IJRETS: International Journal Of Research In Engineering, Technology And Science,
Volume XIII, Issue VIII, November.2020, ISSN 2454-1915, www.ijrets.com,
1st online international conference on informatics, robotics, construction & communication, 2020

PUBLIC KEY INTEGRITY VERIFICATION AGAINST THIRD PARTY AUDITORS

S.Saravanan[1], R. Sundar Dass[2]
Assistant Professor[1], Assistant Professor[2] PERI Institute of Technology
saravananoct18@gmail.com[1], apcesundar@gmail.com[2]

ABSTRACT:

The sending of distributed storage administrations has critical advantages in overseeing information for clients. Be that as it may, it likewise causes numerous security concerns, and one of them is information uprightness. Open check methods can empower a client to utilize an outsider evaluator to confirm the information honesty for the benefit of the organization, while existing open confirmation plans are defenseless examiners who may not perform confirmations clearly. In this paper we propose a third-party auditor delegated for the background verification process which is done on the part of every organization. In our project a novel way of verification introduced which implements the block chain technology. By usage of block chain each and every data about the candidate which is available in the database will remains secured. We use this technology to access the related previous data about a candidate who is going to be verified by the auditor, by providing a unique identity for the each entity involved in the verification process. After the process gets over, the auditor will update the results status into the database and then the candidate will be available to the organization for further process. By the usage of this block chain technology the background details of the persons will stored in a confidential manner.

Keywords : Block chain , Unique Key

I.INTRODUCTION

WITH cloud storage services, users outsource their data to cloud servers and access that data remotely over the Internet [1], [2]. These services provide users an effificient and flflexible way to manage their data, while users are free from heavy local storage costs [3], [4], [5]. Although users enjoy great benefifits from these services, data outsourcinghas also incurred critical security issues [6], [7], [8]. One of the most important security concerns is data integrity [9],[10]. Unlike traditional data management paradigm, where users store their data locally, users would not physically own their data once having outsourced the data to cloud servers. Therefore, users