A Personal Information Management Using Block Chain

Shubhankar Kanore, Aditya Yadav, Sawid Deshmukh

Shatabdi College of Engineering

Abstract: The recent increase in reported incidents of surveillance and security breaches compromising user's privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Disclosure of user's personal data is a serious breach of privacy. Traditional database storage options have proven to be quite inefficient in protecting such sensitive data. Records can be stolen and tampered with on cloud based services. Our system proposes a decentralized system of storing user personal data using a novel technology, Block chain. Block chain technology has thus far been able to prevent unauthorized access with its secured cryptographic algorithms and its immutability makes the data tamperproof. We are creating the smart system which is based on data ownership, data transparency, auditability and fine-grained access control. According to the results of this study, countries where national data protection authorities have the power, and the resources, to enforce data protection laws in a consistent and predictable manner represent a positive institutional environment for organizations. In these contexts, organizations are more likely to develop a strong privacy culture, which is a necessary condition to adopt fair information practices and respect data subject's rights. We are storing personal data using block chain to avoid unauthenticated modifications and data stealing, Block chain provide features to overcome the draw backs of existing system

Keywords: Decentralized system, Block chain, Data, Transparency, access control.

INTRODUCTION

We are creating the smart system which is based on data ownership, data transparency, auditability and fine-grained access control. According to the results of this study, countries where national data protection authorities have the power, and the resources, to enforce data protection laws in a consistent and predictable manner represent a positive institutional environment for organizations. A block chain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a block chain is resistant to modification of the data.Personal Data Clouds ("PDCs") is one such privacy enhancing solution that has recently garnered considerable attention1 . PDCs are data management and sharing systems designed to empower individuals and help them regain control over their data. The term "PDC" is sometimes used interchangeably with "Personal Data Vaults", "Personal Data Stores", or "Personal Data Services". The origin of PDCs can be traced to the development of personal information management systems, which in turn arose out of the need to achieve better management of dispersed data. These systems, however, were not primarily concerned with the preservation of privacy, which is why the idea of PDCs is not only to enable individuals to collect, store, manage, use, and share their personal data, but to do so according to their own levels of privacy comfort, trust and needs. These developments have been bolstered by the appearance of technical standards, such as XDI ("extensible Data Interchange"), a semantic data interchange format and protocol under development by the OASIS XDI Technical Committee.2

LITURATURE SURVEY

- "Big Data Model of Security Sharing Based on Blockchain", P Li Yue ; Huang Junqin ; Qin Shengzhi ;is a author of this paper, this paper published in 2017. Advantage of his project is, The rise of big data age in the Internet has led to the explosive growth of data size. However, trust issue has become the biggest problem of big data, leading to the difficulty in data safe circulation and industry development. The blockchain technology provides a new solution to this problem by combining non-tampering, traceable features with smart contracts that automatically execute default instructions. In this paper, we present a credible big data sharing model based on blockchain technology and smart contract to ensure the safe circulation of data resources.
- "Blockchain: A game changer for securing IoT data" is paper of S Madhusudan Singh ; Abhiraj Singh ; Shiho Kim National Conference on Emerging Trends in Engineering Technology 2018 Internet of Things (IoT) is now in its initial stage but very soon, it is going to influence almost every day-to-day items we use. The more it will be included in our lifestyle, more will be the threat of it being misused. There is an urgent need to make IoT devices secure from getting cracked. Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems. Existing security technologies are just not enough to deal with this problem. Blockchain has emerged as the possible solution for creating more secure IoT systems in the time to come. In this paper, first an overview of the blockchain technology and its implementation has been explained; then we have discussed the infrastructure of IoT which is based on Blockchain network and at last a model has been provided for the security of internet of things using blockchain.
- Sunghyun Cho ; Sejong Lee [1] in this paper described A network composed of lightweight devices such as IoT has problems due to limited resources such as 3 Admission process using Blockchain lack of storage space and low computing performance. These issues pose significant challenges in the application of robust security technologies, which reduces network security performance. The blockchain with strong security is a suitable technology to solve IoT problems with weak security. As a result, various research is being carried out to increase security, lightness, and efficiency of the IoT network by applying blockchain to IoT. This paper introduces the trend of research to apply blockchain to IoT.
- The Blockchain is an emerging paradigm that could solve security and trust issues for Internet of Things (IoT) platforms. We recently introduced in an IETF draft ("Blockchain Transaction Protocol for Constraint Nodes") the BIoT paradigm, whose main idea is to insert sensor data in blockchain transactions. Because objects are not logically connected to blockchain platforms,

controller entities forward all information needed for transaction forgery. Never less in order to generate cryptographic signatures, object needs some trusted computing resources. In previous papers we proposed the Four-Quater Architecture integrating general purpose unit (GPU), radio SoC, sensors/actuators and secure elements including TLS/DTLS stacks. These secure microcontrollers also manage crypto libraries required for blockchain operation. The BIoT concept has four main benefits: publication/duplication of sensors data in public and distributed ledgers, time stamping by the blockchain infrastructure, data authentication, and non repudiation.

