huovila, I. Pinto-Seppa,¨ and M. Airaksinen, "What are the differences between sustainable and smart cities," Cities, vol. 60, pp. 234-245, Feb. 2017.

[5] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Sep. 2016, pp. 1-3.

[6] A. Haapio, "Towards sustainable urban communities," Environ. Impact Assessment Rev., vol. 32, no. 1, pp. 165-169, Jan. 2012.

[7] X MANAF ZGHAIBEH , UMER FAROOQ , NAJAM UL HASAN AND. Zhang, "Toward a regenerative sustainability paradigm for the built environ-ment: From vision to reality," J. Cleaner Prod., vol. 65, pp. 36, Feb. 2014.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, Aug. 2016, pp. 25-30.

[9] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174-1188, Aug. 2014.

[10] A. Mohsen Nia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological information leakage:A new frontier in health information security," IEEE Trans. Emerg. Topics Comput., vol. 4, no. 3, pp. 321-334, Jul. 2016.