AIM & OBJECTIVES

- Our aim is to provide a Innovative system that allows user to secure his/her information from unauthentic access.
- Basic objective of system to provide better quality in minimum cost.

MOTIVATION

Data is often presented as “the new oil” of our (digital) world, a key asset with both economic and social value . The term “big data” is used to describe the massive processing of high volumes of data produced very quickly by various sources. Despite the opportunities, innovation and growth arising from this omnipresence of data, users find it all the more difficult to have their privacy boundaries clearly delineated and respected in the era of big data. Increasingly, the same sets of personal data are collected by different service providers, each with their purpose and specific approach. Data subjects seeking to access their own data must acquiesce to the terms imposed by these providers, which dramatically decreases the effective control that users have over their personal data.

SYSTEM ARCHITECTURE

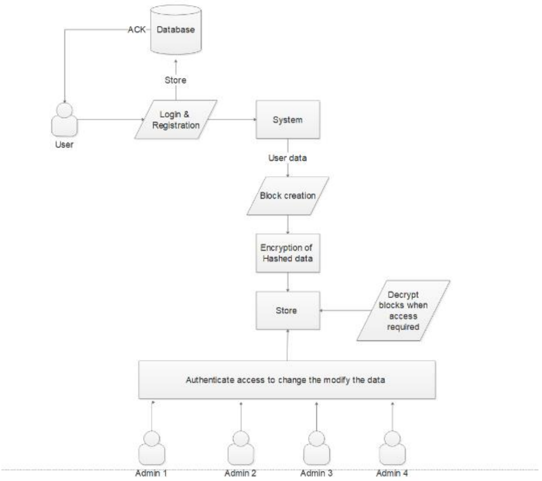
ACK
Database
Store
User
Login & Registration
System
User data
Block creation
Encryption of Hashed data
Store
Decrypt blocks when access required
Authenticate access to change the modify the data
Admin 1
Admin 2
Admin 3
Admin 4

Fig -1: System Architecture Diagram

APPLICATION:

- Institutions for teaching the Data Privacy material developed by the developer for mobile learning.
- Students can study with ease.
- The education application developer can use this framework for developing number of applications that can be imported on mobile devices

FUNCTIONAL & NON-FUNCTIONAL REQUIREMENTS

Functional requirements: may involve calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describe all the cases where the system uses the functional requirements; these are captured in use cases.

Nonfunctional Requirements: (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.

Functional requirements

- Registration
- User Login
- Creation of database: Users Mandatory Information

Design Constraints:

1. Database
2. Operating System
3. Web-Based Non-functional Requirements

Security:

1. User Identification
2. Login ID

3. Modification

Performance Requirement:

1. Response Time
2. Capacity
3. User Interface
4. Maintainability
5. Availability

SYSTEM REQUIREMENTS

Software Used:

- HTML
- Action Script
- PHP

Hardware Used:

- AMD/Intel Processor
- 2GB RAM for application development • Min. 16 GB Hard Disk

Summary

Block chain technology is employed in SCM in a variety of sectors. The present state of use of block chain and smart contracts in numerous major industrial domains is studied in this paper. The survey delivers academically sound data on the overall state of block chain deployment for various supply chains. The study's findings show that research on block chain -based supply chains is a growing topic garnering a lot of attention. The majority of the reviewed papers that were evaluated agreed on the prospective benefits that block chain may offer to the supply chain**.**

REFERENCES

[1] James Ball. Nsa's prism surveillance program: how it works and what it can do. The Guardian, 2013.

[2] Mobile Data Privacy in review: Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proceedings of the twentieth annual ACM symposium on Theory of computing, pages 1–10. ACM, 1988

[3] A Design Requirements Framework for Mobile Data Privacy EnvironmentsEUROPEAN COMMISSION. Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. 2012

[4] Mobile Data Privacy in the 21st century: Benefit for learners;Geddes S.,In The knowledge tree, December 2010.

[5] Mobile learning: A handbook for educators and trainers;Kukulska-Hulme, A., and Traxler, J.,In London: Routledge,2010.

[6] Moving mobile into the mainstream;Stead, G.,In Proceedings of mLearn,2010.

[7] Mobile Data Privacy anytime everywhere;Corlett and Sharples, In London: Data Privacy and Skills Development Agency, 2010.

[8] Cooperative learning: Increasing college faculty instructional productivity;Johnson, In Washington D.C.: School of Education and Human Development, 2011.

[9] Evolution towards Data Security,Marela Andres, EdTechie, 2011.